CYC- 104

Cyber Crimes

And

Consumer Protection in Cyber Space

School of Law

UTTARAKHAND OPEN UNIVERSITY

Teen Pani Bypass Road, Near Transport Nagar,
Haldwani -263139
Phone No- 05946 - 261122, 261123
Toll Free No. 18001804025

BOARD OF STUDIES

UNIT WRITING

UNIT WRITERS	UNIT
[1] *Dr. Razit Sharma, Assistant Professor, Law College, Uttaranchal University, Dehradun Uttarakhand*	Unit- 1,2,3,4
[2] *Ms. Sapna Agarwal, Advocate High Court of Uttarakhand, Nainital*	Unit- 5,6,7
[3 *Mr. Rajeev Bhatt, Advocate High Court of Uttarakhand, Ex. RTI Advisor Kumaun University Nainital, Ex. Assistant Professor Unity Law College Rudrapur*	Unit- 8 ,9,10
[4] *Dr. Sushim Shukla, Assistant Professor, Law College, Uttaranchal University, Dehradun Uttarakhand*	Unit- 11, 12, 13

EDITOR

Dr. Deepankur Joshi, Assistant Professor& Coordinator,
School of Law, Uttarakhand Open University, Haldwani, (Nainital)

Edition- 2022, Pre-Publication copy for Limited Circulation ISBN-

Publication- Directorate of Studies and Publication, Uttarakhand Open University, Haldwani, Nainital.

E- Mail: studies@uou.ac.in

.

CYC- 104

CYBERCRIMES AND CONSUMER PROTECTION IN CYBER SPACE

INDEX

UNIT-1

DEFINING CRIME

1.1.INTRODUCTION

Crime is a social and economic phenomenon which goes against legal obligations and certain moral sentiments developed in the history of human society. In ancient days any conduct

offending the interest or threatening the security of mankind was a crime. Crime is a dynamic concept which changes with social transformation. As the societies grow and with new and advanced science and technological developments new forms of crimes began to emerge. Present world is experiencing the growing importance of internet in every sphere of life. Undoubtedly, the crimes in cyberspace are also growing fast. This unit in specific discusses the introductory part of crimes committed thorough internet.

1.2.OBJECTIVES

The study of the chapter will make students understand

- The concept of crime
- The Origin and Development of Cyber crime
- Classifications of Cybercrime
- Impact of Cybercrime and its challenges

1.3.STRUCTURE

1.3.1. Defining Crime

The word crime is derived from a Latin word 'Crimean' which means 'charge' or 'cry of distresses. It typically refers to an intellectual mistake or an offense against a society or an individual. Crime is an act which is deemed to be socially harmful, unacceptable and is punishable by law. This approach to the concept of crime changes according to the social, political, psychological and economic structure of a society. Several factors like sociological factors, psychological factors, circumstantial elements etc, influences the criminal activity of an individual or a group. Crimes are again of different types like monetary crime, Sexual crimes, Political crime and miscellaneous crimes. With the advent of science and technology crime also has completely taken a new dimension. It has grown to that extent that it is measured in hours and minutes rather than months and years.

1.3.2. Cyberspace

Cyberspace is a term used to describe the virtual world of computers. William Gibson coined the term 'Cyber space' in his book "Neuromancer" in the year 1984. In simple words it can be stated that Cyberspace is an intricate environment that involves interactions between people, software, and services. This is in fact controlled by the worldwide distribution of information and communication technology devices and networks. Due to the advancements in technology and increase in networks and devices connected, the cyberspace today serves as a common platform for users from different fields that it has become difficult to define a clear boundary among the different groups. People involved in cyberspace, use of computers, Information technology and internet are known as 'Netizens'. It is a word coined from the association of two words 'Internet' and 'Citizen'. Cyberspace can be considered to be global village in the electronic world with instantaneous communication and no geographical boundaries.

