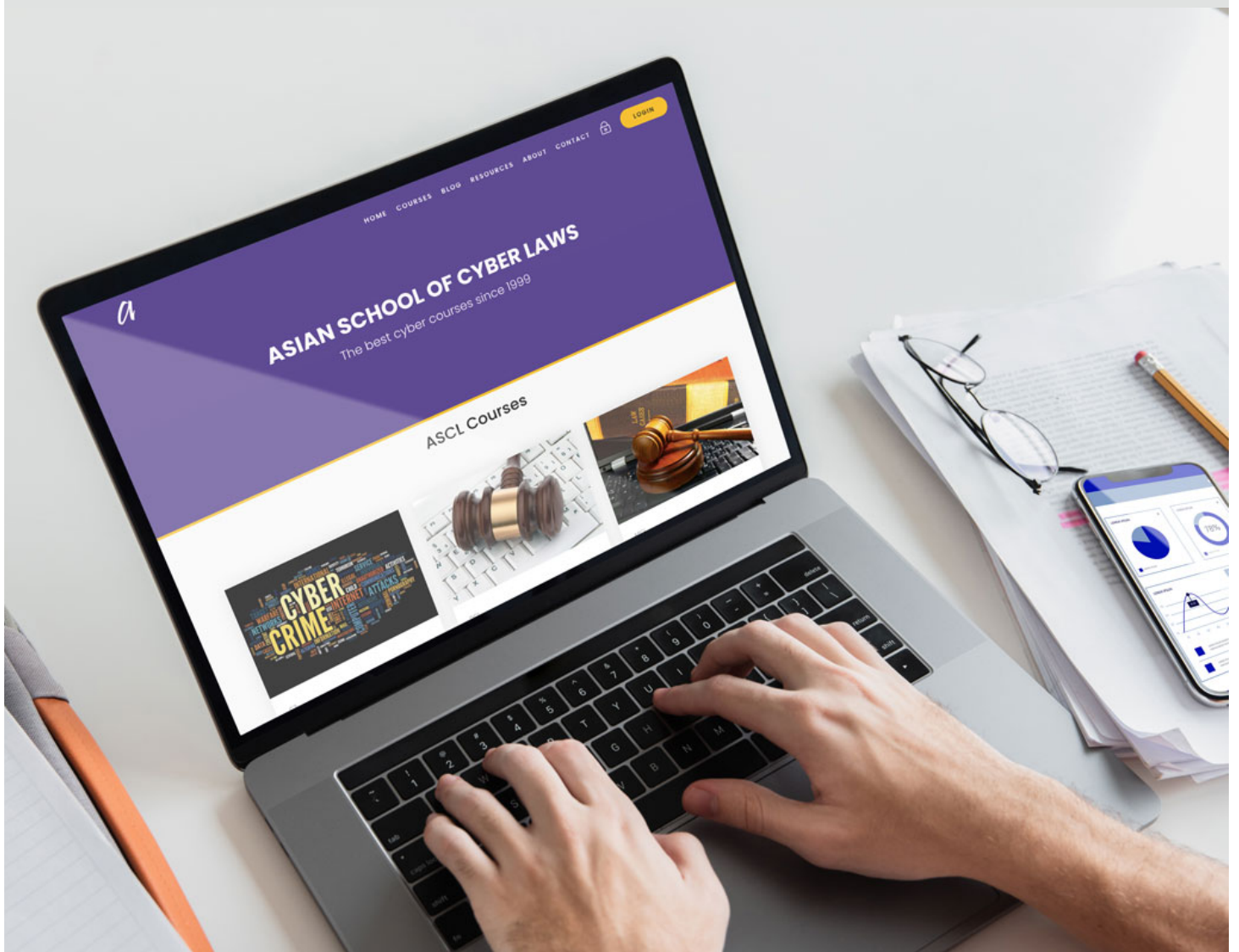


# Cyber Crime Law in India

Asian School of Cyber Laws



**(c) 2021 Asian School of Cyber Laws (ASCL). All rights reserved.**

The information in ASCL documents, social media networks, websites, and videos is for general information only and should not be taken as constituting professional advice.

ASCL is not liable for any loss caused, whether due to negligence or otherwise arising from the use of, or reliance on, the information provided directly or indirectly. ASCL links to external resources for your convenience. We are selective about them but we don't endorse them.

No investigation has been made of common-law trademark rights in any word. Words that are known to have current trademark registrations are shown with an initial capital and are also identified as trademarks. The inclusion or exclusion of any word, or its capitalization is not, however, an expression of the author's opinion as to whether or not it is subject to proprietary rights, nor is it to be regarded as affecting the validity of any trademark.

This book is provided "as is" and the author makes no representations or warranties, express or implied either in respect of this book or the software, websites and other information referred to in this book. By way of example, but not limitation, the author makes no representations or warranties of merchantability or fitness for any particular purpose or that the use of licensed software, database or documentation will not infringe any third party patents, copyrights, trademarks or other rights.

The chosen case scenarios are for instructional purposes only and any association to an actual case and litigation is purely coincidental. Names and locations presented in the case scenarios are fictitious and are not intended to reflect actual people or places. Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favouring by the author, and the information and statements shall not be used for the purposes of advertising.

**Images courtesy:** Unsplash, Freepik, Pixabay, Wikipedia

# Contents

1. Introduction to Criminal Law.....	05
2. Sec 43(a) - Unauthorised access.....	07
3. Sec 43(b) - Unauthorised downloading, copying or extraction.....	12
4. Sec 43(c) - Computer virus, worm, contaminant.....	20
5. Sec 43(d) - Damaging a computer.....	23
6. Sec 43(e) - Disruption of a computer.....	26
7. Sec 43(f) - Denial of Service.....	28
8. Sec 43(g) - Facilitating unauthorised access.....	31
9. Sec 43(h) - Tampering or manipulating computer.....	34
10. Sec 43(i) - Destruction, deletion or alteration.....	38
11. Sec 43(j) - Source code theft.....	45
12. Sec 43A - Failure to protect data.....	54
13. Section 63 – Compounding of Contraventions.....	59
14. Sec 65 - Tampering with computer source documents.....	60
15. Sec 66 - Computer related offenses.....	68
16. Sec 66A - Sending offensive messages.....	73
17. Sec 66B - Dishonestly receiving stolen computer.....	75
18. Sec 66C - Identity Theft.....	77
19. Sec 66D - Cheating by personation.....	78
20. Sec 66E - Violation of privacy.....	81
21. Sec 66F - Cyber Terrorism.....	85
22. Sec 67 - Transmitting obscene electronic material.....	89
23. Sec 67A - Electronic material containing sexually explicit act.....	96
24. Sec 67B - Child Pornography.....	97
25. Sec 67C - Preservation & retention of information by intermediaries.....	109
26. Sec 68 - Power of the Controller to give directions.....	112
27. Sec 69 - Interception or monitoring or decryption of any information.....	114

28. Sec 69A - Blocking of information for public access.....	118
29. Sec 69B - Monitoring and collecting traffic data.....	122
30. Sec 70 - Protected System.....	125
31. Sec 70B - Indian Computer Emergency Response Team.....	129
32. Sec 71 - Penalty for misrepresentation.....	131
33. Sec 72 - Breach of confidentiality and privacy.....	133
34. Sec 72A - Disclosure of information in breach of lawful contract.....	135
35. Sec 73 - Publishing false Electronic Signature Certificate.....	137
36. Sec 74 - Publication for fraudulent purpose.....	139
37. Sec 77A – Compounding of Offences.....	140
38. IPC, Bharatiya Nyaya Sanhita & Cyber crimes against women.....	141

# 1. Introduction to Criminal Law

We have come across instances of theft, marital dispute, murder, defamation, cyber terrorism, etc. How will you know whether these fall under civil or criminal law or both?

Before we look into the various categories of cyber crimes classified under the IT Act, it is imperative to understand what is civil law and how it differs from criminal law.

Under civil law, a dispute arises between two individuals or two classes of individuals. When an individual's right has been violated, he (i.e. the aggrieved party) may approach the court for resolution of that dispute because of which his right has been violated. The aggrieved party (who is called as the plaintiff/claimant) files a suit before a court of law against the respondent.

The court after considering the case, examines the balance of convenience i.e. the balance of comparative loss caused to the applicant and the respondent in the case of not passing the order and thereafter passes an order. The remedies under the order may be given in the form of damages, injunction, specific performance, etc. Civil law at times may also be retrospective in nature.

Although Criminal law also aims at bringing justice to the person to whom wrong has been done, however the larger picture is to deal with situations that are harmful to society as a whole and to maintain law and order. In criminal law, the case is filed by the aggrieved person with the police, who then investigates the matter and thereafter a case is filed in the court. When the court is deciding a criminal case, it relies upon two essential principles - *Mens Rea and Actus Reus*.

Mens Rea means 'guilty mind'. Before a criminal is made liable, the court will look into whether the said criminal had the intention of doing wrong. In addition to Mens Rea, courts also apply the principle of Actus Reus i.e. the 'guilty act'.

It is the guilty intention coupled with the guilty act committed which causes a criminal to be held liable. Under criminal law, the onus is on the prosecution to prove guilt beyond a reasonable doubt. The court may pass an order in the form of imprisonment or fine or both, as per the circumstances of each case.

## 2. Section 43(a) – Unauthorized Access

Unauthorised access is covered by section 43(a) of the Information Technology Act. This section states as under:

### **43. Penalty and compensation for damage to computer, computer system, etc.**

**If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,-**

**(a) accesses or secures access to such computer, computer system or computer network or computer resource;**

**.....he shall be liable to pay damages by way of compensation to the person so affected.**

The two concepts covered in this provision are “accesses” and “secures access”.

According to section 2(1)(a) of the *Information Technology Act*, "access" with its grammatical variations and cognate expressions, means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network;

Essentials of the term “access” are:

(A) Gaining entry into a computer, computer system or computer network

(B) Instructing the logical, arithmetical, or memory function resources of a computer, computer system or computer network

(C) Communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

**Grammatical variations** of access include terms such as accesses, accessed, accessing etc. Cognate expressions are related words and phrases. Depending upon the situation, these could include “log on”, “retrieve” etc. Gaining entry into applies to physical access.

The terms computer, computer system and computer network have been defined very widely under the *Information Technology Act*. These terms may include the physical box (cabinet) in which a computer is housed. They may also include the physical room in which a computer network or super computer is housed.

**Illustration:** A massive super computer is housed in particular premises. Sameer breaks open the door and enters the premises. He has gained entry into the computer.

**Illustration:** A Government computer contains critical information in its hard disk. Sameer unscrews the cabinet of the computer in order to steal the hard disk. He has gained entry into the computer.

**Instructing** means “to give orders” or “to direct”. Instructing is essentially a one way process which does not require two-way communication between the instructor and the instructed.

**Illustration:** A Government computer contains critical information. Sameer enters the room where the computer is located and keys in some commands into the keyboard. He does not realize that the keyboard is disconnected from the computer. Here, Sameer has not instructed the logical, arithmetic or memory functions of the computer.

**Communicating with** is essentially a two-way process that involves exchange of information.

**Illustration:** Sameer is a hacker attempting to steal some information from Sanya’s computer. He first remotely scans Sanya’s computer using specialized software. The software sends out queries to Sanya’s computer which replies to the queries. As a result of this, Sameer obtains details of the operating system installed on Sanya’s computer. Sameer has communicated with Sanya’s computer.

**Secures access** is a term that needs to be examined next. The term “secure” means “to make certain”. The term “secures access” would mean “to make certain that access can be achieved as and when desired by the person seeking to access”. When such access is ensured by a person, he is said to have secured access.



However, the IT Act not only makes a person liable for securing access, but it also makes a person in certain circumstances where he is attempting to secure access. For example, if a person secures access or attempts to secure access to a protected system, he will be held liable under section 70 of the IT Act.

**Illustration:** Sanya is the network administrator of a Government department. She stores the passwords of the Government department main server in her personal laptop.

Sameer is Sanya's friend. Without Sanya's permission, he switches on her laptop and notes down the passwords of the Government department main server. He has accessed Sanya's laptop without her permission.

He has "secured access" to the Government server. Although he has not accessed the Government server, he has "secured" access to it. By obtaining the passwords, he has made certain that he can access the server as and when he desires.

This section covers incidents where the "permission" of the owner or other person in charge of the computer is not obtained. Permission is the "authorization granted to do something" e.g. Sanya permits Sameer to switch on her computer. Permission can be express or implied. Permission can also be complete or partial.

**Illustration:** Sanya is the network administrator of Noodle Ltd. The employment contract that she has signed with Noodle Ltd states that she is responsible for the "complete maintenance and security of the Noodle Ltd computer systems and networks". Noodle Ltd has given her the express permission to access their systems. This is also complete permission. As the network administrator Sanya would need complete access to all parts of the systems.

**Illustration:** Tanya is an employee of the marketing department of Noodle Ltd. All the marketing department employees have been allotted usernames and passwords which allows them to log into the Noodle Ltd main server. Noodle Ltd has given Tanya the implied permission to access their systems. This is also a partial permission. As an employee of the marketing department, Tanya would need access only to that part of the system that contains information relevant to the marketing department.

This section also covers acts that **exceed permission**.

**Illustration:** Sameer is an employee of the finance department of Noodle Ltd. His username and password entitles him to access only limited information on the official Noodle server. Tanya is the senior manager of the finance department. One day, while Tanya is abroad on official business, she calls up Sameer and gives him her username and password. She requests Sameer to retrieve some official documents from the Noodle server and email those documents to her. Sameer complies with her request.

Several days later, Sameer again uses Tanya's password to access the Noodle server. Now he has exceeded the scope of his permission. Tanya had given Sameer an implied permission to use her password only on one occasion. The subsequent use of the password by Sameer is unauthorised and amounts to exceeding the scope of his permission.

Compensation is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim.

Simply put, damages are the compensation for legal injury. Damages can be of various types:

(1) **Compensatory damages** are allowed as a recompense for injury actually suffered.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

(2) **Consequential damages** are consequential upon the act complained of.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.

(3) **Exemplary or punitive damages** are awarded as a punishment and serve as a warning to others.

**Illustration:** Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

(4) **General damages** are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

**Illustration:** Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs 10 lakh as compensation.

# 3. Section 43(b) – Unauthorized Downloading, Copying or Extraction

Unauthorised downloading, copying or extraction is covered by section 43(b) of the Information Technology Act. This section states as under:

## **43. Penalty and compensation for damage to computer, computer system, etc.**

**If any person without permission of the owner or any other person who is in charge of a 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;**

**.....he shall be liable to pay damages by way of compensation to the person so affected.**

This section penalises the following unauthorised acts:

- (1) downloading from a computer, computer system or computer network,
- (2) copying from a computer, computer system or computer network,
- (3) extracting data, database or information from a computer, computer

system or computer network.

Let us examine some of these terms in detail.

The term **download** is generally used for transferring information, software etc. –

- (1) from a remote or distant to a nearby computer
- (2) from a larger to a smaller computer
- (3) from a computer to a peripheral device (e.g. floppy or pen-drive).

**Illustration:** Sameer is browsing the Internet and comes across a useful software program stored on a website. He downloads it from the Internet onto his computer. He then installs it on his computer.

**Illustration:** Pooja uses her personal laptop to connect to her office server. She then downloads the Office Manual from the server onto her laptop.

**Illustration:** Pooja makes an online purchase of some songs. After the payment is processed, she downloads the song from the music company's website onto her cell phone which is connected to her laptop.

**Copies** means “to duplicate or reproduce or imitate something”. The original information is not affected by the copying. It remains unchanged. The copied information may be in a different format as compared to the format of the original information. This can be understood from the following examples.

**Illustration:** Pooja stores all her important data on her laptop in the “D” drive. In order to prevent accidental deletion of her data, she copies it onto the “E” drive of her laptop.

**Illustration:** Pooja reads a very funny joke on a website. The website has stored the joke in an image file so that people cannot simply copy the joke and email it to their friends. The website wants users to refer their friends to its webpage in order to read the joke. Pooja reads the joke on the website and then types it in word by word into a text file in her computer. She has copied the joke.

**Illustration:** Pooja has created an MS Word document on her laptop. She then uses specialised software to convert the document into a PDF (Portable Document Format) file. She has copied the original file and reproduced it in a new format.

**Illustration:** Pooja has purchased a CD containing dozens of songs in mp3 format. Using her computer, she copies the songs from the CD onto her cell phone.

**Extracts** means to derive or obtain something. Extracting usually requires some special effort or skill.

**Illustration:** Pooja has purchased a CD containing songs in “cda” format. Using her computer, she converts the songs into ‘mp3’ format. She has extracted the mp3 format songs from the audio CD that she had purchased.

**Illustration:** Pooja obtains the source code files for open source software. She then uses “compiler” software to convert the source code files into the executable file. This executable file can be used to install the software onto a computer. She has extracted the executable file from the source code files.

**Illustration:** Pooja obtains a software executable file. She then uses “decompiler” software to obtain the source code files that were used to create the executable file. She has extracted the source code file from the executable file.

**Data** is a formalised representation of information, knowledge, facts, concepts or instructions. Data undergoes processing by a computer. Data can be in electronic form (e.g. stored in a CD) or physical form (e.g. computer printouts). Examples of data include computerised attendance records of a school, information in the RAM of a computer, printouts of a computerised accounting system etc.

**Computer database** is a formalised representation of information. The term includes information produced by a computer and intended for use in a computer. This is best understood through the following illustration.

**Illustration:** Noodle School has an automated system for student administration. This system is powered by a database that contains detailed student information. One table of this database is titled “basic\_info” and contains the following categories of information.