1.3.3. Internet

Due to the significant development of computer technology, the present generation cannot imagine a life without computers. They have invaded every aspect of life and the impact is that it has created challenge even to the fundamental principles of law. The administration of Internet is not in the hands of any individual, Government, Corporation or firm. It includes a

network of hundreds and thousands of computers connected to use common data transfer protocol or exchange of information with other computers. This series of networks of computers is called as "Internet", which has the quality of rapidly transmitting communication. Information available at any link means information is available to all connected with that link and there is no individual to control all the information that is available in the Internet.

1.3.4. Communication through Internet

In order to understand the legal issues involved one should have a thorough knowledge of the means of communication available to transfer through Internet.
In general, there are three means available for a user to access Internet.

(i) **Direct Access**- In this mode a user can be directly linked to the Internet without an intermediary. Generally, Government offices, Educational Institutions, Business establishments maintain a computer network linked directly.

(ii) **Service Providers**- Here certain commercial entities provide Internet facility to general public in lieu of the fee paid, thus making a commercial use of the Internet.

(iii) **Commercial online Service**- Here the commercial entities provides direct access to their own content, to the users of their service without any fee.

Exchange of communication through Internet is done by different modes.

1. One to one communication (e.g. E-mail)
2. One to many communication (e.g. List server)
3. Sharing of information databases. (e.g. USENET)
4. Real Time Communication (e.g. Internet Relay Chat)
5. Real time remote computer utilization (e.g. Telnet)
6. Remote Information retrieval (e.g. World Wide Web)

As Technology is growing at a faster pace, there are certain issues like security of transactions, privacy, protection of children against easy access to inappropriate contents etc. that has to address urgently with a strict legal regime.

1.3.5. Concept of Cybercrime

Cybercrime is the term used to refer electronic offenses, e-crimes, white collar crimes etc. In other words, any illegal activity carried out with the help of computer, Internet or electronic gadget is called as 'Cyber-crime'. The phenomenal growth of Internet has provided new panorama to the increase of computer related crimes. Here computer or the data itself is the target of offence or a tool to commit any offence. The term 'Cybercrime' or 'Computer crime' are the terms generally used and includes a wide range of activity ranging from unauthorised access to computer or the data stored in it, trafficking in passwords, transmission of pornographic material, selling pirated copies of software etc. Hence currently the term 'Computer-Related crime' is widely used. However, in a specific context, 'Computer Crime' is where the criminal has an expertise in computer technology. In 'Cybercrime' the perpetrators use their specialised knowledge and skills on cyberspace.

A computer crime is defined by the US Department of Justice as "An illegal act requiring knowledge of computer technology for its perpetration, investigation or prosecution". But the

definition is not exhaustive and it can also be plainly defined as "Crimes directed at a computer or a computer system". However, cybercrime is complex in nature and cannot be expressed in simple terms.

1.3.6. Cybercriminals

Cybercriminals also known as hackers are individuals or a group of people engaged in malicious activity with the use of computer as a tool or a target. It is highly difficult to identify hackers as they use various security measures to hide their original identity. Their intent is to steal sensitive information of an individual or an organisation to generate profit. Cybercriminals use various methods to achieve their objective, and their proficiency depends upon the advancement of technology. Growth of global cybercriminal network poses a great threat to the society.

Types of Cyber criminals

a. Identity Thieves
   These are cybercriminals who try to gain access on the victims' personal details like-name, address, credit card information etc. Initially hackers used the technique to modify the data or uncover the desired information. But due to the advancement in computing the identity thieves manage to hack government or corporate database leading to major losses.
b. Internet Stalkers
   Internet stalkers are criminals who monitor the online activity of the victim with a malicious intent. The motif of such attacks is mainly to blackmail or for bribery.
c. Phishing Scammers
   Phishers are cybercriminals who try to get a hold on the personal information of the victim. Later this is used for identity fraud scams or they sell it in the dark web.
d. Cyber Terrorists
   Cyber terrorism is a cyber-attack done with a political intention, where the criminal attempts to steal data or corrupt government system or network resulting in harming the country at large.