**Illustration:** Pooja has purchased a CD containing dozens of songs in mp3 format. Using her computer, she copies the songs from the CD onto her cell phone.

**Extracts** means to derive or obtain something. Extracting usually requires some special effort or skill.

**Illustration:** Pooja has purchased a CD containing songs in “cda” format. Using her computer, she converts the songs into ‘mp3’ format. She has extracted the mp3 format songs from the audio CD that she had purchased.

**Illustration:** Pooja obtains the source code files for open source software. She then uses “compiler” software to convert the source code files into the executable file. This executable file can be used to install the software onto a computer. She has extracted the executable file from the source code files.

**Illustration:** Pooja obtains a software executable file. She then uses “decompiler” software to obtain the source code files that were used to create the executable file. She has extracted the source code file from the executable file.

**Data** is a formalised representation of information, knowledge, facts, concepts or instructions. Data undergoes processing by a computer. Data can be in electronic form (e.g. stored in a CD) or physical form (e.g. computer printouts). Examples of data include computerised attendance records of a school, information in the RAM of a computer, printouts of a computerised accounting system etc.

**Computer database** is a formalised representation of information. The term includes information produced by a computer and intended for use in a computer. This is best understood through the following illustration.

**Illustration:** Noodle School has an automated system for student administration. This system is powered by a database that contains detailed student information. One table of this database is titled “basic\_info” and contains the following categories of information.

Roll no.	Name	Address	Phone	Email

Another table is titled “student\_marks” and contains the following categories of information:

Roll no.	Test 1	Test 2	Test 3	Final

When a student’s report card is to be prepared, the system automatically takes the marks from the “student\_marks” table and the name and contact information from the “basic\_details” table. It then collates the information and prepares the final report card.

**Information** includes data, text, images, sound, voice, codes, computer programmes, software and databases or microfilm or computer generated micro fiche. Microfilms are processed sheets of plastic (similar to the commonly used photograph rolls) that carry images of documents. These images are usually about 25 times reduced from the original document size.

The images cannot be read by the naked eye and special readers are used to project the images on a screen. They are most commonly used in libraries for transmission, storage, reading and printing of books. Microfiche is a type of microfilm which carries several micro images.

**Illustration:** The following are information: (1) a photo stored on a DVD (2) a song stored on a CD (3) the eBook version of this book (4) a recording of a phone conversation.

**Removable storage medium** is a storage medium that retains the stored information even after it has been removed from a computer e.g. hard disks, floppies, USB disks, zip drives, CD, VCD, DVD. The RAM of a computer would not be removable storage medium as it loses all stored data as soon as it is removed from the host computer.

It is relevant to note section 81 of the *Information Technology Act*, which states-

**81. Act to have overriding effect. –**

**The provisions of this Act shall have effect notwithstanding anything consistent therewith contained in any other law for the time being in force.**



**Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 or the Patents Act, 1970.**

Sub-sections (aa), (ab), (ac) and (ad) of section 52 of the *Copyright Act* are relevant. They state-

**(aa) the making of copies or adaptation of a computer programme by the lawful possessor of a copy of such computer programme from such copy- (i) in order to utilise the computer programme for the purpose for which it was supplied; or (ii) to make back-up copies purely as a temporary protection against loss, destruction or damage in order only to utilise the computer programme for the purpose for which it was supplied;**

**(ab) the doing of any act necessary to obtain information essential for operating inter-operability of an independently created computer programme with other programmes by a lawful possessor of a computer programme provided that such information is not otherwise readily available;**

**(ac) the observation, study or test of functioning of the computer programme in order to determine the ideas and principles which underline any elements of the programme while performing such acts necessary for the functions for which the computer programme was supplied;**

**(ad) the making of copies or adaptation of the computer programme from a personally legally obtained copy for non-commercial personal use;**

Section 47 of the *Patent Act* is relevant. It states-

#### **Section 47 - Grant of patents to be subject to certain conditions**

**The grant of patent under this Act shall be subject to the condition that—**

**(1) any machine, apparatus or other article in respect of which the patent is granted or any article made by using a process in respect of which the patent is granted, may be imported or made by or on behalf of the Government for the purpose merely of its own use;**

**(2) any process in respect of which the patent is granted may be used by or on behalf of the Government for the purpose merely of its own use;**

**(3) any machine, apparatus or other article in respect of which the patent is granted or any article made by the use of the process in respect of which the patent is granted, may be made or used, and any process in respect of which the patent is granted may be used, by any person, for the purpose merely of experiment or research including the imparting of instructions to pupils; and**

**(4) in the case of a patent in respect of any medicine or drug, the medicine or drug may be imported by the Government for the purpose merely of its own use or for distribution in any dispensary, hospital or other medical institution maintained by or on behalf of the Government or any other dispensary, hospital or other medical institution which the Central Government may, having regard to the public service that such dispensary, hospital or medical institution renders, specify in this behalf by notification in the Official Gazette.**

**Compensation** is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim.

Simply put, damages are the compensation for legal injury. Damages can be of various types:

(1) Compensatory damages are allowed as a recompense for injury actually suffered.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

(2) Consequential damages are consequential upon the act complained of.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.

(3) Exemplary or punitive damages are awarded as a punishment and serve as a warning to others.

**Illustration:** Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

(4) General damages are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

**Illustration:** Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs 10 lakh as compensation.

# 4. Section 43(c) – Computer Virus, Worm, Contaminant

Unauthorised introduction of a virus etc into a computer is covered by section 43(c) of the Information Technology Act. This section states as under:

## **43. Penalty and compensation for damage to computer, computer system, etc.**

**If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,-  
(c) 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 to the person so affected.**

This section penalises two acts namely:

- (1) introducing a virus or contaminant into a computer,
- (2) causing the introduction of a virus or contaminant into a computer.

These acts may be directed towards a computer, a computer system or computer network. Let us discuss the important terms:

**Computer virus** means any computer instruction, information, data or programme that

- (1) destroys, damages, degrades or adversely affects the performance of a computer resource or
- (2) 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.

**Illustration:** The Love Bug virus comes as an attachment to an email with the subject “I Love You”. When a victim clicks on the attachment, the virus overwrites all files on the victim’s computer with junk data thereby destroying and damaging all the data.

**Illustration:** Macro viruses usually come embedded in Microsoft Word and Excel files. When a user runs the infected file, the macro virus gets activated and damages his data.

**Illustration:** The Chernobyl virus can lie dormant for the entire year in a victim’s computer. Most versions of the virus get activated only on April 26<sup>th</sup>. The virus, which was originally called CIH, is referred to as the Chernobyl Virus because it attacks on April 26<sup>th</sup> which is the date when the Chernobyl nuclear accident took place in Ukraine in 1986.

**Computer contaminant** means any set of computer instructions that are designed to

- (1) modify, destroy, record, transmit data or programme residing within a computer, or
- (2) usurp the normal operation of the computer.

**Illustration:** Sameer sends an online greeting card to Pooja. The greeting card is an image file that is infected with a “Computer Trojan”. When Pooja clicks on the greeting card to view it, the Trojan gets installed on her computer. The Trojan usurps the functioning of Pooja’s computer. It gives complete control of the computer to Sameer. He can now remotely alter files on Pooja’s computer. This is an example of a computer contaminant.

**Illustration:** Sameer installs a key logger on a cyber café computer. The key logger automatically records all text entered on the infected computer by users. Every evening at 5 pm the key logger transmits this recorded data to Sameer’s email account. This is an example of a computer contaminant.

**Compensation** is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim.

Simply put, damages are the compensation for legal injury. Damages can be of various types:

(1) **Compensatory damages** are allowed as a recompense for injury actually suffered.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

(2) **Consequential damages** are consequential upon the act complained of.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.

(3) **Exemplary or punitive damages** are awarded as a punishment and serve as a warning to others.

**Illustration:** Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

(4) **General damages** are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

**Illustration:** Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs 10 lakh as compensation.

# 5. Section 43(d) – Damaging a Computer

Unauthorised damage is covered by section 43(d) of the Information Technology Act. This section states as under:

## **43. Penalty and compensation for damage to computer, computer system, etc.**

**If any person without permission of the owner or any other person who is in charge of a 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 programmes residing in such computer, computer system or computer network;  
.....he shall be liable to pay damages by way of compensation to the person so affected.**

This section penalises two acts namely (1) damaging and (2) causing to be damaged. These acts may be directed towards a computer, a computer system, computer network, data, computer database or other programs.

Let us discuss the important terms:

**Data** is a formalised representation of information, knowledge, facts, concepts or instructions. Data undergoes processing by a computer. Data can be in electronic form (e.g. stored in a CD) or physical form (e.g. computer printouts). Examples of data include computerised attendance records of a school, information in the RAM of a computer, printouts of a computerised accounting system etc.

**Computer database** is a formalised representation of information. The term includes information produced by a computer and intended for use in a computer. This is best understood through the following illustration.

**Illustration:** Noodle School has an automated system for student administration. This system is powered by a database that contains detailed student information. One table of this database is titled “basic\_info” and contains the following categories of information.

Roll no.	Name	Address	Phone	Email

Another table is titled “student\_marks” and contains the following categories of information:

Roll no.	Test 1	Test 2	Test 3	Final

When a student’s report card is to be prepared, the system automatically takes the marks from the “student\_marks” table and the name and contact information from the “basic\_details” table. It then collates the information and prepares the final report card.

**Damage** for the purposes of this section implies to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

**Illustration:** Sameer deletes the “address column” of the “basic\_info” table of the Noodle School database from the illustration above. Now, although the final report card can be prepared, the address labels to courier the report cards cannot be prepared. Sameer has damaged the database.

**Illustration:** Sameer picks up Pooja’s laptop with the intention of stealing it. He then accidentally drops it on the floor, thereby destroying it. Sameer has damaged Pooja’s laptop.

**To cause** means to make something happen. Cause can be direct or indirect.

**Illustration:** Sameer pressed the “delete” button on the keyboard causing the data to be deleted. Sameer’s act of pressing the delete button is the direct cause of the data being deleted.

**Illustration:** Sameer switched off the power connection to the house, thereby causing the computer to switch off. Due to the sudden switch off, Pooja could not save her data and it was lost. Sameer’s act of switching off the power to the house was the indirect cause of the data loss. The unexpected switching off of the computer was the direct cause of the data loss.



Compensation is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim.

Simply put, damages are the compensation for legal injury. Damages can be of various types:

(1) Compensatory damages are allowed as a recompense for injury actually suffered.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

(2) Consequential damages are consequential upon the act complained of.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.

(3) Exemplary or punitive damages are awarded as a punishment and serve as a warning to others.

**Illustration:** Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

(4) General damages are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

**Illustration:** Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs 10 lakh as compensation.

# 6. Section 43(e) – Disruption of a Computer

Unauthorised disruption of a computer is covered by section 43(e) of the Information Technology Act. This section states as under:

**43. Penalty and compensation for damage to computer, computer system, etc.**

**If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,-  
(e) disrupts or causes disruption of any computer, computer system or computer network;  
.....he shall be liable to pay damages by way of compensation to the person so affected.**

This section penalises two acts namely (1) disrupting and (2) causing to be disrupted. These acts may be directed towards a computer, a computer system or computer network. Let us discuss the important terms:

Disrupting means “to prevent the normal continuance of”, “to throw into confusion or disorder”, “to interrupt or impede the progress of”. Disruption can be total or partial.

**Illustration:** Noodle Ltd has a large computer network that spans 3 continents. Noodle employees around the globe use the network to transfer important data. Sameer creates a computer worm that affects the Noodle network. The worm multiplies and replicates and clogs up all the resources thereby slowing the Noodle network. Sameer has partially disrupted the Noodle network.

**Illustration:** Sameer is an employee of the Pune office of Noodle Ltd. The office has a dozen computers connected to each other through a wireless access point. This access point creates a wireless network within the office. Sameer deliberately switches off the access point. The computers are no longer in a network. Sameer has totally disrupted the Noodle network.

**Illustration:** Sameer is an employee of the Mumbai office of Noodle Ltd. The office has a medium speed Internet connection. Sameer starts downloading several movies from the Internet simultaneously. This slows down the Internet speed available to the other Noodle employees. Sameer has partially disrupted the Noodle network.

Compensation is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim.

Simply put, damages are the compensation for legal injury. Damages can be of various types:

(1) Compensatory damages are allowed as a recompense for injury actually suffered.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

(2) Consequential damages are consequential upon the act complained of.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.

(3) Exemplary or punitive damages are awarded as a punishment and serve as a warning to others.

**Illustration:** Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

(4) General damages are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

**Illustration:** Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs 10 lakh as compensation.

# 7. Section 43(f) – Denial of Service

Denial of Service is covered by section 43(f) of the Information Technology Act. This section states as under:

## **43. Penalty and compensation for damage to computer, computer system, etc.**

**If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, - (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;**

**.....he shall be liable to pay damages by way of compensation to the person so affected.**

This section penalises two acts namely:

- (1) denying an authorised person access to a computer
- (2) causing the denial of access to an authorised person.

These acts may be directed towards a computer, a computer system or computer network. Let us discuss the important terms:

To deny access means “to restrict access” or “to disallow access”. This denial can be total or partial.

**Illustration:** Sameer is the network administrator of the Mumbai office of Noodle Ltd. He is disgruntled that his salary has not been raised. He disables the passwords of the other employees so they are unable to access the Noodle servers. Sameer has totally denied access to the authorised employees.

**Illustration:** Sameer has created a computer virus that opens up multiple program windows on a victim computer. This virus affects Pooja’s computer and opens up hundreds of program windows on her computer. This results in her computer becoming unusable. Sameer has caused total denial of access.

**Illustration:** A series of more than 125 separate but coordinated denial of service attacks hit the cyber infrastructure of Estonia in early 2007. It is suspected that the attacks were carried out by Russian hackers using sophisticated automated denial of service software. The software made millions of requests to Estonia Government servers. The servers could not handle so many requests and they crashed. This resulted in legitimate users being unable to access the servers. This is a total denial of access.

**Illustration:** Sameer is the network administrator of the Mumbai office of Noodle Ltd. He is disgruntled that his salary has not been raised. He shuts down one of the Noodle servers. Legitimate users are unable to access that server but can access the other servers. Sameer has caused a partial denial of access.

This section does not penalize instances where an unauthorised person is denied access to a computer.

**Illustration:** The senior management of Noodle Ltd is suspicious that Sameer is involved in corporate espionage and is selling confidential information to rival companies. They ask the Noodle network administrator to immediately block Sameer's access to the main servers.

Although Sameer has not been officially suspended or removed from his job, he cannot claim damages from Noodle Ltd for this denial of access. The computer systems belong to Noodle Ltd and the management can withdraw access permissions at any time and without giving prior notice.

Compensation is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim. Simply put, damages are the compensation for legal injury. Damages can be of various types:

(1) Compensatory damages are allowed as a recompense for injury actually suffered.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

(2) Consequential damages are consequential upon the act complained of.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.

(3) Exemplary or punitive damages are awarded as a punishment and serve as a warning to others.

**Illustration:** Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

(4) General damages are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

**Illustration:** Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs 10 lakh as compensation.

# 8. Section 43(g) – Facilitating Unauthorized Access

Providing assistance to facilitate illegal access is covered by section 43(g) of the Information Technology Act. This section states as under:

## **43. Penalty and compensation for damage to computer, computer system, etc.**

**If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, - (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; .....he shall be liable to pay damages by way of compensation to the person so affected.**

The essential element of this section is that assistance is provided for obtaining access to a computer in contravention of the IT Act and its allied laws. A person who obtains access to a computer in contravention of the IT Act would be liable under the relevant sections (e.g. 43(a) or 66 or 70 etc). What this section specifically covers is providing assistance to such a person. Such assistance must facilitate the unlawful access.

**Assistance** is the act of helping or aiding.

**Facilitate** means “to make easier” or “to make less difficult” or to “assist in the progress of”.

Let us consider some illustrations to understand this concept.

**Illustration:** Sameer is planning to gain unauthorised access into the computer systems of Noodle Bank Ltd. Aditi, the manager of Noodle, hands over a list of passwords to Sameer. Using these passwords, Sameer gains the unlawful access. Aditi has provided assistance to Sameer to facilitate his unlawful access.

**Illustration:** Sameer is planning to gain unauthorised access into the computer systems of Noodle Bank Ltd. Priyanka, the network security administrator of Noodle, is his good friend. She is monitoring the Intrusion Detection System (IDS) of Noodle at the time when Sameer is launching his attack. The IDS detects the attack and gives a warning. Priyanka deliberately ignores the warning and does not use any measures to stop the attack. Priyanka has provided assistance to Sameer to facilitate his unlawful access.

**Illustration:** Sameer is planning to gain unauthorised access into the computer systems of Noodle Bank Ltd. Priyanka, the network security administrator of Noodle, is his good friend. She disables the Noodle firewall at the time when Sameer is launching his attack. Priyanka has provided assistance to Sameer to facilitate his unlawful access.

Compensation is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim.

Simply put, damages are the compensation for legal injury. Damages can be of various types:

(1) Compensatory damages are allowed as a recompense for injury actually suffered.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

(2) Consequential damages are consequential upon the act complained of.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.



(3) Exemplary or punitive damages are awarded as a punishment and serve as a warning to others.

**Illustration:** Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

(4) General damages are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

**Illustration:** Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs 10 lakh as compensation.

# 9. Section 43(h) – Tampering or Manipulating Computer

Tampering or manipulating computer is covered by section 43(h) of the Information Technology Act. This section states as under:

**43. Penalty and compensation for damage to computer, computer system, etc.**

**If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, - (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network, .....he shall be liable to pay damages by way of compensation to the person so affected.**

An illustration to clarify the essential elements of this section is:

- (1) Sameer avails of some service e.g. purchases a software
- (2) Pooja's account with Noodle Bank is charged for this purchase
- (3) This has been done by Sameer's manipulation of the Noodle Bank computers

Let us discuss the key terms in this section.