1.3.7. Origin/Development of Cybercrime

Historically, *abacus* can be called the earliest version of a computer and hence history of computer dates back to the origin of abacus in ancient nations like India, China and Japan for more than 5000 years. During 1950's, the size of computer was so big that it occupied the space of an entire room and was too expensive to operate. Few people who had the knowledge of its operation were allowed to work on it. People started using computer individually when IBM introduced its stand-alone "personal computer" in the year 1981 thus exposing them to get access to wide database storage.

The first cybercrime took place in the year 1820 when Joseph-Marie Jacquard's textile employees sabotaged the new technology fearing that it would threaten their livelihood. This was the first recorded cybercrime. In the 1960's when computer was the size of a transistor, offences focused on physical damage of the system and its stored data. The next ten decade

saw a change in the nature of crime which included the illegal use of computer systems and manipulation of electronic data. The 1980's saw emergence of software piracy and spread of malicious software and computer viruses, worms etc. 21st century saw new trends in cybercrime like phishing, e-mail bombing, data-diddling etc. Computer technology which has improved the quality of life has also paved way for increased cybercrime threats on a daily basis.

1.3.8. Nature and Scope of Cyber crime

Crime is a social phenomenon and criminal laws and punishment have been in existence for ages. Cybercrime is that which takes place in virtual world, more unreal and everlasting and hence it is a difficult task to keep a check on it. The nature and scope of this crime changes with the advancement in technology. Complexity of a crime is determined by the complexity of a society. The socio-economic and political structure of the society should be able to keep a track on such crimes. Computer technology has put an end to barriers of time and space making life convenient bringing people closer socially and culturally. This has brought unmanageable ambiguity to cybercrime, making it difficult to identify from the legal aspect. Cybercrime is a global threat, which demands International understanding and regulation. The evolution of Internet Technology has provided a wider scope for criminals to execute crime with the least notion of being detected. This does not require physical strength and only the technological know-how helps the individual in committing the crime. They are silent in nature and could be committed in privacy without the need to reach the victim physically. One salient character of cybercrime is that it is committed with a single click on the mouse, swiftly and silently without the fear of being caught red handed. Huge profit with less or no investment has made this venture a rewarding one. Another striking feature is that it is easy to commit, difficult to detect and even harder to prove. Hence it is the need of the hour to indulge in defensive mechanism and to face this serious challenge against mankind as a whole.

1.3.9. Causes for Internet Crimes

Similar to other crimes the causes for Internet crime is basically greed and need to commit the crime coupled along with the opportunities provoke criminals to commit the crime. Monetary benefit or the greed to make quick money is one factor which induces to commit cybercrime. Internet is widely used by terrorists and extremists to attack the websites and network for political reasons. People who are sexually deviant use porn sites to fulfil their immoral desires and quench their sexual impulses. Some people use social websites to ventilate their emotions. Revenge is well planned and is more dangerous than anger when executed by a cybercriminal. Other factors which come in queue along with this are absence of awareness of common user on what is private data and public data and sharing of personal and private information in social networking sites.

1.3.10. Difference between traditional Crime and Crime Cyber crime

Crime, criminal laws and punishments are as old as mankind. Traditional crime or Conventional crimes like rape, murder, burglary etc. Is one where a weapon or a tool or use of force is involved? But in case of a Cybercrime there is no requirement of force as in this type the criminals use fake identity to steal any secret information. The other distinguishing feature between the two is based on evidence. In a traditional crime the criminal unknowingly leaves a trace of his evidence like finger print or any tangible object whereas Cyber criminals commit

the crime through internet with fake identity making it difficult to track the culprit. Investigation process in a traditional crime begins from the crime scene whereas in a cybercrime it begins from sequence of actions that took place. External support or an eyewitness is needed as an evidence in a conventional crime to track the culprit where it requires the support of service providers like Internet, Mail, Search engines, portals etc., to investigate a cybercrime. Jurisdiction is again clear and well defined in a Traditional crime whereas in case of a cybercrime a thorough investigation has to be carried out.

1.3.11. Classification of Cyber crime

Computer related crime has become a serious concern in today's scenario. One prime factor that has to be taken in to consideration while categorising this crime is that there should be a clarity between what is unethical and what is illegal. The rate of cybercrime is directly proportionate to the advancement of computer technology of that particular country. Cybercrime includes a wide variety of criminal conduct and includes a broad range of offences. This constantly evolves with the invention of new technology.
The following are the crimes, which can be committed under various groups

1.3.11.1 Crime against Individuals

i. Harassment via e-mails.
ii. Cyber-stalking.
iii. Dissemination of obscene material.
iv. Defamation.
v. Unauthorized control/access over computer system.
vi. Indecent exposure
vii. Email spoofing
viii. Cheating & Fraud

1.3.11.2. Crime against Property

i Computer vandalism.

ii. Transmitting virus.

iii. Unauthorized control/access over computer system.

iv. Intellectual Property crimes

v. Internet time thefts

1.3. 11.3. Crime against organisation

i. Unauthorized control/access over computer system
ii. Possession of unauthorized information.
iii. Cyber terrorism against the government organization.
iv. Distribution of pirated software etc.

Against Society at large:

i. Pornography (basically child pornography).

ii. Polluting the youth through indecent exposure.
iii. Trafficking
iv. Financial crimes
v. Sale of illegal articles
vi. Online gambling
vii. Forgery

1.3.12. Frequently used Cybercrimes

Unauthorised access to data and computer network is referred to as hacking. It also includes theft of information in electronic form or that is stored in computer hard disks, or any removable device. E-mail bombing is another menace where the criminal sends repeatedly irrelevant mails resulting in the crash of the victim's system.

Data diddling

This kind of cybercrime is where the raw data is altered before it is processed by a computer and then changing it back once the processing is completed.

Salami attacks

This attack is mainly associated with finance. In this case the alteration made is so insignificant that it completely goes unnoticed in a single case. This is used to siphon a meagre amount of money in several attempts.

Denial of Service attack

This involves flooding of computer resource or exceeding the limit that the servers' system can support or handle. This leads to the crash of the server where the user is denied services offered by the resource.

Virus / worm attacks

Viruses are programs that attach themselves to a computer or a file and then spread to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

1.3.13. Different channels of cybercrime

As discussed earlier Cybercrimes are of different types and can be classified under various criteria.

Cybercrime can be categorised on the basis of victims as:

i. Crime against individual
ii. Crime against property
iii. Crime against a society, organisation or even a nation

On the basis of Modus Operandi, it can be categorised as:

i. Physical attack targeting the hardware
ii. Software attack targeting the information resources
iii. Network access i.e. attacking the system through a vulnerability in the network with or without the help of a software vulnerability.
iv. Insider threat i.e. hacking the information asset of an organisation through an employee of the organisation.

On the legal and investigation aspect, it can be categorised as:

i. Coming under IT Act or the IT Amendment Act along with their civil and criminal jurisdictions
ii. Indian Penal Code for the criminal trial process
iii. Other Acts for their criminal procedures
iv. Other civil Acts and torts wherein computers are involved and only compensation and not a punishment

Broadly speaking any cybercrime can be categorised under any of the above said channels. The type of cybercrime mainly depends on the Modus Operandi of the crime and investigation has to be carried understanding the channel and its effects.