**Tampering** implies “meddling so as to misuse”.

**Illustration:** Pooja has put a “BIOS” password on her computer. This means that as soon as her computer is switched on, it asks for a password. It does not boot up the operating system till this password is entered. Sameer removes the CMOS battery of Pooja's computer for a few minutes. He then puts the battery back and starts her computer. The “BIOS” password gets deleted and he is able to obtain unauthorised access to her computer. He has tampered with her computer.

**Illustration:** Noodle Ltd. has secured its computer network by configuring a firewall. Sameer places a powerful magnet near the computer on which the firewall is configured. Over a few days this magnet corrupts the hard disk and the firewall becomes ineffective. Sameer then remotely secures unauthorised access to the Noodle network. He has tampered with the Noodle computer.

**Manipulating** implies “influencing something skilfully in an unfair manner”.

**Illustration:** Pooja is checking her email account with gmail.com. As she is logged in to gmail, the gmail authentication cookie is present on her machine.

She receives an email from Sameer containing a really funny joke. The email contains a link to a site which promises her lots more jokes. She clicks on the link and is very happy with the site that opens up.

What she does not realize is that this joke site has forged a request to the gmail “Create Filter” wizard. This creates a filter that forwards a copy of all emails coming into Pooja’s account to Sameer!

Gmail accepts the request to create the filter because the genuine gmail account holder (Pooja) is authenticated and logged in at the moment and her session cookie is passed along with the forged request. Sameer has manipulated Pooja’s gmail account.

**Note:** This is a cross-site request forgery (CSRF) attack that transmits unauthorized commands to a website from a trusted user.

Now that we have understood the key terms, let us examine some scenarios where this section would be violated.

**Illustration:** Pooja regularly uses her computer to log into her online banking account with Noodle Bank. Sameer sends Pooja a spoofed email that appears to come from Noodle Bank. The email contains a link to what appears to be a Noodle Bank webpage. Pooja enters her login details on this webpage (which is actually a forged / phished webpage). Now Sameer has obtained her login information. He then purchases some software online and uses Pooja’s online bank account to pay for it. He will be liable under this section.

**Illustration:** Sameer is a hotel waiter. He secretly notes down credit card information of the hotel customers. He then purchases a software program from a website.

In order to pay for the purchase, he provides the credit card information of one of the hotel customers. This information is then passed on by the website to the payment gateway (e.g. Master, Visa etc.). The automated software at the gateway authenticates the transaction as the credit card information is correct. In reality, the gateway has been manipulated to allow a fraudulent transaction to go through.

**Illustration:** Noodle Ltd is a book selling company. Customers can place the orders via phone. They are also required to provide their credit card information on the phone. A Noodle employee enters the order details and the credit card information directly into the Noodle computer systems.

The order is then processed in due course. Sameer has designed the Noodle systems in such a way that every 17<sup>th</sup> payment is credited to “Nooodle” instead of “Noodle”. Suppose in a day there are 600 orders. Then the payment for the 17<sup>th</sup>, 34<sup>th</sup>, 51<sup>st</sup>, 68<sup>th</sup> ... order will be made to a company called “Nooodle” which is owned by Sameer.

In case of these orders the payment is not received by Noodle Ltd but the deliveries are made by them, so the customers never understand the fraud and do not lodge any complaint. Sameer has manipulated the Noodle systems.

Compensation is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim.

Simply put, damages are the compensation for legal injury. Damages can be of various types:

(1) Compensatory damages are allowed as a recompense for injury actually suffered.

**Illustration:** Sameer physically damages Pooja’s laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

(2) Consequential damages are consequential upon the act complained of.

**Illustration:** Sameer physically damages Pooja’s laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.

(3) Exemplary or punitive damages are awarded as a punishment and serve as a warning to others.

**Illustration:** Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

(4) General damages are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

**Illustration:** Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs 10 lakh as compensation.

# 10. Section 43(i) – Destruction, Deletion or Alteration

Unauthorised destruction, deletion or alteration of information is covered by section 43(i) of the Information Technology Act. This section states as under:

## **43. Penalty and compensation for damage to computer, computer system, etc.**

**If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,-  
(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;**

**.....he shall be liable to pay damages by way of compensation to the person so affected.**

The elements of this section are (1) destruction / deletion /alteration of information in a computer, or (2) diminishing value or utility of a computer resource, or (3) injuriously affecting a computer resource.

Let us discuss the relevant terms and issues in detail.

**Information** includes data, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche. Data is a formalised representation of information, knowledge, facts, concepts or instructions. Data undergoes processing by a computer. Data can be in electronic form (e.g. stored in a CD) or physical form (e.g. computer printouts). Examples of data include computerised attendance records of a school, information in the RAM of a computer, printouts of a computerised accounting system etc.

**Microfilms** are processed sheets of plastic (similar to the commonly used photograph rolls) that carry images of documents. These images are usually about 25 times reduced from the original. The images cannot be viewed by the naked eye and special readers are used to project the images on a screen. They are most commonly used in libraries for transmission, storage, reading and printing of books.

**Microfiche** is a type of microfilm containing several micro images.

**Illustration:** The following are information: (1) photos stored on a DVD (2) songs stored on a CD (3) the eBook version of this book (4) the recording of a phone conversation.

**Computer resource** includes computer, computer system, computer network, data, computer data base or software.

**Information residing in a computer resource** must be construed in a wide manner. It includes information that exists or is present in a computer resource temporarily or permanently. This is best discussed through the following illustrations.

**Illustration:** A personal computer has a BIOS chip that contains basic instructions needed to boot up a computer. These instructions are in the form of “information permanently residing” on the BIOS (which is a computer resource).

**Illustration:** Pooja is browsing a website. While she is viewing the website on her monitor, the information is cached in her computer in a folder specially reserved for temporary files. Some of that information is also stored in the RAM of her computer. When the computer is shutdown, the information in the RAM is lost. These are examples of information that is “temporarily residing” in a computer resource.

**Illustration:** Other illustrations of information residing in a computer resource are: (1) music files stored in an iPod (2) software installed on a computer (3) ebook stored on a CD (4) software installed in a cell phone (5) software embedded in a microwave oven.

**Destroy** means “to make useless”, “cause to cease to exist”, “nullify”, “to demolish”, or “reduce to nothing”.

**Destroying information** also includes acts that render the information useless for the purpose for which it had been created.

**Illustration:** Noodle Ltd has created a vast database of customer details and buying habits. The Noodle managers can query this database using a sophisticated “query management system”.

Sameer has developed this unique and path breaking “query management system” entirely on his own. One day, Sameer quits his job and takes the entire code of the “query management system” with him.

Now the information in the database is still intact but it is no longer usable for the purpose of predicting customer orders. Sameer has, in effect, destroyed the information contained in the database.

**Deletes** in relation to electronic information means “to remove”, “to erase”, “to make invisible” etc. Such deletion can be temporary or permanent.

**Illustration:** Pooja has created a text file containing her resume. Sameer deletes the file from her computer. On deletion, the file gets automatically transferred to the “recycle bin” of Pooja’s computer, from where it can be easily retrieved. Here Sameer has temporarily deleted the file. Sameer empties the “recycle bin” of Pooja’s computer. The file is still only temporarily deleted as it can be recovered using cyber forensics.

Sameer then uses specialised wiping software so that the file cannot be recovered using forensics. Now he has permanently deleted the file.

**Illustration:** Pooja is a novice computer user. She has created a text file containing her resume. Sameer changes the properties of the file and makes it a “hidden” file. Although the file still exists on Pooja’s computer, she can no longer see it. Sameer has deleted the file.

**Alters**, in relation to electronic information, means “modifies”, “changes”, “makes different” etc. This modification or change could be in respect to size, properties, format, value, utility etc. Alteration can be permanent or temporary. It can also be reversible or irreversible.



**Illustration:** Pooja has created a webpage for her client. A webpage is essentially an HTML (Hyper Text Markup Language) file. Sameer changes the file from HTML to text format. He has altered the file. This is a reversible alteration.

**Illustration:** Pooja has created a text file. Sameer changes the properties of the file and makes it a “hidden” file. The file retains its original content but it has been altered as its attributes have changed (it is now a hidden file). This is a reversible alteration.

**Illustration:** Pooja has created a text file named “pooja.txt”. Sameer changes the name of this file to “pooja1.txt”. Although the file retains its original content, it has been altered. This is a reversible alteration.

**Illustration:** Pooja is investigating Sameer’s computer for suspected cyber pornography. She seizes a word file that contains incriminating evidence against Sameer. As per procedure, she computes the hash value of the file and notes it in her report.

Sameer later manages to access the seized file and adds a “#” symbol to the contents of the file. The hash value of this altered file will be different from the hash value computed earlier by Pooja.

This is a permanent irreversible alteration. Even after the “#” symbol is removed, the hash value of the file will never be the same as the original computed by Pooja.

**Illustration:** Pooja is a graphics designer. She creates very high-resolution images for her clients. A high-resolution image can be magnified several times and still look clear.

Sameer is one of her employees. He changes some of the high-resolution images into low resolution images. Although the low-resolution images look the same as the high-resolution ones, they cannot be magnified. The value and utility of the images has been reduced. This is an example of permanent and irreversible alteration.

**Value** implies monetary worth.

**Illustration:** Pooja is a graphics designer. She buys a sophisticated computer for Rs 2 lakh. The value of the computer is Rs 2 lakh. She purchases one license of specialised graphics software for Rs 50,000 and installs the software on her computer. The value of the computer is now Rs 2.5 lakh. She then hires a specialist to configure her computer for optimal performance. The specialist charges her Rs 10,000 for his services. The value of the computer is now Rs 2.6 lakh.

**Utility** means “usefulness”.

**Illustration:** The utility of a high-resolution image lies in its ability to be magnified several times. This enables the image to be used for various purposes such as on a website, in a printed catalogue, on a large hoarding etc.

**Illustration:** The utility of anti-virus software lies in its ability to detect computer viruses and other malicious code.

**Illustration:** The utility of a sophisticated computer is its ability to render high resolution graphics files in a very short time.

**Diminish** means “reduce” or “lessen”,

**Illustration:** A computer worm replicates itself and thereby hogs up system resources such as hard disk space, bandwidth etc. This can diminish the performance and speed of the computer network.

**Diminishes value** means “reduces the monetary worth”.

**Illustration:** Pooja is a graphics designer. She creates very high-resolution images for her clients. A high-resolution image can be magnified several times and still look clear. She can sell each image for around Rs 5000.

Sameer is one of her employees. He changes some of the high-resolution images into low resolution images. Although the low-resolution images look the same as the high-resolution ones, they cannot be magnified. Now she cannot sell an image for more than Rs 400. Sameer has thus diminished the value of the images.

**Diminishes utility** means “reduces the usefulness”.

**Illustration:** Pooja has purchased a very sophisticated computer that has 2 GB RAM. This enables the computer to render a large image file in 3 seconds. Sameer steals 1 GB RAM from the computer. Now the computer takes more than 5 seconds to render the image file. Sameer's act of stealing the RAM has diminished the utility of Pooja's computer.

**Affects** means "influences" or "produces a change in".

**Illustration:** A computer virus changes the data stored in a computer. The virus affects the data.

**Injurious** means "harmful", "hurtful", or "detrimental".

**Illustration:** A computer virus is injurious to the data stored in a computer.

**Affects injuriously** means produces a "harmful or detrimental change".

**Illustration:** Placing a powerful magnet close to a floppy disk causes permanent and irreversible damage to the disk. We can say that the magnet affects the disk injuriously.

**Illustration:** Dropping a laptop on the floor can affect it injuriously.

**Illustration:** Dropping water on a laptop can affect it injuriously. Compensation is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim.

Simply put, damages are the compensation for legal injury. Damages can be of various types:

(1) Compensatory damages are allowed as a recompense for injury actually suffered.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

(2) Consequential damages are consequential upon the act complained of.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.

(3) Exemplary or punitive damages are awarded as a punishment and serve as a warning to others.

**Illustration:** Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

(4) General damages are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

**Illustration:** Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs 10 lakh as compensation.

# 11. Section 43(j) – Source Code Theft

Stealing, concealing, destroying or altering source code is covered by section 43(j) of the Information Technology Act. This section states as under:


**43. Penalty and compensation for damage to computer, computer system, etc.**

**If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, - (j) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage; .....he shall be liable to pay damages by way of compensation to the person so affected.**

Computer source code is the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. Computer source code need not only be in the electronic form. It can be printed on paper (e.g. printouts of flowcharts for designing a software application).

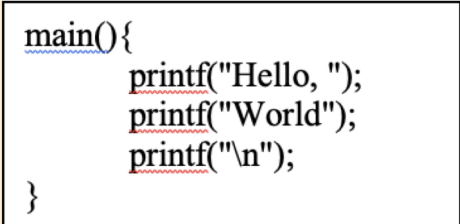
Let us understand this using some illustrations.

**Illustration:** Pooja has created a simple computer program. When a user double-clicks on the *hello.exe* file created by Pooja, the following small screen opens up:



Hello World

The *hello.exe* file created by Pooja is the executable file that she can give to others.



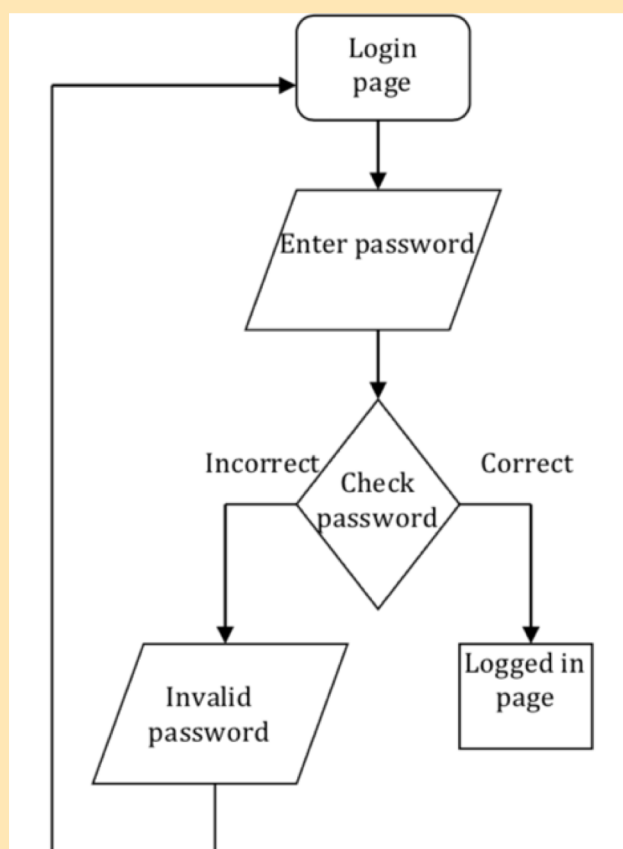
```
main(){  
    printf("Hello, ");  
    printf("World");  
    printf("\n");  
}
```

Stealing, concealing, destroying or altering source code is covered by section The small screen that opens up is the output of the software program written by Pooja. Pooja has created the executable file using the programming language called “C”. Using this programming language, she created the following lines of code:

These lines of code are referred to as the source code.

**Illustration:** Noodle Ltd has created software for viewing and creating image files. The programmers who developed this program used the computer-programming language called Visual C++. Using the syntax of these languages, they wrote thousands of lines of code. This code is then compiled into an executable file and given to end-users. All that the end user has to do is double-click on a file (called setup.exe) and the program gets installed on his computer. The lines of code are known as computer source code.

**Illustration:** Pooja is creating a simple website. A registered user of the website would have to enter the correct password to access the content of the website. She creates the following flowchart outlining the functioning of the authentication process of the website.



She takes a printout of the flowchart to discuss it with her client. The printout is source code.

The following acts are prohibited in respect of the source code (1) stealing, concealing, destroying or altering (2) causing another to steal, conceal, destroy or alter.

Let us discuss the relevant terms and issues in detail.

The term steal and “commit theft” are usually used interchangeably. Section 378 of the Indian Penal Code defines theft as “Whoever intending to take dishonestly any moveable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft.”

Section 303(1) of the Bharatiya Nyaya Sanhita is the corresponding section to “commit theft”.

**Illustration:** Pooja has created a software program. The source code files of the program are contained in a pen-drive. Sameer takes that pen-drive out of Pooja’s cupboard without informing her. He has “stolen” the source code.

*Conceal* simply means “to hide”.

**Illustration:** Pooja has created a software program. The source code files of the program are contained in a folder on Pooja’s laptop. Sameer changes the properties of the folder and makes it a “hidden” folder.

Although the source code folder still exists on Pooja’s computer, she can no longer see it. Sameer has concealed the source code.

*Destroy* means “to make useless”, “cause to cease to exist”, “nullify”, “to demolish”, or “reduce to nothing”.

*Destroying source code* also includes acts that render the source code useless for the purpose for which it had been created.

**Illustration:** Pooja has created a software program. The source code files of the program are contained in a folder on Pooja’s laptop. Sameer deletes the folder. He has destroyed the source code.

**Illustration:** Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer deletes one of the source code files. Now the source code cannot be compiled into the final product. He has destroyed the source code.

**Illustration:** Pooja is designing a software program. She draws out the flowchart depicting the outline of the functioning of the program. Sameer tears up the paper on which she had drawn the flowchart. Sameer has destroyed the source code.

*Alters*, in relation to source code, means "modifies", "changes", "makes different" etc. This modification or change could be in respect to size, properties, format, value, utility etc.

**Illustration:** Pooja has created a webpage for her client. The source code of the webpage is in HTML (Hyper Text Markup Language) format. Sameer changes the file from HTML to text format. He has altered the source code.

The inclusion of the words '*intention to cause damage*' under this section is to lay emphasis on the element of mens rea. Hence, in order to be held liable under section 43(j), it will have to be proved that the accused had the guilty intention of causing damage.

Compensation is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim.

Simply put, damages are the compensation for legal injury. Damages can be of various types:

(1) Compensatory damages are allowed as a recompense for injury actually suffered.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

(2) Consequential damages are consequential upon the act complained of.



**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.

(3) Exemplary or punitive damages are awarded as a punishment and serve as a warning to others.

**Illustration:** Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

(4) General damages are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

**Illustration:** Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs 10 lakh as compensation.

# **Shashank Shekhar Mishra Vs. Ajay Gupta**

IN THE HIGH COURT OF DELHI

CS (OS) No. 1144/2011

Decided On: 05.09.2011

Citation: 2011VIIIAD(Delhi)139, 184(2011)DLT675,  
ILR(2011)Supp.(4)Delhi612, 2011(48)PTC156(Del)

Shashank Shekhar Mishra (Plaintiff)

Vs.

Ajay Gupta (Defendant)

## **Background of Case:**

The said suit was filed for permanent injunction, rendition of accounts, delivery up of the infringing material and damages under section 43 of the IT Act.

## **Contention of Plaintiff:**

The Plaintiff claimed to be a tech savvy professional with vast experience in the field of web technologies including PHP, HTML, CSS, Java Script, Query, Word press, Photoshop etc. According to plaintiff, he is the author of "Quizpro Word press Plugin", using which the Word press users can easily use quiz on their Word press Blogs or Word press driven websites.

It is alleged that the Plaintiff purchased a laptop for Rs. 34,100/- and used it extensively for the purpose of web designing (creating, storing and retaining the original web designing templates, designs and styles) and processing various technology related activities on the internet. He was also storing various user IDs, passwords and other data in the laptop. Confidential financial information of the plaintiff including details of his mother's bank account as well as credit card information belonging to his cousin brother was stored in the laptop.

The Plaintiff claims to be the author of his original web designing templates, designs and styles, software, computer programme, software source code etc., the same being original "literary works" within the meaning of section 2(o) of Copyright Act, 1957.

The Plaintiff claims to have been very active on e-commerce website [www.algulfnet.biz](http://www.algulfnet.biz) and also claims to have got various accounts therein. [www.algulfnet.biz](http://www.algulfnet.biz) is a service driven website which offers people the opportunity to participate in surveys and earn online and also to purchase subscription for Surveys Online Today E-Zine.

The website works on the superstructure of ePins, wherein one pin is equivalent to Rs. 3600/- of actual commercial value. The website allows the user, who has generated a minimum specified number of points, to monetize those points and redeem them for actual money.

According to the Plaintiff, he had accumulated thousands of points in his various accounts by participating in various surveys conducted by [www.algulfnet.biz](http://www.algulfnet.biz) and had generated 212 ePins which are being displayed in his two accounts. Thus, these e-pins are virtual data and information in the electronic form, which are capable of being translated into physical money. The value of these 212 e-Pins is alleged to be Rs. 763200/-.

The case of the Plaintiff is that on 25th April, 2011, the Defendant who was known to him, barged into his room along with 2 anti-social elements and snatched away his laptop which contained confidential data including sensitive personal data, personally identifiable information, banking and credit card details as well as his 212 ePins. The Defendant also threatened to make public all photographs, messages etc. so as to tarnish the reputation of the plaintiff.

The Plaintiff sought injunction restraining the Defendant infringing his copyright. He also sought an injunction restraining the Defendant from downloading, extracting, distributing, transmitting, publishing, releasing or disclosing the personal, confidential data and information of the plaintiff. He has also sought injunction directing Defendant to handover the original laptop, CDs, inlay cards, hard disks etc. of the Plaintiff to him.

#### **Contention of Defendant:**

In this case even though the Defendant given notice of the said case being filed against him, he chose not to appear before the Court. Hence, the Court proceeded accordingly.

### **Points considered by Court:**

Though Section 43 of the IT Act provides for payment of damages by way of compensation in case of theft of a computer source Code with an intention to cause damage, for accessing or securing access to a computer or computer resource as well as destroying, deleting or altering any information stored in a computer resource, it does not provide for payment of damages for theft of data other than the computer source Code. Hence, the jurisdiction of a Civil Court is not excluded under Section 61 of the Act.

The Defendant has no right to use the computer programme authored by the Plaintiff or to make that work available to any other person. If the Defendant uses the work authored by the plaintiff or provides its copies to any person without license from the plaintiff, he would be infringing the copyright of the plaintiff.

The Plaintiff is entitled to injunction restraining the Defendant from infringing the copyright of the plaintiff in the literary work authored by him including the computer source Code of the Software Quizpro Word press plugin.

The Plaintiff must have suffered a lot of mental agony and anxiety on account of theft of the computer programme authored by him as well as all important data which was stored in the laptop. He would always remain apprehensive and live under a constant fear that the data which he had stored in the laptop may be misused either by the Defendant or any other person who is able to have access to it, causing substantial financial loss to him besides mental trauma, agony and anxiety, which he is beyond to suffer in case that data is used.

The right to privacy has been recognized as a valuable right of an individual which is implicit in his right to life and liberty which is guaranteed by Article 21 of the Constitution. The right of privacy affords protection of personal intimacies of family, marriage, friendship and other matters which are of a private nature. It is a right to be let alone and everyone is entitled to safeguard his privacy. No one has a right to peep into the private life of another person without his consent and if he does so he would be violating the right to privacy and would be liable to pay damages in an action under the law of torts.

**Conclusion of Court:**

A decree for permanent injunction was passed restraining the Defendant from infringing the copyright of the Plaintiff in the "literary works" authored by him. He was also restrained from disclosing the information of the Defendant and also from using it in any manner whatsoever.

A decree for recovery of laptop was passed or in the alternative for recovery of Rs. 34,100/- was also passed in favour of the Plaintiff.

A decree for damages amounting to Rs. 10 lakh was also passed in favour of the Plaintiff. The plaintiff was also be entitled to pendente lite (pending litigation) and future damages @ 6% p.a. on the aforesaid amount of Rs. 10 lakh, in addition to proportionate costs of the suit.

# 12. Section 43A – Failure to Protect Data

Compensation for failure to protect data is covered by section 43A of the Information Technology Act. This section states as under:

## **43 A. Compensation for failure to protect data**

**Where a body corporate, 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 of compensation to the person so affected.**

**Explanation – For the purposes of this section,-**

**(i) “body corporate” means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;**

**(ii) “reasonable security practices and procedures” means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;**

**(iii) “sensitive personal data or information” means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.**

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 have been made under this section. They came into force on 11th April 2011.

According to these rules, sensitive personal data or information of a person means such personal information which consists of information relating to; —

- (i) password;
- (ii) financial information such as Bank account or credit card or debit card or other payment instrument details;
- (iii) physical, physiological and mental health condition;
- (iv) sexual orientation;
- (v) medical records and history;
- (vi) Biometric information;
- (vii) any detail relating to the above clauses as provided to body corporate for providing service; and
- (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

The following information is not regarded as sensitive personal data or information:

- (1) any information that is freely available or accessible in public domain
- (2) any information that is furnished under the Right to Information Act, 2005 or any other law for the time being in force

The data privacy rules lay down several provisions for:

- (1) A privacy policy including:
  - (A) clear and easily accessible statements of its practices and policies;
  - (B) type of personal or sensitive personal data or information collected under rule;
  - (C) purpose of collection and usage of such information;
  - (D) disclosure of information including sensitive personal data or information under rule 6;
  - (E) reasonable security practices and procedures as provided under rule 8
- (2) Collection of information
- (3) Disclosure of information

(4) Transfer of information

(5) Reasonable Security Practices and Procedures

In 2018, the Personal Data Protection Bill has been introduced in India. In an era when India is heading towards becoming a digital economy, a robust data protection law is the need of the hour.

### **Right to Privacy under the Constitution of India**

An interesting question arose before the Andhra Pradesh High Court in the case of Rayala M. Bhuvaneshwari vs. Nagaphanender Rayala.

The parties in this case had filed for divorce before a Family Court and the husband had filed an application before the said Family Court wherein he contended that he should be allowed to produce a hard disc for the purpose of evidence relating to certain conversations of his wife.

The husband contended that his wife had admitted the voice while she was being cross-examined in the Family Court but she had denied some portions of the conversation. Because of her denial of certain portions, the husband wanted the hard disk to be sent to an expert to check if there was any alteration, insertion or addition in the conversation.

The Family Court allowed the request of the husband. The wife, aggrieved by the order of the Family Court approached the Andhra Pradesh High Court. The said High Court ruled in favour of the wife and held the following:

The husband does not derive any power whatsoever to record a telephonic conversation of his wife without her knowledge.

The right to privacy by itself has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. But the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "right to privacy". Conversations on the telephone are often of an intimate and confidential character.

Right of Privacy is an essential component of right to life envisaged by Article 21.



The act of tapping itself by the husband of the conversation of his wife with others was illegal and it infringed the right of privacy of the wife. Therefore, the tapes, even if true, cannot be admissible in evidence.

Compensation is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim.

Simply put, damages are the compensation for legal injury. Damages can be of various types:

(1) Compensatory damages are allowed as a recompense for injury actually suffered.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

(2) Consequential damages are consequential upon the act complained of.

**Illustration:** Sameer physically damages Pooja's laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.

(3) Exemplary or punitive damages are awarded as a punishment and serve as a warning to others.

**Illustration:** Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

(4) General damages are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

**Illustration:** Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs 10 lakh as compensation.

Non-compliance with any of the provisions of the data privacy rules is also penalized with a compensation /penalty of upto Rs. 25,000 under section 45 of the Information Technology Act. This section is as under:

**45. Residuary penalty.**

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

# 13. Section 63 – Compounding of Contraventions

In Concise Oxford Dictionary in Law, the meaning for the word “compound” is given as: (a) condone a liability or offence in exchange for money etc., (b) forbear from prosecuting (a felony) from private motives, and Law come to terms with a person, for foregoing a claim etc., for an offence.

For the expression “Compounding” in Ramanathan Aiyar's Law Lexicon, is “Arranging, coming to terms, condone for money; arranging with the creditor to his satisfaction.” Section 63 provides for compounding of any contravention under the IT Act. Ingredients of section 63 are as below:

Any contravention under IT Act, either before or after the adjudication proceedings, may be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer subject to any conditions that they may specify.

The sum compounded should not exceed the maximum amount of the penalty which may be imposed under the IT Act for the contravention.

Provisions relating to compounding shall not apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

Where any contravention has been compounded, no proceeding or further proceeding, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

# 14. Section 65 – Tampering with Computer Source Documents

Tampering with computer source documents is covered by section 65 of the Information Technology Act. This section states 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.**

Computer source code is the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. Computer source code need not only be in the electronic form. It can be printed on paper (e.g. printouts of flowcharts for designing a software application). Let us understand this using some illustrations.

**Illustration:** Pooja has created a simple computer program. When a user double-clicks on the hello.exe file created by Pooja, the following small screen opens up:



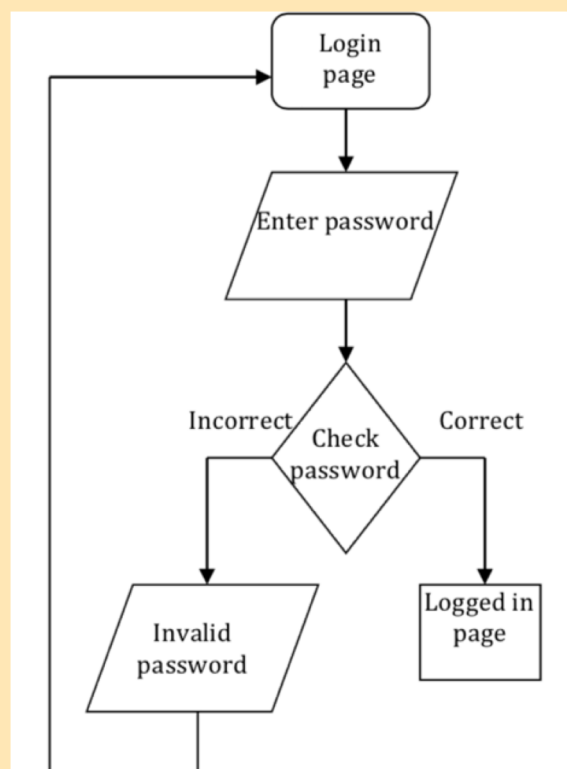
Hello World

The hello.exe file created by Pooja is the executable file that she can give to others. The small screen that opens up is the output of the software program written by Pooja. Pooja has created the executable file using the programming language called "C". Using this programming language, she created the following lines of code:

```
main()
{
    printf("Hello, ");
    printf("World");
}
```

These lines of code are referred to as the source code.

**Illustration:** Noodle Ltd has created software for viewing and creating image files. The programmers who developed this program used the computer-programming language called Visual C++. Using the syntax of these languages, they wrote thousands of lines of code. This code is then compiled into an executable file and given to end-users. All that the end user has to do is double-click on a file (called setup.exe) and the program gets installed on his computer. The lines of code are known as computer source code.



**Illustration:** Pooja is creating a simple website. A registered user of the website would have to enter the correct password to access the content of the website. She creates the following flowchart outlining the functioning of the authentication process of the website. She takes a printout of the flowchart to discuss it with her client. The printout is source code.

This section relates to computer source code that is either: required to be kept (e.g. in a cell phone, hard disk, server etc), or required to be maintained by law.

The following acts are prohibited in respect of the source code

1. knowingly concealing or destroying or altering
2. intentionally concealing or destroying or altering
3. knowingly causing another to conceal or destroy or alter
4. intentionally causing another to conceal or destroy or alter.

Let us discuss the relevant terms and issues in detail.

*Conceal* simply means “to hide”.

**Illustration:** Pooja has created a software program. The source code files of the program are contained in a folder on Pooja’s laptop. Sameer changes the properties of the folder and makes it a “hidden” folder. Although the source code folder still exists on Pooja’s computer, she can no longer see it. Sameer has concealed the source code.

*Destroy* means “to make useless”, “cause to cease to exist”, “nullify”, “to demolish”, or “reduce to nothing”.

Destroying source code also includes acts that render the source code useless for the purpose for which it had been created.

**Illustration:** Pooja has created a software program. The source code files of the program are contained in a folder on Pooja’s laptop. Sameer deletes the folder. He has destroyed the source code.

**Illustration:** Pooja has created a software program. The source code files of the program are contained in a folder on Pooja’s laptop. Sameer deletes one of the source code files. Now the source code cannot be compiled into the final product. He has destroyed the source code.

**Illustration:** Pooja is designing a software program. She draws out the flowchart depicting the outline of the functioning of the program. Sameer tears up the paper on which she had drawn the flowchart. Sameer has destroyed the source code.

Alters, in relation to source code, means “modifies”, “changes”, “makes different” etc. This modification or change could be in respect to size, properties, format, value, utility etc.

**Illustration:** Pooja has created a webpage for her client. The source code of the webpage is in HTML (Hyper Text Markup Language) format. Sameer changes the file from HTML to text format. He has altered the source code.

## **CASE LAW:**

Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh & Anr.  
[2005CriLJ4314]

### **Summary of the case:**

Tata Indicom employees were arrested for manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm. The court held that such manipulation amounted to tampering with computer source code as envisaged by section 65 of the Information Technology Act, 2000.

### **Background of the case:**

Reliance Infocomm launched a scheme under which a cell phone subscriber was given a digital handset worth Rs. 10,500 as well as service bundle for 3 years with an initial payment of Rs. 3350 and monthly outflow of Rs. 600. The subscriber was also provided a 1-year warranty and 3 year insurance on the handset.

The condition was that the handset was technologically locked so that it would only work with the Reliance Infocomm services. If the customer wanted to leave Reliance services, he would have to pay some charges including the true price of the handset. Since the handset was of a high quality, the market response to the scheme was phenomenal.

Unidentified persons contacted Reliance customers with an offer to change to a lower priced Tata Indicom scheme. As part of the deal, their phone would be technologically “unlocked” so that the exclusive Reliance handsets could be used for the Tata Indicom service.

Reliance officials came to know about this “unlocking” by Tata employees and lodged a First Information Report (FIR) under various provisions of the Indian Penal Code, Information Technology Act and the Copyright Act.

The police then raided some offices of Tata Indicom in Andhra Pradesh and arrested a few Tata Teleservices Limited officials for re-programming the Reliance handsets.



These arrested persons approached the High Court requesting the court to quash the FIR on the grounds that their acts did not violate the said legal provisions.

### **Issues raised by the Defence:**

(1) Subscribers always had an option to change from one service provider to another.

(2) The subscriber who wants to change from Tata Indicom always takes his handset, to other service providers to get service connected and to give up Tata services.

(3) The handsets brought to Tata by Reliance subscribers are capable of accommodating two separate lines and can be activated on principal assignment mobile (NAM 1 or NAM 2). The mere activation of NAM 1 or NAM 2 by Tata in relation to a handset brought to it by a Reliance subscriber does not amount to any crime.

(4) A telephone handset is neither a computer nor a computer system containing a computer programme.

(5) There is no law in force which requires the maintenance of "computer source code". Hence section 65 of the Information Technology Act does not apply.

### **Findings of the court**

(1) As per section 2 of the Information Technology Act, any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.