1.3.14. Impact of Cyber crime

Internet has influenced mankind to a great extent than any other inventions of the 20th century. Internet Addiction is a growing menace. Excessive use of computer and its impact on daily life is given the term Internet Addiction Disorder (IAD). Similarly, the impact of cybercrime like fraud, siphoning of money, data diddling and disruption of services creates an irreparable damage, if left unchecked. Several cyber-attacks have been carried out on individuals, government and public sectors to steal information, money or to disrupt the services. Hacking is one such crime which can create a massive financial destruction or loss for individuals, companies or even governments. Hackers are of different types and they may interfere with the resources, information, integrity or reputation of the targeted victim. Effects of hacking cannot be ignored in this digital era as its risks and the danger is increasing leading to vital consequences. Most of the transactions are being done thorough online using plastic currency and this when used without due security can be manipulated by anyone who has the knowledge of technology. Combating cybercrime has become a challenging task even for the government as it is difficult to determine political borders and cyber criminals in the cyberspace. Even sensitive Government departments like NASA had been a prey to this cybercrime, as one juvenile cracked the security code and managed to access the main server. Hence it had to shut down for 21 days all over U.S. to reconstruct a new code. Concept of cybercrime has gained a greater pace, and human society which is highly dependent on technology has become vulnerable. Thus, the impact of cybercrime in this era of globalization has been felt in every fields like social, economic and political aspects as well.

1.3.15. Preventive measures to combat Cybercrime

Cybercrime can be committed from anywhere at any time. Globalisation of commercial activity and ubiquity of the Internet environment has led to a phenomenal increase in the rate of cybercrime. Preventive measures are certain safeguards deployed to avoid, detect or minimise

the security risk or the negative impact. Efficient security control mitigates the security risks to all property be it physical or intellectual.

A broad classification of security controls are as follows:

1. Hardware and Physical control
2. Software and logical control
3. Network control or database control
4. Other controls including those by third parties

Simple measures to control cybercrime:

- Computer users should install antivirus software such as McAfee or Norton.
- Must use a firewall to protect from hackers.
- Passwords should be strong including letters, numerals and some special keys. It should be changed at least once in a month. Avoid storing these details on mobile phones.
- Parents should keep a check on the websites used by children and should limit their time of surfing internet.
- One should avoid disclosing personal data or details on social networking sites.
- Maintain a regular back-up for important documents and use encryption for sensitive files related to finance.
- Business transactions or financial transactions are to be avoided using public Wi-Fi Hotspots.

1.4. SUMMARY

Crime is as old as human beings. Greed accompanied with opportunity provided by the victims is the justification which the criminal gives himself. Any activity which is illegal and punishable by law done through the means of computer and technology is termed as cybercrime. There is a vast difference between traditional crime and cybercrime. Channel of crime is the manner in which it is committed and is essential to make an indepth analysis to categorise the nature of crime. Preventive measures should be taken from all angles for a successful and efficient data protection. 1.5.

1.5. SAQS

1. Short Answer Questions
   a. Explain the concept of Cybercrime.
   b. Write a short note on the differences between Traditional Crime and Cybercrime
2. Fill in the blanks
   a. Cybercrimes are _____ acts where the computer is used either as a _____or both.
   b. _____is a term used to describe the virtual world of computer.
3. True or False
   a. Cybercrime involves physical force.
   b. One should avoid disclosing personal data or details on social networking sites.

1.5. REFERENCES

Prevention of Cyber Crimes and Fraud Management by Indian Institute of Banking and Finance, Mumbai, 2017.

Cybercrimes by Talat Fatima, Eastern Book Company, Lucknow, 2011.

Cyber Law in India by Dr. Farooq Ahmad, New Era Law Publications, 2008.

1.6. SUGGESTED READINGS

Cyber Law by Anirudh Rastogi, LexisNexis, Gurgaon, 2014.

Textbook on Cyber Law by Pavan Duggal, Universal Law Publishing Co., New Delhi, 2014.

1.8. TERMINAL QUESTIONS AND MODEL QUESTIONS

a. Discuss in detail the concept of cybercrime and also discuss the channels of cybercrime.
b. Write an explanatory note on the causes and effects of Cybercrime. Also discuss the preventive measures to combat cybercrimes.

Answers

1. a. refer 1.1.1 b. refer 1.3.10.
2. Illegal, target or tool b. Cyberspace
3. a. False b. True

TERMINAL QUESTIONS AND MODEL QUESTIONS

a. 1.3.11. b. 1.3.9., 1.3.14. & 1.3.15.