(2) The instructions or programme given to computer in a language known to the computer are not seen by the users of the computer/consumers of computer functions. This is known as source code in computer parlance.

(3) A city can be divided into several cells. A person using a phone in one cell will be plugged to the central transmitter of the telecom provider. This central transmitter will receive the signals and then divert them to the relevant phones.

(4) When the person moves from one cell to another cell in the same city, the system i.e., Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower.

(5) All cell phone service providers have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider.

(6) System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Every cell phone operator is required to obtain SID from the Government of India. SID is programmed into a phone when one purchases a service plan and has the phone activated.

(7) Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. ESN is a permanent part of the phone.

(8) Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. MIN is programmed into a phone when one purchases a service plan.

(9) When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing.

(10) If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range.

(11) When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in a database, knows which cell phone you are using and gives a ring.

(12) So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the outgoing audio signals and incoming signals.

(13) This is a micro processor similar to the one generally used in the compact disk of a desktop computer. Without the circuit board, cell phone instrument cannot function.

(14) When a Reliance customer opts for its services, the MIN and SID are programmed into the handset. If someone manipulates and alters ESN, handsets which are exclusively used by them become usable by other service providers like TATA Indicom.

### **Conclusions of the court**

(1) A cell phone is a computer as envisaged under the Information Technology Act.

(2) ESN and SID come within the definition of "computer source code" under section 65 of the Information Technology Act.

(3) When ESN is altered, the offence under Section 65 of Information Technology Act is attracted because every service provider has to maintain its own SID code and also give a customer specific number to each instrument used to avail the services provided.

(4) Whether a cell phone operator is maintaining computer source code, is a matter of evidence.

(5) In Section 65 of Information Technology Act the disjunctive word "or" is used in between the two phrases – (a) "when the computer source code is required to be kept" (b) "maintained by law for the time being in force".

# 15. Section 66 – Computer Related Offences

Computer related offences are covered by section 66 of the Information Technology Act. This section states as under:

## **66. Computer related offences.**

**If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.**

**Explanation – For the purposes of this section, -**

**(a) the word “dishonestly” shall have the meaning assigned to it in section 24 of the Indian Penal Code;**

**(b) the word “fraudulently” shall have the meaning assigned to it in section 25 of the Indian Penal Code.**

Section 2(7) and section 2(9) of the Bharatiya Nyaya Sanhita are the corresponding sections which talk about “dishonestly” and “fraudulently” respectively.

The acts referred to in section 43 of the *Information Technology Act* are:

(a) accessing or securing access to a computer, computer system, computer network or computer resource without the permission of the owner or person in-charge;

(b) downloading, copying or extracting any data, computer data base or information from a computer, computer system or computer network or removable storage medium without the permission of the owner or person in-charge;

(c) introducing or caused to be introduced any computer contaminant or computer virus into any computer, computer system or computer network without the permission of the owner or person in-charge;

(d) damaging or causing to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network without the permission of the owner or person in-charge;

(e) disrupting or causing disruption of any computer, computer system or computer network;

(f) denying or causing the denial of access to any person authorised to access any computer, computer system or computer network by any means without the permission of the owner or person in-charge;

(g) providing 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 without the permission of the owner or person in-charge;

(h) charging the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network without the permission of the owner or person in-charge;

(i) destroying, deleting or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously by any means without the permission of the owner or person in-charge;

(j) stealing, concealing, destroying or altering or causing any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage without the permission of the owner or person in-charge;

Section 24 of *Indian Penal Code* states-

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

Section 25 of *Indian Penal Code* states-

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

Another relevant provision is Section 23 of *Indian Penal Code* which defines some of the words discussed above, as under:

**"Wrongful gain" is gain by unlawful means of property to which the person gaining is not legally entitled.**

**"Wrongful loss".--"Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled.**

Gaining wrongfully, losing wrongfully. - A person is said to gain wrongfully when such person retains wrongfully, as well as when such person acquires wrongfully. A person is said to lose wrongfully when such person is wrongfully kept out of any property, as well as when such person is wrongfully deprived of property.

Section 2(7) of Bharatiya Nyaya Sanhita is the corresponding section which talks about "dishonestly"

Section 2(9) of Bharatiya Nyaya Sanhita is the corresponding section which talks about "fraudulently"

Section 2(36) and 2(37) of Bharatiya Nyaya Sanhita is the corresponding section which talks about "wrongful gain" and "wrongful loss" respectively.

# **Amit Dilip Patwardhan vs. Rud India Chains Pvt. Ltd. & Ors.**

IN THE OFFICE OF THE ADJUDICATING OFFICER  
RAJESH AGGARWAL, SECRETARY, (INFORMATION TECHNOLOGY),  
GOVERNMENT OF MAHARASHTRA  
Complaint no. 1 of 2013 dt 16/01/2013

**Amit Dilip Patwardhan (Complainant)**

**vs.**

**Rud India Chains Pvt. Ltd. & Ors. (Respondent)**

## **Background of Case:**

The Complainant was an employee of Respondent No. 1 i.e. Rud India Chains Pvt. Ltd. from April 2008 to March 2012. Later, he left the company to join a rival company, Heko Chains. The Respondent claims that the Complainant took away company secrets and was receiving gratification from Heko Chains to lure away their customers even while he was employed with them. Rud India Chains Pvt. Ltd. had already filed a civil suit for damages for theft of trade secrets. The Complainant had approached the Adjudicating Officer claiming that his bank statement was filed as evidence in the court by the Respondent and the said bank statement was obtained by hacking into the bank system. Hence, relief was sought under IT Act.

## **Contention of Complainant:**

The Respondents had no authority to get his bank statement and have committed offence under sections 43(b) and 66 of the IT Act.

## **Contention of Respondent:**

The Respondent claims that the Complainant took away company secrets and was receiving gratification from Heko Chains to lure away their customers even while he was employed with them.

**Points considered by Court:**

The Adjudicating Officer observed that the content of the bank statement filed before the police match with the Complainant's bank account data but the format is not the standard format in which the bank gives a print out.

The bank policy is not to give the detailed bank statement to anybody without the approval of the customer. Hence, the bank has no knowledge about how the Respondent obtained the bank statement of their ex-employee.

The Respondents have not explained how they got the statement. The bank has denied that the statement was given to the Respondents by them and hence the only possibility is that the Respondents hacked into the computer systems or got someone in the bank to give it to them by inducement, or pretending to be a customer, or employed a private eye to do it for them.

**Conclusion of Court:**

The Respondents have violated the privacy of the Complainant and accessed his personal sensitive data through dubious means. They had no right to the bank details of their ex-employee. The bank statement had not been obtained from physical records kept by the bank but from electronic records. Hence, the Respondents were guilty of violating section 43(b) of IT Act read with section 66.

Since the Complainant had not come to the forum with clean hands either (i.e. prima facie it showed that he was disloyal to his employer), the Adjudicating Officer did not impose any punishment on the Respondents but held them guilty of violating the privacy of the Complainant.



# 16. Section 66A – Sending Offensive Messages

The Supreme Court of India in *Shreya Singhal vs U.O.I* on 24 March, 2015 declared "Section 66A of the Information Technology Act, 2000 is struck down in its entirety being violative of Article 19(1)(a) and not saved under Article 19(2)".

Section 66A of the Information Technology Act (IT Act) was much debated (and hated) primarily because it was seen as being against "freedom of speech" and also because it used "vague" words like grossly offensive, menacing character etc.

This section was not part of the original IT Act that came into force in 2000. It was added in 2009.

In the last few years, this section was used in many controversial cases including the April 2012 arrest of a Chemistry professor at Jadavpur University for forwarding a cartoon featuring the West Bengal CM Mamata Banerjee.

A month later, two Air India cabin crew members were arrested and jailed for 12 days for posting "derogatory" remarks against the Prime Minister's Office, the national flag and the Supreme Court, while commenting on a strike by Air India pilots.

Later that year, two girls were arrested over a Facebook post questioning the shutdown in Mumbai for Shiv Sena patriarch Bal Thackeray's funeral. This arrest led a nation-wide protest and prompted a law student to file a public interest litigation challenging the constitutional validity of section 66A.

On 9th January, 2013, the Central Government issued an advisory to the effect that an arrest under section 66A must be first approved by an officer of the rank of the Inspector General, Deputy Commissioner or Superintendent of Police.

On 24th March, 2015, the Supreme Court, in a 122-page judgement, struck down section 66A in its entirety for violating the fundamental right of speech and expression.

# 17. Section 66B – Dishonestly Receiving Stolen Computer

Punishment for dishonestly receiving stolen computer resource or communication device is covered by section 66b of the Information Technology Act. This section states as under:

## **66B. Punishment for dishonestly receiving stolen computer resource or communication device**

**Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.**

This section addresses the issue of dishonestly receiving stolen computer resource or communication device. This section applies to a person who dishonestly receives or retains

(1) any stolen computer resource (computer, computer system, computer network, data, computer data base or software), or

(2) any stolen communication device (cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image).

Section 24 of *Indian Penal Code* states- **Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly"**. This section applies only if the person knows or has reason to believe that the computer resource or communication device is stolen.

Section 2(7) of Bharatiya Nyaya Sanhita is the corresponding section which talks about “dishonestly”

**Illustration:** Sameer has been arrested several times in the past for offences relating to theft. One day, he approaches Parag with 15 cell phones and offers to sell them for half their market value. Parag buys the cell phones from Sameer and then sells them in his shop for the full market value. Parag would be liable under this section.

# 18. Section 66C – Identity Theft

Identity theft is covered by section 66C of the Information Technology Act. This section states as under:

## **66C. Punishment for identity theft.**

**Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.**

This section penalises identity theft. This section applies to cases where someone who dishonestly or fraudulently does the following: (1) makes use of the electronic signature of any other person, or (2) makes use of the password of any other person, or (3) makes use of any other unique identification feature of any other person.

**Illustration:** Sameer is a junior employee in a bank. He oversees his senior Pooja typing her password into her official computer. One day, Sameer logs into the banks system using Pooja’s password and transfers some money into his account. He will be liable under this section.

Section 24 of *Indian Penal Code* states- **Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".**

Section 25 of *Indian Penal Code* states- **A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.**

Section 2(7) of *Bharatiya Nyaya Sanhita* is the corresponding section which talks about “dishonestly”

Section 2(9) of *Bharatiya Nyaya Sanhita* is the corresponding section which talks about “fraudulently”

# 19. Section 66D – Cheating by Personation

Cheating by personation is covered by section 66D of the Information Technology Act. This section states as under:

## **66D. Punishment for cheating by personation by using computer resource**

**Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.**

The term “cheating” is defined in section 415 of the *Indian Penal Code*, which states:

**Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".**

**Explanation: A dishonest concealment of facts is a deception within the meaning of this section.**

The term “cheating by personation” is defined in section 416 of the *Indian Penal Code*, which states:

**A person is said to "cheat by personation" if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.**

**Explanation: The offence is committed whether the individual personated is a real or imaginary person.**

Section 318(1) of Bharatiya Nyaya Sanhita is the corresponding section which talks about “cheating”.

Section 319(1) of Bharatiya Nyaya Sanhita is the corresponding section which talks about “cheating by personation”.

**Illustration:** Pooja receives an email that appears to have been sent from her bank. The email urges her to click on the link in the email. When she does so, she is taken to “a secure page on the bank’s website”.

She believes the web page to be authentic and enters her username, password and other information. In reality, the website is a fake and Pooja’s information is stolen and misused. The fake email and fake website had been created by Sameer. He would be liable under this section.

## Phishing

One of the first decisions on phishing was passed by the Delhi High Court in the case of NASSCOM vs. Ajay Sood.

In this case, fraudulent e-mails purportedly originating from the plaintiff were sent using the trade mark 'NASSCOM'. Because NASSCOM is a well-known name in India, the defendants portrayed themselves as NASSCOM to obtain personal data from various addresses which they could then use for head-hunting.

Although the Court did not cite section 66D of the IT Act, the Court explained the concept of phishing as below:

*'Phishing' is a form of internet fraud. In a case of 'Phishing', a person pretending to be a legitimate association such as a bank or an insurance company in order to extract personal data from a user such as access codes, passwords etc. which are then used to his own advantage, misrepresents on the identity of the legitimate party.*

The Court stated that at present there is no legislation in India on 'phishing'. An act which amounts to phishing under the Indian law would be a misrepresentation as it would lead to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer, but even the person whose name, identity or password is misused. The Court in this case granted an injunction in favour of the plaintiff and the defendants were ordered to refrain from circulating fraudulent emails.



# 20. Section 66E – Violation of Privacy

Violation of privacy is covered by section 66E of the Information Technology Act. This section states as under:

## **66E. Punishment for violation of privacy.**

**Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.**

**Explanation – For the purposes of this section –**

**(a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;**

**(b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means;**

**(c) “private area” means the naked or undergarment clad genitals, public area, buttocks or female breast;**

**(d) “publishes” means reproduction in the printed or electronic form and making it available for public;**

**(e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that –**

**(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or**

**(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.**

This section penalizes intentionally or knowingly doing the following in respect of the image of a private area of any person without consent: (1) capturing, or (2) publishing, or (3) transmitting. The above is penalized if it is done under circumstances violating the privacy of that person.

**Illustration:** Pooja is trying out a new dress in the changing room of a clothing store. Sameer, an employee of the store has hidden a camera that records Pooja while she is changing her clothes. Sameer will be liable under this section.

**Illustration:** Pooja is a model for a company selling ladies undergarments. As part of her modelling assignment, she poses in underwear. Siddharth is the photographer for that assignment. He takes several photographs of Pooja while she is wearing the underwear. Siddharth will not be liable under this section.

# **The State (Cyber Cell) vs. Yogesh Pandurang Prabhu**

IN THE COURT OF ADDL. CHIEF METROPOLITAN MAGISTRATE, 37TH COURT,  
ESPLANADE, MUMBAI

C.C. NO. 3700686/PS/2009

The State (Cyber Cell) ...Complainant

Vs.

Yogesh Pandurang Prabhu ...Accused

## **Background of Case:**

The victim, Sonali Sawai lodged a report in Cyber Cell, Mumbai. The victim had an orkut profile where she came in contact with the accused and they became friends. When they met, the victim did not like his nature after which she unfriended him.

On 03/03/2009 the victim received one email from an unknown email address. The email contained vulgar comments on her, however she neglected the same. She received similar emails on 05/03/2009, 06/03/2009 and 08/03/2009.

These emails contained nude photographs, pornographic postures, etc. The emails explicitly described the private parts of the victim and the accused expressed his desire to have sexual intercourse with the victim. Thereafter, Sonali filed a complaint with the Cyber Cell.

On inquiry it was found that the emails were received from 15 IP addresses of Airtel and Reliance company. The physical address of the first 12 IP addresses matched with the work place of the accused. The crime was registered under section 509 of Indian Penal Code and under IT Act.

**Contention of Complainant:**

The accused had made her fake profile on the internet after which she started receiving calls from taxi drivers and rickshaw drivers demanding sex in view of emails received by them. She further claimed that obscene emails and pictures were sent from same IP address through the laptop of accused which was provided to him by company.

**Points considered by Court:**

The investigating machinery after making inquiries and technical investigation concluded towards the guilt of the accused. The Investigating Officer further carried out technical investigation like seizure of harddisk from which the disputed the emails were sent, which further confirmed traces of the disputed emails found in it.

**Conclusion of the court:**

The evidence gathered showed that accused intentionally and knowingly violated the privacy of victim which attracts provisions of section 66E of IT Act along with section 509 of Indian Penal Code.

Accused was sentenced to simple imprisonment for 3 months for offence punishable under section 66(E) of IT Act and a fine of Rs. 10,000/ was imposed.

# 21. Section 66F – Cyber Terrorism

Cyber Terrorism is covered by section 66F of the Information Technology Act. This section states as under:

## **66F. Punishment for cyber terrorism.**

**(1) Whoever, -**

**(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by -**

**(i) denying or cause the denial of access to any person authorised to access computer resource; or**

**(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or**

**(iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or**

**(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.**

**(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.**

# **Mehid Masroor Biswas vs. State of Karnataka**

**IN THE HIGH COURT OF KARNATAKA**

**Criminal Petition No. 4039 of 2016**

**Mehid Masroor Biswas (Petitioner)**

**vs.**

**State of Karnataka (Respondent)**

## **Background of Case:**

The petitioner was a B.Tech graduate in the field of Electronic Engineering and was working with ITC, Bangalore. He was a follower of Sunni set of Islam.

The police received information on 12th December 2014 that the petitioner was the brain behind a twitter handle namely "@shamiwitness" which was sympathetic to the cause Islamic State of Iraq and Syria (ISIS) and was working towards motivating and the fighters.

A case was registered by Gangamma Gudi Police Station, Bangalore City against the petitioner for the offences punishable under Section 66(F) of Information Technology Act, 2000, under Section 125 of the Indian Penal Code and under Sections 18, 13, 39 of Unlawful Activities (Prevention) Act, 1967. The petitioner was arrested on 14th December 2014 and was in judicial custody since then.

The petitioner had filed the said case for grant of bail.

## **Contention of Petitioner:**

ISIS had been banned by Government of India with effect from 16th February 2015, whereas, the petitioner was arrested for the said offence on 14th December 2014, that is to say much before the activities of ISIS was banned and hence, it cannot be termed as an offence.

The case of the prosecution that the petitioner involved in the offence to wage war against the State, cannot be accepted. Waging war against the State or the Society could be attributed against fleet of persons who are working with weapons against the State. He submitted that the petitioner is a law-abiding citizen and is also an Engineering graduate and under these circumstances, he has to be extended the benefit of bail.