UNIT-2

CRIME IN CONTEXT OF INTERNET-ACTUS REA/MENS REA

2.1. INTRODUCTION

There are two components of crime generally. These are actus reus and mens rea, with certain exceptions. It is the general principle of criminal law that no person is to be convicted of an offence unless it is proved beyond reasonable doubt by the prosecution that his conduct is prohibited by criminal law. Further, it is to be proved that he is liable for the same and also that he had a defined state of mind in relation to the commission of the crime. Actus Reus means the act or omission which is prohibited by law. There must be commission or omission to constitute a crime. As far as mens rea is concerned, it means guilty state of mind. The mental element constitutes the other vital ingredient of crime. Almost all the crimes require proof of mental element of some sort. As far cybercrime goes it is very difficult to determine the mens rea in cybercrimes. Actus Reus in cybercrimes has become a challenge as the entire act is committed in intangible surroundings. There may be certain marks left on the electronic device or computer but it is almost impossible for the law enforcement machinery to prove it in the courts, as it is required to be in physical form or at least in such a form where it becomes admissible in evidence.

2.2. OBJECTIVES

The study of this chapter will make students understand

- The components of cybercrime.
- the methods and modus operandi for crimes on internet.
- Issues and challenges regarding crimes on internet.

2.3. SUBJECT

2.3.1. WHAT IS THE INTERNET?

The word 'Internet' is a contraction between the words of international and networks. It is a vast worldwide network of powerful computer sensors which are constantly connected to each other via high-speed communication cables. This clearly states that nobody is a single owner. When you connect to the Internet, you connect to just one of these computers, but it is able to give you access to all the files stored on the other servers. whenever you connect to the internet by dialling to your Internet Service Provider (ISP) using your modem, you become the part of the network. The ISP is the link between the internet backbone, which connects the entire data route, and the user. Internet connection is also called going on-line or dialing-up. Internet is, therefore, a virtual space in which users send and receive e-mail, log in to remote computers, browse- databases information and send and receive programmes contained in these computers.

The Internet has changed the facets of transactions in every sphere of life and is undoubtedly a very potent source of information. Internet provides easy and cheap access to a vast reservoir of information and entertainment. It has transformed the nature of commerce and Government everywhere across the globe. However, there is one major demerits of use of internet which is a considerable hike in the number of crimes on internet.

Crime on the Internet takes place in many forms like hacking, viruses, fraud, scams, money laundering, industrial espionage, prostitution, certain forms of gambling, drug use, drug smuggling, suicide assistance, abetting crimes, defamatory allegations, cyber stalking, cyber terrorism and actual terrorism.

2.3.2. Actus reus

Actus reus includes act or omission on the part of wrongdoer. It is the act or series of actions which constitutes crime. The actus reus of cybercrime is very dynamic and diverse. For e.g. when with a keyboard and mouse one start functioning with computer, when one is attempting access to information on other's computer without the consent or approval of the authorized person, when is one attempting for hacking, flowing viruses, to commit cybercrime and actually caused those acts etc. these are human conduct or actus reus in cyberspace which law seeks to prevent i.e. they are actus reus of cybercrimes.

2.3.3. Actus reus in cybercrimes

Actus reus in cybercrimes has become a challenge as the entire act is committed in intangible surroundings. The perpetrator may leave some footmarks in the machine itself though it becomes a tough task for the law enforcer to prove it in the court of law. It is required to be in

physical form or at least in such form it becomes admissible. In relation to the computer any of the following actions are regarded as actus reus.

1. Trying to do some act using the computer.
2. Either attempting to access data stored on a computer or from outside through the said computer.
3. Every time the computer is used by its user while gaining access, signals pass through various computers which are made to perform some functions when the command given by the user pass through it. Each such function falls under the term "actus reus". Even failed attempts to log in constitute an act and hence, actus reus.