The allegation made against the petitioner does not satisfy the allegation of Cyber terrorism and the petitioner has not used any cyber weapons like radio frequency, electromagnetic bomb or computer viruses, etc. There are no allegations as to the fact that the petitioner has sent viruses and delivered to any computer, or of having hacked into any computer, password protected the information system and then deleted all data.

### **Contention of Respondent:**

The petitioner successfully masked his identity for a long time and tweeted to promote and support the claim of the terrorist organization, ISIS from January 2013 until he was exposed by Chanel-4 of Britain on 12th December 2014. He had sent thousands of messages, posted pictures, photos and videos glorifying the Islamic Caliphate and implementation of Sharia by overthrowing legitimate rulers of various countries including Iraq and Syria.

ISIS is a banned organization listed in the schedule to the United Nations Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007 made under Section 2 of the United Nations (Security Council) Act, 1947. The Government of India had officially banned ISIS under the Unlawful Activities (Prevention) Act and a Notification was also issued to that effect by the Ministry of Home Affairs.

Petitioner's twitter handle "@shamiwitness" was one of the popular handles for ISIS sympathizers. By using the said twitter handle, the petitioner spoke to British Jihadis regularly before they left to join ISIS and and if they died, he praised them as 'martyrs'. Thousands of updates were being posted to the account every month usually from his mobile phone and his fixed-line broadband connection. He incited his followers on twitter to support the activities of ISIS in its goal towards establishing Islamic State.

The accused was using softwares like VPN and Ghost IP to successfully mask his IP address and his identity; and to delete incriminating materials on a regular basis he has used 'C Cleaner' and other software.

He regularly browsed internet pages where ISIS posted messages in Arabic and he would immediately translate them to English by using Google Translate Software and tweet them.

These instances pose a threat to the Nation and the society and the Respondent submitted that under these circumstances the petition for bail should be dismissed.

**Points considered by Court:**

The Court did not accept the ground urged by the petitioner that as on the date of the arrest of the petitioner, ISIS was not banned by Government of India. The United Nations Organisation itself has banned it in the year 2007 thereby the organization is a terrorist organization under Unlawful Activities (Prevention) Act, 1967.

**Conclusion of Court:**

Investigation papers and the statement recorded on behalf of the prosecution convinced the Court about involvement of the accused.

Effort made by the petitioner is for the specific purpose of destabilizing the Nation and Society. Destabilizing the Society and the State can be done not only verbally, but also by using soft and illegal methods like the one used by the petitioner.

The paramount importance is always security and safety of the Nation and the society. Evidence in the hands of the prosecution against which the charge sheet is filed is sufficient for the purpose of rejecting bail of the petitioner.



# 22. Section 67 – Transmitting Obscene Electronic Material

Transmitting obscene electronic material is covered by section 67 of the Information Technology Act. This section states as under:

## **67. Punishment for publishing or transmitting obscene material in electronic form.**

**Whoever publishes or transmits or causes to be published or transmitted 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 three years and with fine which may extend to five lakh rupees and in the event of 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 ten lakh rupees.**

There is no settled definition of pornography or obscenity. What is considered simply sexually explicit but not obscene in USA may well be considered obscene in India. There have been many attempts to limit the availability of pornographic content on the Internet by governments and law enforcement bodies all around the world but with little effect.

Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories. The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression, it has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as “offensive to modesty or decency; lewd, filthy, repulsive.

Other than the Information Technology Act, other Indian laws that deal with pornography include the Indecent Representation of Women (Prohibition) Act, the Indian Penal Code and the Bharatiya Nyaya Sanhita from 1st of July, 2024.

This section explains what is considered to be obscene and also lists the acts in relation to such obscenity that are illegal. To understand what constitutes obscenity in the electronic form, let us analyse the relevant terms.

Any material in the context of this section would include video files, audio files, text files, images, animations etc. These may be stored on CDs, websites, computers, cell phones etc.

Lascivious is something that tends to excite lust.

Appeals to, in this context, means “arouses interest”.

Prurient interest is characterized by lustful thoughts.

Effect means to produce or cause some change or event.

Tend to deprave and corrupt in the context of this section means “to lead someone to become morally bad”.

Persons here refers to natural persons (men, women, children) and not artificial persons (such as companies, societies etc).

Having understood these terms, let us analyse what constitutes obscenity. To be considered obscene for the purpose of this section, the matter must satisfy at least one of the following conditions: (1) it must tend to excite lust, or (2) it must arouse interest in lustful thoughts, or (3) it must cause a person to become morally bad.

The above conditions must be satisfied in respect of a person who is the likely target of the material. This can be understood from the following illustration:

**Illustration:** Sameer launches a website that contains information on sex education. The website is targeted at higher secondary school students. Pooja is one such student who is browsing the said website. Her illiterate young maid servant happens to see some explicit photographs on the website and is filled with lustful thoughts.

This website would not be considered obscene. This is because it is most likely to be seen by educated youngsters who appreciate the knowledge sought to be imparted through the photographs. It is under very rare circumstances that an illiterate person would see these explicit images.

To understand the acts that are punishable in respect of obscenity in the electronic form, let us analyse the relevant terms.

Publishes means “to make known to others”. It is essential that at least one natural person (man, woman or child) becomes aware or understands the information that is published. Simply putting up a website that is never visited by any person does not amount to publishing.

**Illustration:** Sameer has just hosted a website containing his articles written in English. Sameer has not published the articles. An automated software released by an Internet search engine indexes Sameer’s website. Sameer has still not published the articles.

A Chinese man, who does not understand a word of English, accidentally visits Sameer’s website. Sameer has still not published the articles. Pooja, who understands English, visits Sameer’s website and reads some of his articles. Now, Sameer has published his articles.

Transmits means to pass along, convey or spread. It is not necessary that the “transmitter” actually understands the information being transmitted.

**Illustration:** Sameer has just hosted a website containing his articles. Pooja uses an Internet connection provided by Noodle Ltd to visit Sameer’s website. Noodle Ltd has transmitted Sameer’s articles to Pooja. However, Noodle employees are not actually aware of the information being transmitted by their computers.

Causes to be published means “to bring about the publishing of something”. It is essential that the actual publishing must take place.

**Illustration:** Sameer has just hosted a website containing his articles. An automated software released by Noodle Internet search engine indexes Sameer’s website. But no human being has still used that index to read these articles. Noodle has not caused Sameer’s articles to be published.

Based upon the index created by Noodle, Pooja reaches Sameer's website and reads some of his articles. Now, Noodle has caused Sameer's articles to be published.

Information in the electronic form includes websites, songs on a CD, movies on a DVD, jokes on a cell phone, photo sent as an email attachment etc.

**CASE LAW:** Avnish Bajaj vs. State (N.C.T.) of Delhi  
[(2005)3CompLJ364(Del), 116(2005) DLT427, 2005(79)DRJ576]

### **Summary of the case**

Avnish Bajaj, CEO of Baazee.com, an online auction website, was arrested for distributing cyber pornography. The charges stemmed from the fact that someone had sold copies of a pornographic CD through the Baazee.com website. The court granted him bail in the case.

### **The major factors considered by the court were:**

- (1) There was no prima facie evidence that Mr. Bajaj directly or indirectly published pornography,
- (2) The actual obscene recording/clip could not be viewed on Baazee.com,
- (3) Mr. Bajaj was of Indian origin and had family ties in India.

### **Background**

Avnish Bajaj is the CEO of Baazee.com, a customer-to-customer website, which facilitates the online sale of property. Baazee.com receives commission from such sales and also generates revenue from advertisements carried on its web pages.

An obscene MMS clipping was listed for sale on Baazee.com on 27<sup>th</sup> November, 2004 in the name of "DPS Girl having fun". Some copies of the clipping were sold through Baazee.com and the seller received the money for the sale. Avnish Bajaj was arrested under section 67 of the Information Technology Act, 2000 and his bail application was rejected by the trial court. He then approached the Delhi High Court for bail.

### **Issues raised by the Prosecution**

- (1) The accused did not stop payment through banking channels after learning of the illegal nature of the transaction.
- (2) The item description "DPS Girl having fun" should have raised an alarm.

### **Issues raised by the Defence**

- (1) Section 67 of the Information Technology Act relates to publication of obscene material. It does not relate to transmission of such material.

(2) On coming to learn of the illegal character of the sale, remedial steps were taken within 38 hours, since the intervening period was a weekend.

### **Findings of the court**

(1) It has not been established that publication took place by the accused, directly or indirectly.

(2) The actual obscene recording/clip could not be viewed on the portal of Baazee.com.

(3) The sale consideration was not routed through the accused.

(4) Prima facie Baazee.com had endeavoured to plug the loophole.

(5) The accused had actively participated in the investigations.

(6) The nature of the alleged offence is such that the evidence has already crystallized and may even be tamper proof.

(7) Even though the accused is a foreign citizen, he is of Indian origin with family roots in India.

(8) The evidence that has been collected indicates only that the obscene material may have been unwittingly offered for sale on the website.

(9) The evidence that has been collected indicates that the heinous nature of the alleged crime may be attributable to some other person.

### **Decision of the court**

(1) The court granted bail to Mr. Bajaj subject to furnishing two sureties of Rs. 1 lakh each.

(2) The court ordered Mr. Bajaj to surrender his passport and not to leave India without the permission of the Court.

(3) The court also ordered Mr. Bajaj to participate and assist in the investigation.

### **Enforcement of section 67**

Courts have taken a very stringent view in matters under section 67 of the IT Act. In one such case of *Kalandi Charan Lenka vs State of Odisha*, obscene messages affecting the character of the victim were sent to her as well as the mobile phone of her father.

Also, the accused sent written letters containing vulgar language imputing the character of the victim girl. In addition, thereto, pamphlet against the character of the girl was also pasted on the wall of the College Hostel where she was studying.

Also, a fake Facebook account in the name of the girl was created where the accused morphed naked photographs of the girl with the intention to outrage her modesty. The victim filed an FIR and after conclusion of detailed investigation by the Cyber Cell, the accused was arrested.

The accused was in jail for over two months and thereafter bail was granted subject to the following stringent conditions -

The accused was released on bail of Rs. 50,000/- with two solvent sureties each, out of which one surety should be one of his parents;

He would not commit any offence including the offence through the electronic form while on bail;

He would not induce or threaten the victim or her parents or any prosecution witnesses directly or indirectly;

He would also not visit the town of Pattamundai where the victim or her family members reside and place where the victim is studying or working except in the occasion when he would have to appear before the investigating officer or before the Court till conclusion of the trial.

# 23. Section 67A – Electronic Material Containing Sexually Explicit Act

Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form is covered by section 67A of the Information Technology Act. This section states as under:

**67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.**

**Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct 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 ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.**

This section penalises publishing or transmitting of material containing sexually explicit act in the electronic form.

**Illustration:** Sameer and Pooja are engaged in the act of sexual intercourse in their hotel room. Siddharth, an employee of the hotel uses a hidden video camera to record this act. He then copies this video recording onto a CD and gives a copy to his friend. Siddharth is liable under this section.

This section does not apply to material justified as being for the public good (e.g. in the interest of science, literature, art, learning etc) or which is kept or used for bona fide heritage or religious purposes.



# 24. Section 67B – Child Pornography

Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form is covered by section 67B of the Information Technology Act. This section states as under:

**67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.**

**Whoever, -**

**(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or**

**(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or**

**(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or**

**(d) facilitates abusing children online; or**

**(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,**

**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 ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:**

**Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form –**

**(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 for bona fide heritage or religious purposes.**

**Explanation – For the purposes of this section, “children” means a person who has not completed the age of 18 years.**

This section penalises acts relating to obscene electronic material involving persons below the age of 18 years. The following acts are punishable under this section:

- (1) Publishing or transmitting electronic material which depicts children engaged in sexually explicit act or conduct;
- (2) Causing to be published or transmitted electronic material which depicts children engaged in sexually explicit act or conduct;
- (3) Creating text or digital images depicting children in obscene or indecent or sexually explicit manner;
- (4) Collecting, seeking, browsing, downloading, advertising, promoting, exchanging or distributing electronic material depicting children in obscene or indecent or sexually explicit manner;
- (5) Enticing or inducing children for online relationships for sexually explicit acts;
- (6) Facilitating the online abuse of children;
- (7) Recording in any electronic form sexually explicit acts with children.

This section does not apply to material justified as being for the public good (e.g. in the interest of science, literature, art, learning etc) or which is kept or used for bona fide heritage or religious purposes.

Section 13 of the POCSO Act, 2012 (Protection Of Children from Sexual Offences Act ) criminalizes the use of children in any form of media for sexual gratification, including child pornography.

Section 14 of POCSO prescribes the punishment for such offences.

Section 15 POCSO prescribes punishment for storage of pornographic material involving a child.

The IT Act addresses offences related to online child pornography, particularly under Section 67B which deals with publishing, transmitting, and storing child pornographic content electronically. Together, these laws ensure comprehensive legal coverage for the protection of children against sexual exploitation, both offline and online.

**Section 13** of POCSO states that :

“Whoever, uses a child in any form of media (including programme or advertisement telecast by television channels or internet or any other electronic form or printed form, whether or not such programme or advertisement is intended for personal use or for distribution), for the purposes of sexual gratification, which includes—

- (a) representation of the sexual organs of a child;
- (b) usage of a child engaged in real or simulated sexual acts (with or without penetration);
- (c) the indecent or obscene representation of a child, shall be guilty of the offence of using a child for pornographic purposes

Explanation.—For the purposes of this section, the expression “use a child” shall include involving a child through any medium like print, electronic, computer or any other technology for preparation, production, offering, transmitting, publishing, facilitation and distribution of the pornographic material.”

Section 2(d) of POCSO defines a child as :

"child" means any person below the age of eighteen years”.

Let us break down the Section 13 of POCSO for easier understanding:

**Whoever** (gender neutral, any age - here if the person committing the violation is below 18 years of age, such person will be tried under the Juvenile Justice Act, 2015 ),

**Uses a child** (any gender, below the age of 18 - to be read along with the explanation)

**In any form of media**

- Including programme or advertisement (other media like reels, shorts, photographs, posts, gifs, video etc.)
- telecast by television channels or internet or any other electronic form (content held in storage devices like pen drive, hard disks, cloud etc.) or printed form,
- whether or not such programme or advertisement is intended for personal use or for distribution,

**For the purposes of sexual gratification**, which includes —

representation of the sexual organs of a child;  
usage of a child engaged in real or simulated sexual acts (with or without penetration);  
the indecent or obscene representation of a child,

shall be guilty of the offence of using a child for pornographic purposes

**ILLUSTRATION** : Ramesh records a video of a nude child bathing on his mobile phone. Later he uploads it as a reel on his social media. In such a case Ramesh will be liable for punishment under section 13 of the POCSO Act, 2012.

**Section 14** of POCSO prescribes the punishment for offences committed under section 13.

For the first Conviction for Child Pornography (Section 13 violation):

Imprisonment: Up to 5 years and fine as decided by the court.

Subsequent Conviction for Child Pornography:

Imprisonment: Up to 7 years and fine as decided by the court.

**Section 15** of the POCSO Act provides punishments for :

Storage of Child Pornography for Commercial Use.

Punishment : Imprisonment: Up to 3 years and fine as decided by the court.

Section 15 of POCSO Act states that :

“15. Punishment for storage of pornographic material involving child.—

(1) Any person, who stores or possesses pornographic material in any form involving a child, but fails to delete or destroy or report the same to the designated authority, as may be prescribed, with an intention to share or transmit child pornography, shall be liable to fine not less than five thousand rupees and in the event of second or subsequent offence, with fine which shall not be less than ten thousand rupees.

Let us break down the Section 15(1) of POCSO for easier understanding:

**Any person**, (gender neutral, any age - here if the person committing the violation is below 18 years of age, such person will be tried under the Juvenile Justice Act, 2015 )

**who stores or possesses** (here the word ‘*store*’ could mean the act of actively saving the content in a hard disk, flash drive, cloud or other storage medium, including physical storage medium and the word ‘*possess*’ could mean the act of physically or virtually being in possession of the said content)

**pornographic material** (although the term ‘pornographic material’ has not been defined under the Act it could be inferred from section 13 that any material which is used for sexual gratification, including -

representation of the sexual organs - real or simulated sexual acts (with or without penetration); - the indecent or obscene representation of a person, could mean pornographic material)

**in any form** (digital, printed, animated, AI generated etc.)

**involving a child**, (as defined under Section 2(d))

**but fails to delete or destroy or report the same to the designated authority, as may be prescribed**, (note here that the words or have been used - delete or destroy or report - meaning thereby that *any one* must be done)

**with an intention to share or transmit child pornography**, (this is a crucial part of the section wherein the intent to share or transmit the content must be present for conviction under this section. This will be governed by Section 30 (*Presumption of Culpable Mental State*) of POCSO - meaning that the burden of proof will be on the accused)

**shall be liable to fine not less than five thousand rupees and in the event of second or subsequent offence, with fine which shall not be less than ten thousand rupees.**

ILLUSTRATION 1: Ramesh downloads pornographic images of children from the internet and saves them in a folder in his hard disk naming the folder '*for Prem*'. The presumption in this case will be that Ramesh had downloaded the content with the intention to share it and the burden of proof will be on Ramesh that Section 15(1) of POCSO Act, 2012.

Let us break down the Section 15(2) of POCSO for easier understanding:

(2) Any person, who stores or possesses pornographic material in any form involving a child for transmitting or propagating or displaying or distributing in any manner at any time except for the purpose of reporting, as may be prescribed, or for use as evidence in court, shall be punished with imprisonment of either description which may extend to three years, or with fine, or with both.

**Any person**, (gender neutral, any age - here if the person committing the violation is below 18 years of age, such person will be tried under the Juvenile Justice Act, 2015 )

**who stores or possesses** (here the word '*store*' could mean the act of actively saving the content in a hard disk, flash drive, cloud or other storage medium, including physical storage medium and the word '*possess*' could mean the act of physically or virtually being in possession of the said content)

**pornographic material** (although the term 'pornographic material' has not been defined under the Act it could be inferred from section 13 that any material which is used for sexual gratification, including - representation of the sexual organs - real or simulated sexual acts (with or without penetration); - the indecent or obscene representation of a person, could mean pornographic material)

**in any form** (digital, printed, animated, AI generated etc.)

**involving a child**, (as defined under Section 2(d) of POCSO Act)

**for transmitting or propagating or displaying or distributing in any manner at anytime** (here any one of the following acts of transmitting or propagating or displaying or distributing must be committed, in the context of the pornographic material. None of these words have been defined under the act but the word '*transmits*', has been explained under Section 66E(a) of the IT Act, 2000)

**except for the purpose of reporting, as may be prescribed, or for use as evidence in court** (this is an exception created under the section where, transmitting or propagating or displaying or distributing can be allowed only if it pertains to reporting or if such pornographic material is used as an evidence in the court of law.)

**shall be punished with imprisonment of either description which may extend to three years, or with fine, or with both.**

ILLUSTRATION 1 : Ramesh receives a WhatsApp forward from his friend Prem Chopra obscenely depicting nude pictures of a minor. Ramesh immediately reports the matter to the authorities. In such case Prem Chopra will be liable for transmitting / distributing pornographic material under section 15(2) of POCSO Act, 2012.

ILLUSTRATION 2: In a case where the lawyer for a minor sends images found in possession of the accused to the judge as evidence (in a hard disk), such transmission of pornographic material would fall under the exception to section 15(2) of POCSO Act, 2012.

(3) Any person, who stores or possesses pornographic material in any form involving a child for commercial purpose shall be punished on the first conviction with imprisonment of either description which shall not be less than three years which may extend to five years, or with fine, or with both and in the event of second or subsequent conviction, with imprisonment of either description which shall not be less than five years which may extend to seven years and shall also be liable to fine.”

Let us break down the Section 15(3) of POCSO for easier understanding:

**Any person**, (gender neutral, any age - here if the person committing the violation is below 18 years of age, such person will be tried under the Juvenile Justice Act, 2015 )

**who stores or possesses** (here the word ‘store’ could mean the act of actively saving the content in a hard disk, flash drive, cloud or other storage medium, including physical storage medium and the word ‘possess’ could mean the act of physically or virtually being in possession of the said content)

**pornographic material** (although the term ‘pornographic material’ has not been defined under the Act it could be inferred from section 13 that any material which is used for sexual gratification, including - representation of the sexual organs - real or simulated sexual acts (with or without penetration); - the indecent or obscene representation of a person, could mean pornographic material)



**in any form** (digital, printed, animated, AI generated etc.)

**involving a child**, (as define under Section 2(d))

**for commercial purpose** (although this term has not been defined under the act it could be inferred from definitions under other legislations to mean activity done with an intent of commercial gain)

**shall be punished on the first conviction with imprisonment of either description which shall not be less than three years which may extend to five years, or with fine, or with both and in the event of second or subsequent conviction, with imprisonment of either description which shall not be less than five years which may extend to seven years and shall also be liable to fine.**

Illustration : "A" downloads pornographic material involving children from the internet and stores it in his computer. Later he uploads the same content onto a pornographic website and earns revenue / money by doing so. In this case "A" will be punishable under section 15 of POCSO Act.

**Section 2(da)** "child pornography" means any visual depiction of sexually explicit conduct involving a child which include photograph, video, digital or computer generated image indistinguishable from an actual child and image created, adapted, or modified, but appear to depict a child;]

Let us break down the Section 2(da) of POCSO for easier understanding:

"child pornography" means

**Any visual depiction of**

**sexually explicit conduct** (not defined under the Act)

**involving a child** (according to Section 2(a) - "child" means any person below the age of eighteen years")

Here '*visual depiction*' would include photograph, video, digital or computer generated image indistinguishable from an actual child and image created, adapted, or modified, but appear to depict a child;

**Food for thought:** It is important to note that there are 2 phrases used here namely; '*indistinguishable from an actual child*' and '*appear to depict a child*'- the purpose of this distinction could be to get AI generated / animated content created to depict children within the ambit of the section.

The term *Sexually Explicit Conduct* has however been defined under [18 USC § 2256\(2\)](#) of the United States Code as:

(2) (A) Except as provided in subparagraph (B), “sexually explicit conduct” means actual or simulated— (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the anus, genitals, or pubic area of any person; (B) For purposes of subsection 8(B) of this section, “sexually explicit conduct” means— (i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the anus, genitals, or pubic area of any person;

## **Case Law**

### **Just Rights for Children Alliance v S. Harish (2024)**

In a landmark judgement in the Case of "Just Rights for Children Alliance vs. S. Harish", the Supreme Court addressed a few extremely pertinent issues involving child pornography, intermediary liability, and certain legislative clarity under the Protection of Children from Sexual Offences Act, 2012 (POCSO) and the Information Technology Act, 2000.

Facts of the case in a nutshell:

Harish was found to be watching child pornographic films. Upon questioning Harish admitted to regularly viewing pornography. After a thorough investigation, it was found that many pornographic video files were downloaded and stored in Harish's mobile phone. A case was registered against Harish for offenses under Section 67B of the IT Act and Section 15(1) of the POCSO Act based on the findings.

The Supreme Court thoroughly examined the case and offered clarity on several key issues.

**Scope of Child Pornography Under POCSO :** The judgement stated that mere possession of child pornographic material can attract penalties, especially when there is an intent to transmit or failure to delete or destroy it.

**Liabilities of Intermediary :** The Court emphasized the responsibilities of intermediaries under Section 79 of the IT Act and the POCSO Rules. Guidelines were given to all the intermediary platforms, like Google, Facebook, and Instagram, etc, to exercise due diligence and immediately remove and report to the designated authorities if they come across any material that is sexually exploitative of the child.

**Inconsistent High Court rulings :** The question of whether possession and storage of child pornography constitutes an offence as per Section 15 POCSO and Section 65B of the IT Act has come up before several high courts in the past. They have led to a series of conflicting judgments. While some High Courts had ruled that mere downloading or viewing does not amount to an offence, few others have ruled the opposite. But in the said case Supreme Court clarified that even viewing and possessing child pornographic material constitutes an offence under POCSO and IT Act.

**Amendment of definition :** The Supreme Court emphasised the need to amend the definition of the term “child pornography” to “Child Sexual Exploitative and Abuse Material (CSEAM),” so as to accurately emphasise the exploitive and abusive nature of the offence.

**Culpable Mental state :** Under Section 30 of the POCSO Act, the law assumes that the accused had a guilty state of mind when committing the offence. However it was clarified that the burden to prove was on the accused to show that he did not intentionally download / view / store / possess the child pornographic content.

**Other aspects of the judgement :** Guidelines were provided by the Supreme Court identification and rehabilitation of victims of child pornography. The Court directed the Ministry of Women and Child Development to implement sex education programs to ensure awareness regarding legal and ethical ramifications of child pornography. It suggested that public campaigns on child sexual exploitative material should be organised, and “at-risk” young people with ‘problematic sexual behaviour’ (PSB) be identified and supported by educators, healthcare providers and law enforcement agencies.

# 25. Section 67C – Preservation and Retention of Information by Intermediaries

Preservation and retention of information by intermediaries is covered by section 67C of the Information Technology Act. This section states as under:

## **67C. Preservation and retention of information by intermediaries**

**(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.**

**(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.**

# **State of Maharashtra vs. Vishal Hiranman Bhogade & Ors.**

**IN THE COURT OF JUDICIAL MAGISTRATE FIRST CLASS,**

**(COURT NO. 3), PUNE  
R C. C. No. 2095/2013**

**State of Maharashtra (Complainant)**

**vs.**

**Vishal Hiranman Bhogade & Ors. (Accused)**

## **Background of Case:**

Informant, Dr. Sanjay Tungar was working in Cyber Crime Cell, Commissioner office, Pune. On 25/8/2012, one e-mail was received on mail-ID of Police Commissioner, Pune. Subject of that mail was "In Ganesh festival bomb blast". The e-mail contained a message as "Mission Ganesh attack. If you want to stop try but don't cry". As it was an objectionable e-mail, it was sent to the Cyber Crime Cell, Pune for investigation.

Dr. Tungar conducted preliminary inquiry. He obtained information from Yahoo Company and BSNL. It revealed in the investigation that said e-mail was sent from Raje Computers, Rajgurunagar, Pune. He visited the said cyber cafe. Internet connection was in the name of accused Vishal Bhogade and the cyber cafe was being run by Sandesh Dere. The said cyber cafe was not registered, necessary records required by law were not maintained and I.D. proofs were not obtained from users. Hence, the police could not reach to the main culprit. Dr. Tungar lodged FIR against present accused.

## **Contention of Complainant:**

Under the IT Act, 'intermediary' includes cyber cafe. Cyber cafe means any facility from where access to the internet is occurred by any person in the ordinary course of business to the members of the public. As per rule 3 of the Information Technology (Guidelines for Cyber Cafe) Rules 2011, registration of cyber cafe is compulsory. As per rule 4, taking ID proof of users is compulsory.

As per rule 5, maintenance of log register is compulsory. Preserving the information under rule 4 and 5 for 1 year is compulsory. In the present case cyber cafe was not registered. Requisite information was not obtained and preserved. As per section 67C(1) of IT Act preserving and retaining the information by intermediary is compulsory.

**Contention of Accused:**

Accused submitted that they are law abiding persons with no criminal record. They are attending the court regularly and they requested to impose minimum punishment.

**Points considered by Court:**

Intention behind the Information Technology (Guidelines for Cyber Cafe) Rules 2011 needs to be considered. Cyber crime or cyber terrorism is a big challenge/ threat before the world and specially before India. To cope up with that challenge various rules are framed.

With the help of cyber cafe anyone can commit cyber crime and if proper record is not maintained, the criminal may escape from the clutches of the police. In the present case, objectionable e-mail was received but due to the non-maintenance of record by the accused, the main culprit could not be traced.

**Conclusion of the Court:**

Offence punishable under section 67C of IT Act is proved against the accused. Offence is for non-registration of cyber cafe and non-maintenance of required information.

The court passed an order for imprisonment of 15 days and fine of Rs. 10,000/- upon each accused.

# 26. Section 68 – Power of the Controller to Give Directions

Power of the Controller to give directions are covered by section 68 of the Information Technology Act. This section states as under:

## **68. Power of the Controller to give directions.**

**(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 order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.**

**(2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both.**

This is a simple section that empowers the Controller to order a Certifying Authority and its employees to comply with the *Information Technology Act* and allied laws. If they do not comply with the order to take suitable measures or cease certain activities, then they are liable for punishment under this section.

**Illustration:** The Controller orders Siddharth, a director of Noodle Certifying Authority to provide information about Sameer. Noodle had issued a digital signature certificate to Sameer. This information is needed in the adjudication of a case involving Sameer. If Noodle does not provide this information, it will be liable under this section.



**Illustration:** Noodle Certifying Authority is making statements in the media against other Certifying Authorities. Such statements are affecting the public confidence in the use of digital signatures and e-governance. The Controller orders Siddharth, a director of Noodle Certifying Authority to stop making such statements. If Siddharth does not stop such activities, he will be liable under this section.

# **27. Section 69 – Interception or Monitoring or Decryption of any Information**

Power to issue directions for interception or monitoring or decryption of any information through any computer resource are covered by section 69 of the Information Technology Act. This section states as under:

## **69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.**

**(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.**

**(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.**

**(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to –**

- (a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or**
- (b) intercept, monitor, or decrypt the information, as the case may be; or**

**(c) provide information stored in computer resource.**

**(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.**

Section 69 is a very important section that gives wide powers to the Government to intercept, monitor and decrypt information under special circumstances. The outline of this section is:

(1) The Government can direct any agency (e.g. police, CBI etc) to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer resource.

(2) The reasons for this order are to be recorded in writing.

(3) The Government must be satisfied that this order is necessary: (a) in the interest of the sovereignty or integrity or defence of India, or (b) in the interest of the security of the State, or (c) in the interest of friendly relations with foreign States, or (d) in the interest of public order, or (d) for preventing incitement to the commission of any cognizable offence relating to the above, or (e) for investigation of any offence.

(4) The Government agency can call upon any person for assistance to monitor, provide access to, intercept or decrypt information.

(5) If such a person does not provide such assistance then he is liable for imprisonment up to 7 years and fine.

**Illustration:** It is suspected that some terrorists are using the Noodle Ltd email services to plan a terrorist attack in India. The Government directs the police to intercept these emails.

The police request Sameer, the Director of Noodle Ltd for assistance in obtaining these emails. Sameer refuses to cooperate. He would be liable under this section.

**Illustration:** The Controller suspects that Parag and Siddharth are planning a major hacking attempt on Indian Government websites. The Government directs the police to intercept information being transmitted by them on the Internet.

The suspects are using the Internet services provided by Noodle Ltd. The police request Sameer, the Director of Noodle Ltd for assistance in obtaining this information. Sameer refuses to cooperate. He would be liable under this section.

Under the *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009*, the competent authority is Secretary in the Department of Home Affairs (in case of the Central Government) and Secretary in charge of the Home Department (in case of State Government or Union Territory).

Some of the important terms defined under Rule 2 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 are:

(c) “Decryption” means the process of conversion of information in non-intelligible form to intelligible information via a mathematical formula, code, password or algorithm or a combination thereof;

(d) “Decryption assistance” means to – (i) allow access, to the extent possible, to encrypted information; or (ii) facilitate conversion of encrypted information into an intelligible form;

(e) “Decryption direction” means a direction issued under Rule (3) in terms of which a decryption key holder is directed to – (i) disclose a decryption key; or (ii) provide decryption assistance in respect of encrypted information

(f) “Decryption key” means any key, mathematical formula, code, password, algorithm or any other data which is used to - (i) allow access to encrypted information; or (ii) facilitate the conversion of encrypted information into an intelligible form;

(g) “Decryption key holder” means any person who deploys the decryption mechanism and who is in possession of a decryption key for purposes of subsequent decryption of encrypted information relating to direct or indirect communications;

(i) “Intercept” with its grammatical variations and cognate expressions, means the aural or other acquisition of the contents of any information through the use of any means, including an interception device, so as to make some or all of the contents of a information available to a person other than the sender or recipient or intended recipient of that communication, and includes the -

(a) monitoring of any such communication by means of a monitoring device;

(b) viewing, examination or inspection of the contents of any direct or indirect information; and (c) diversion of any direct or indirect information from its intended destination to any other destination;

(j) “Interception device” means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used whether by itself or in combination with any other instrument, device, equipment or apparatus, to intercept any information;

and a reference to an “interception device” includes, where applicable, a reference to a “monitoring device”;

(l) “Monitor” with its grammatical variations and cognate expressions, includes, to view or to inspect or listen to or record information by means of a monitoring device;

(m) “Monitoring device” means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself in combination with any other instrument, device, equipment or apparatus, to view or to inspect or to listen to or record any information;

The procedure and safeguards have been detailed under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

# 28. Section 69A – Blocking of Information for Public Access

Power to issue directions for blocking for public access of any information through any computer resource is covered by section 69A of the Information Technology Act. This section states as under:

**69A. Power to issue directions for blocking for public access of any information through any computer resource.**

**(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.**

**(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.**

**(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.**

*The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009* contain detailed provisions relating to the procedure and safeguards for blocking for access of information by public.

Section 69A gives powers to the Government to block access to information under special circumstances. The outline of this section is:

(1) The Government can direct any Government agency or intermediary to block for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The reasons for this order are to be recorded in writing.

(3) The Government must be satisfied that this order is necessary:

(a) in the interest of the sovereignty or integrity or defence of India, or

(b) in the interest of the security of the State, or

(c) in the interest of friendly relations with foreign States, or

(d) in the interest of public order, or

(e) for preventing incitement to the commission of any cognizable offence relating to the above.

(4) If the intermediary does not comply, it will be liable for imprisonment up to 7 years and fine.

# **Sneha Kalita vs. Union of India (UOI) and Ors.**

IN THE SUPREME COURT OF INDIA

W.P. (C) Nos. 943 and 872/2017

Sneha Kalita (Appellant)

Vs.

Union of India (UOI) and Ors. (Respondent)

## **Background of the case:**

Writ petition was filed to take immediate measures to ban/block all sites linked with the Blue Whale online game or any other form of violent and immoral games similar in nature.

The Blue Whale online game refers to various steps that the game suggests which leads people in a path where they are brain-washed and dragged to commit suicide.

The Supreme Court contended that the Blue Whale game is dangerous to life and cannot be allowed to be permitted.

## **Points considered by the Court:**

The Ministry of Electronics and Information Technology (MEITY) has set up CERT-In which is engaged in stopping the aforesaid games, so that unwarranted incidents do not occur.

CERT-In had entered into various communications and correspondences with many agencies and is getting cooperation, and the Central Government is determined to stop such games as they have the potentiality to destroy life.

A high-level Committee that had been constituted under the Chairmanship of Director General of CERT-In to investigate all cases where suicides have been committed or attempted allegedly using 'Blue Whale Challenge Game'.

An advisory/awareness document regarding the Blue Whale Challenge Game has been published on the website of MEITY.



MEITY had approached leading academic bodies, R & D institutions & cyber security organizations to find out as to how children are accessing this game and what is the source of information.

Section 69A of the IT Act empowers MEITY to issue directions for blocking of public access to any information through any computer resource in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above.

However, as there are no downloadable applications of the game, there is very little scope for using technical solutions to identify or block the game.

MEITY had issued directives to Google India, Microsoft India, Facebook India and Yahoo India, directing them to ensure that all links of the Blue Whale Challenge Game and of any similar game are immediately removed from their platforms.

**Decision of the court:**

The Chief Secretaries of the States and the Union Territories through their concerned departments were directed to spread awareness in the schools run by the State, who in their turn shall make aware the children about the danger such games propagate by bringing people into a trap.

# 29. Section 69B – Monitoring and Collecting Traffic Data

Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security is covered by section 67A of the Information Technology Act. This section states as under:

**69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.**

**(1) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.**

**(2) The intermediary or any person in-charge of the computer resource shall, when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.**

**(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.**

**(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.**

**Explanation. – For the purposes of this section, -**

**(i) “computer contaminant” shall have the meaning assigned to it in section 43;**

**(ii) “traffic data” means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service and any other information.**

The *Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009* contain detailed provisions for the procedure and safeguard for monitoring and collecting traffic data or information. Some of the important terms defined in rule 2 include:

(f) “Cyber security incident” means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service/ disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization;

(g) “Cyber security breaches” means unauthorized acquisition or unauthorized use by a person of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource;

(i) “Information security practices” means implementation of security policies and standards in order to minimize the cyber security incidents and breaches;

(k) “Monitor” with its grammatical variations and cognate expressions, includes to view or inspect or record or collect traffic data or information by means of a monitoring device;

(l) “Monitoring device” means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself in combination with any other instrument, device, equipment or apparatus, to view or inspect or record or collect traffic data or information;

(m) “Port” or “Application Port” means a set of software rules which identifies and permits communication between application to application, network to network, computer to computer, computer system to computer system;

(o) security policy means documented business rules and processes for protecting information and the computer resource;

Section 69B gives powers to the Government to monitor and collect traffic data or information for cyber security. The outline of this section is:

(1) The Central Government can authorise any Government agency to monitor and collect traffic data or other electronic information.

(2) Such an authorization can be made under the following circumstances:

- (a) to enhance cyber security in the country
- (b) for identification, analysis and prevention of intrusion in the country,  
or
- (c) for identification, analysis and prevention of spread of computer  
contaminant in the country.

(3) Such an authorization must be made by a notification in the Official Gazette.

# 30. Section 70 – Protected System

Protected Systems are covered by section 70 of the Information Technology Act. This section states as under:

## **70. Protected system.**

**(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.**

**Explanation. – For the purposes of this section, “Critical Information Infrastructure” means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety;**

**(2) The appropriate Government may, by order in writing, authorise the persons who are authorised 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 shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.**

**(4) The Central Government shall prescribe the information security practices and procedures for such protected system.**

There are three elements to this section-

(1) Gazette notification by the appropriate Government for declaring a computer resource as a protected system.

(2) Government order authorizing persons to access protected systems.

(3) Punishment for securing access or attempting to secure access to protected systems by unauthorised persons.

Let us discuss the relevant terms and issues in detail.

Appropriate government is determined as per Schedule VII of the Constitution of India. Schedule VII of the Constitution of India contains three lists – Union, State and Concurrent. Parliament has the exclusive right to make laws on items covered in the Union List e.g. defence, Reserve Bank of India etc.

State Governments have the exclusive right to make laws on items covered in the State List e.g. police, prisons etc. Parliament as well as the State Governments can make laws on matters in the Concurrent List e.g. forests, electricity etc.

**Illustration:** If the computer network of the Indian Army is to be declared as a protected system, the Central Government would be the appropriate Government.

**Illustration:** If the computer network of the Mumbai police is to be declared as a protected system, the Government of Maharashtra would be the appropriate Government.

**Illustration:** If the computer network of the Forest Department in Maharashtra is to be declared as a protected system, the Central Government as well as the Government of Maharashtra would be the appropriate Government.

All the acts, rules, regulations etc passed by the Central and State Government are notified in the Official Gazette. The Official Gazette in the electronic form is called the Electronic Gazette. A notification becomes effective on the date of its publication in the Gazette.

The Government order may specify the authorised persons by name or by designation (e.g. all officers of rank of Inspector and above deputed in a particular department).

The two concepts covered in this provision are “secures access” and “attempts to secure access”.

According to section 2(1)(a) of the IT Act, “access” with its grammatical variations and cognate expressions, means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network;

Secures access - the term “secure” means “to make certain”. The term “secures access” would mean “to make certain that access can be achieved as and when desired by the person seeking to access”. When such access is ensured by a person, he is said to have secured access. The term “securing access” in this section is a grammatical variation of the term “secures access”.

**Attempt to secure access** – when a person is attempting to make sure that access can be achieved, he is said to be making an attempt to secure access. Attempt to secure access is a very wide term and can best be understood through the following illustrations.

**Illustration:** Sameer runs a password cracking software to crack the password of a protected system. Irrespective of whether he succeeds in cracking the password, he is guilty of attempting to secure access.

**Illustration:** Sameer runs automated denial of service software to bring down the firewall securing a protected system. Irrespective of whether he succeeds in bringing down the firewall, he is guilty of attempting to secure access.

**Illustration:** Sameer sends a Trojan by email to Pooja, who is the network administrator of a protected system. He plans to Trojanize Pooja's computer and thereby gain unauthorised access to the protected system. Irrespective of whether he succeeds in finally accessing the protected system, he is guilty of attempting to secure access.

As per Executive Order dated 12<sup>th</sup> September, 2002, issued by Ministry of Communications & Information Technology, details of every protected system should be provided to the Controller of Certifying Authorities.



# 31. Section 70B – Indian Computer Emergency Response Team

Section 70B of the Information Technology Act provides for the Indian Computer Emergency Response Team to serve as national agency for incident response. This section states as under:

## **70B. Indian Computer Emergency Response Team to serve as national agency for incident response**

**(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.**

**(2) The Central Government shall provide the agency referred to in sub-section (1) with a Director-General and such other officers and employees as may be prescribed.**

**(3) The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.**

**(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security,-**

**(a) collection, analysis and dissemination of information on cyber incidents;**

**(b) forecast and alerts of cyber security incidents;**

**(c) emergency measures for handling cyber security incidents;**

**(d) coordination of cyber incidents response activities;**

**(e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;**

**(f) such other functions relating to cyber security as may be prescribed.**

**(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.**

**(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person.**

**(7) Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.**

**(8) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (1).**

# 32. Section 71 – Penalty for Misrepresentation

Punishment for misrepresentation for obtaining any license or Electronic Signature Certificate, etc., in electronic form is covered by section 71 of the Information Technology Act. This section states as under:

## **71. 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 Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a terms which may extend to two years, or with fine which may extend to one lakh rupees, or with both.**

This section applies to:

(1) a person, who, for obtaining an electronic signature certificate (a) makes a misrepresentation to the Certifying Authority or (b) suppresses any material fact from the Certifying Authority.

(2) a person obtaining a license to operate as a Certifying Authority (a) makes a misrepresentation to the Controller or (b) suppresses any material fact from the Controller.

Let us examine the essential terms of this section.

Misrepresentation implies “presenting information incorrectly, improperly or falsely”. There must be a deliberate intention to deceive.

**Illustration:** Sameer is applying for a digital signature certificate. He fills in his name as “Siddharth” and also submits photocopies of Siddharth’s passport as proof of identity. Sameer is liable for misrepresenting information to the Certifying Authority.

Suppress implies “to withhold from disclosure”.

**Illustration:** Noodle Ltd is applying for a licence to become a Certifying Authority. One of the questions in the application form is “In case any of the company directors been convicted for a criminal offence, then please mention relevant details.”

One of the Noodle directors has been convicted in the past. But, Noodle officials submit the filled in form with the answer to this question being left blank. The officials will be liable for suppressing information from the Controller.

Material fact implies something that is “relevant, pertinent or essential”.

# 33. Section 72 – Breach of Confidentiality and Privacy

Penalty for breach of confidentiality and privacy is covered by section 72 of the Information Technology Act. This section states as under:

## **72. Penalty for breach of confidentiality and privacy.**

**Save as otherwise provided in this Act or any other law for the time being in force, if 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 the 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.**

The essential elements of this section are:

- (1) It applies to persons who have secured access to some information in pursuance of a power granted under the IT Act or its allied laws (e.g. police, adjudicating officers, Controller etc.).
- (2) Such persons must disclose this information to a third person without authorisation.
- (3) There must be no law which permits such disclosure of information.

**Illustration:** Pooja is a Deputy Superintendent of Police and is investigating an alleged violation of the IT Act. She raids the premises of one of the suspects, Sameer.

During the raid, she seizes several documents and CDs containing incriminating evidence. She later discloses this information to the Magistrate trying the case. Even though Sameer's permission is not taken, Pooja would not be liable under this section.

This is because the Bharatiya Nagarik Suraksha Sanhita permits such information and evidence to be disclosed to the Court. However, if Pooja discloses such information to the press without Sameer's permission, then she will be liable under this section.

# 34. Section 72A – Disclosure of Information in Breach of Lawful Contract

Punishment for disclosure of information in breach of lawful contract. is covered by section 72A of the Information Technology Act. This section states as under:

## **72A. Punishment for disclosure of information in breach of lawful contract.**

**Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.**

This section applies to: any person (including an intermediary) who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person. This person will be penalised if he discloses such material:

- (1) without the consent of the person concerned, or in breach of a lawful contract, and
- (2) with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain.

This section does not apply if the person reveals this information in compliance with any law.

**Illustration:** Sameer works in a call-centre for a large bank. He has access to the financial records of all the customers of the bank. He comes to know that Pooja has fixed deposits worth Rs 2 crore. He passes on this information to his friend Siddharth, who starts threatening Pooja in order to extort money from her. Sameer would be liable under this section.

**Illustration:** Sameer works in a call-centre for a large bank. He has access to the financial records of all the customers of the bank. One day, he is approached by the police who are seeking information about a suspected terrorist who happens to be a customer of the bank. Sameer hands over the banking records of this suspect to the police. He would not be liable under this section as he is acting in conformance with the law which requires everyone to assist the police.



# 35. Section 73 – Publishing False Electronic Signature Certificate

Penalty for publishing Electronic Signature Certificate false in certain particulars is covered by section 73 of the Information Technology Act. This section states as under:

**73. Penalty for publishing Electronic Signature Certificate false in certain particulars.**

**(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that-**  
**(a) the Certifying Authority listed in the certificate has not issued it; or**  
**(b) the subscriber listed in the certificate has not accepted it; or**  
**(c) the certificate has been revoked or suspended,**  
**unless such publication is for the purposes 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.**

Let us examine this section through some illustrations.

**Illustration:** Sameer has created a fake digital signature certificate purporting to have been issued by Noodle Certifying Authority. Sameer plans to use this certificate to carry out some financial frauds. He posts this certificate on his website. He is liable under this section.

**Illustration:** Pooja has applied to Noodle Certifying Authority for a digital signature certificate. Noodle in due course issues the certificate to Pooja. She, however, does not accept it as some of the details are incorrect in the certificate. In the meanwhile, Noodle Ltd publishes her certificate in their online repository. In this case, Noodle Ltd will be liable under this section.

**Illustration:** Pooja is employed with Noodle Ltd. She has obtained a digital signature certificate for official purposes on 1<sup>st</sup> January. She quits her job on 1<sup>st</sup> July and her certificate is revoked on that day. Noodle Ltd continues to keep Pooja's revoked certificate in its online repository even after 1<sup>st</sup> July. Noodle Ltd will be liable under this section. They will not be liable if the purpose behind keeping Pooja's certificate in their repository is to verify documents signed by Pooja between 1<sup>st</sup> January and 1<sup>st</sup> July.

# 36. Section 74 – Publication for Fraudulent Purpose

## **74. Publication for fraudulent purpose.**

**Whoever knowingly creates, publishes or otherwise makes available an Electronic Signature Certificate for any 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.**

**Illustration:** Sameer approaches Noodle Certifying Authority to issue an Electronic Signature Certificate and conveys that he intends to use the same to commit a fraud. Here, both Noodle Certifying Authority and Sameer will be held liable.

# 37. Section 77A – Compounding of Offences

In Concise Oxford Dictionary in Law, the meaning for the word “compound” is given as: (a) condone a liability or offence in exchange for money etc., (b) forbear from prosecuting (a felony) from private motives, and Law come to terms with a person, for foregoing a claim etc., for an offence. For the expression “Compounding” in Ramanathan Aiyar's Law Lexicon, is “Arranging, coming to terms, condone for money; arranging with the creditor to his satisfaction.”

Section 77A of IT Act states that a court of competent jurisdiction may compound offences other than offence for which life imprisonment is imposed or term exceeding three years is provided under the IT Act. Further, Section 77A states that the court shall not grant compounding when an accused is liable by reason of his previous conviction to enhanced punishment or punishment of different kind or if it affects socioeconomic situation of a country or if offence is committed against a child below 18 years or against a woman.

# 38. IPC, Bharatiya Nyaya Sanhita & Cyber crimes against women

The following sections of the Indian Penal Code (IPC) are relevant when it comes to cyber crimes against women:

- 354A. Sexual harassment and punishment for sexual harassment
- 354C. Voyeurism
- 354D. Stalking

## Sexual harassment

Section 354A of the IPC:

**Sexual harassment and punishment for sexual harassment.—**

**(1) A man committing any of the following acts—**

**(i) physical contact and advances involving unwelcome and explicit sexual overtures; or**

**(ii) a demand or request for sexual favours; or**

**(iii) showing pornography against the will of a woman; or**

**(iv) making sexually coloured remarks,**

**shall be guilty of the offence of sexual harassment.**

**(2) Any man who commits the offence specified in clause (i) or clause (ii) or clause (iii) of sub-section (1) shall be punished with rigorous imprisonment for a term which may extend to three years, or with fine, or with both.**

**(3) Any man who commits the offence specified in clause (iv) of sub-section (1) shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.**

From a cyber crime point of view, the following are considered "sexual harassment":

Action	Punishment
Showing or sending pornography to a woman against her will e.g. by email / WhatsApp, or on a social network like Facebook.	Rigorous imprisonment upto 3 years and / or a fine.
Making sexually coloured remarks e.g. by email / WhatsApp, or on a social network like Facebook.	Imprisonment upto 1 year and / or a fine

### Voyeurism

Section 354C of IPC:

**Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.**

**Explanation 1.—For the purpose of this section, “private act” includes an act of watching carried out in a place which, in the circumstances, would reasonably be expected to provide privacy and where the victim's genitals, posterior or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the victim is doing a sexual act that is not of a kind ordinarily done in public.**

**Explanation 2.—Where the victim consents to the capture of the images or any act, but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered an offence under this section.**

### **Let's consider some examples from a cyber voyeurism point of view:**

- Prem Chopra is an employee of a garments store. He places a hidden camera in the changing room and records Pooja while she is trying on some clothes. Prem would be liable for voyeurism.
- Prem Chopra and Pooja are in a romantic relationship. Prem wants to record and photograph their romantic escapades. Pooja agrees to this but tells him never to share the recording with anyone else. A few months later they break up. Prem posts some of the recordings and photos on social media. Prem would be liable for voyeurism.
- Prem Chopra asks his employee Amrish Puri to hide a video camera in the lavatory of the store he owns. This results in the recording of several women who use the lavatory. Prem and Amrish would be liable for voyeurism.
- Pooja is a model for a company selling ladies undergarments. As part of her modeling assignment, she poses in underwear. Prem is the photographer for that assignment. He takes several photographs of Pooja while she is wearing the underwear. Prem will not be liable under this section.

### **Punishment**

- For the first conviction - imprisonment from 1 to 3 years and a fine
- For the second or subsequent conviction - imprisonment from 3 to 7 years and fine

### **Cyber stalking**

Section 354D of IPC:

#### **(1) Any man who—**

**(i) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or**

**(ii) monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking:**

**Provided that such conduct shall not amount to stalking if the man who pursued it proves that—**

**(i) it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or**

**(ii) it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or**

**(iii) in the particular circumstances such conduct was reasonable and justified.**

**(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.**

Let's consider some examples from a cyber stalking point of view:

Prem Chopra has a huge crush on Pooja and proposes to her. She makes it clear that she is not interested in a romantic relationship with him. He continues to profess his love for her via email / WhatsApp / social media. Prem would be liable for cyber stalking.

Prem Chopra operates a cyber cafe frequented by Pooja. He installs a key-logger on all the computers so that he can monitor Pooja's internet, email and social media usage. Prem would be liable for cyber stalking.

### **Punishment**

- For the first conviction - imprisonment upto 3 years and a fine
- For the second or subsequent conviction - imprisonment upto 5 years and fine



A man would not be liable for cyber stalking if he can prove that:

- he was preventing or detecting crime and was authorised by law
- his actions were done to comply with the law
- his actions were reasonable and justified in the particular circumstances

The following sections of the Bharatiya Nyaya Sanhita (BNS) pertain to cyber crimes against women:

- 75 - Sexual harassment and punishment for sexual harassment
- 77 - Voyeurism
- 78 - Stalking

And their corresponding sections of IPC are :

- 354A. Sexual harassment and punishment for sexual harassment
- 354C. Voyeurism
- 354D. Stalking

## **Asian School of Cyber Laws ®**

410, Supreme Headquarters,  
Mumbai-Bangalore Highway,  
Near Audi Showroom,  
Baner,  
Pune - 411045 (INDIA)

Call / Whatsapp us:

9225548601

9225548602

<https://www.asianlaws.org>