2.3.4. Mens rea

Mens rea is another essential element of cybercrime. 'Mens rea' refers to the 'mental element of an offence' and is an essential element of a crime. There is a well-known maxim called Actus non facit reum, nisi mens sit rea which means the action alone is not sufficient to constitute crime unless there is a guilty intention behind it. Till 12th century, only for actus reus a person could be held liable for any injury without proof of mens rea or blameworthy state of mind. In modern Common Law this concept has been changed and now guilty mind is the essential element for crime commission and imposition of penalty. The term 'mens rea' is not used and defined in the Indian Penal Code, 1860. However, the use of words like fraudulently, dishonestly, knowingly, recklessly, intention etc. represents mens rea. E.g. while committing hacking, the hackers have knowledge or intention of unauthorized access and thereby commission of cybercrime.

2.3.5. Mens Rea in cybercrimes

Cyber-crimes being different from the conventional crimes as they are committed in the electronic medium; mens rea is not a requirement but is rather a general rule under the penal provisions of the IT Act. The element of mens rea in Cyber-crimes is that the offender must have been aware at the time of causing the computer to perform the function that the access thus intended to be secured was unauthorized.

2.3.6. Modus Operandi of Cybercrimes

The internet has changed the subject matter of crime and more importantly its modus operandi. The entire criminal act consist of automated machines and the human hand is only at the starting or ending points. This makes the challenge formidable. The challenges posed before the criminal system is mainly due to the following reasons.

1. The transnational nature of cybercrimes where geographical regions and international boundaries have lost their meaning and a single criminal act passes through a number of jurisdictions.

2. The ever-extending nature of the internet and the backwardness of the present criminal law has rendered the law helpless and unresponsive.

3. The technicality involved in cybercrimes makes investigation a highly complicated and purely technical job.

Cybercrimes are crimes of digital age. They are bloodless, nonviolent types of crimes which are committed by computer literate persons whose ways and methods of committing crime is highly sophisticated and technical. Most of the cyber-crimes are committed by a good number of accomplices called “outsiders” and “insiders” who are the workers of communication and internet Service Company. Modus operandi is a system of actions of the criminal (and/or related persons) united by one intention directed on preparing, committing and covering up of the time determined by objective or subjective factors and connected to use of corresponding facilities and means. Modus operandi of committing cyber-crimes mainly involved illegal interference in computer system and network operations. Such illegal interference can be divided into various groups.

2.3.6.1. Ways of Direct Access

This covers damaging, deletion, deterioration, suppression or copying of computer data and includes unauthorised hindering of computer, computer system, or network functioning by inputting corresponding commands from the computer where information is restored. Such direct access can be made both by persons working with data and as well by persons intentionally penetrating in restricted areas or premises where information is restored. However, due to decentralisation of information processing, direct access is decreasing and the preparator finds it easier to intercept computer information during its transfer via telecommunication channels or computer networks. The perpetrator may also restore and examine erased software.

Direct access includes methods of direct and electromagnetic interception of computer data. Data interception is the simplest way of access without right. Interception is made through external communication channels, or by way of direct connection to cables of peripheral devices.

Electromagnetic interception is done through latest technical devices which allows obtaining information directly without being connected to computer system. As a result of emissions, interception of central processors, display, communication channels, printers, etc. is possible. Bugs is one of the most popular electromagnetic interception. These bugs are sensitive microphones designed for listening to conversations of attendants.

2.3.7.2. Ways of Indirect Access

Ways of indirect access includes access without right to certain computer or information system via computer networks from the computer located at certain distance. Following are the ways of indirect or remote distance:

1. Connecting to telecommunication cables of authorised user and obtaining access to his system. Penetrating in other information system by automated picking out of phone numbers of subscribers with further connection to their computers.
2. Penetrating in computer networks with the help of passwords, pretending to be an authorised user is yet another way to obtain access. By using this method, violators crack passwords with the intention to access other computers.

2.3.7.3. Mixed Methods

These methods consist of both direct and indirect access. These are

1. Secret insertion of commands in programs that allow the performance of new unplanned functions, making this program workable.
2. Alterations of programs by way of secret placing of command sets that should come into action under specific conditions and in a given time. Thus, as soon as the program illegally transfers money funds to so called false account, it will self-destruct and delete all the data on the committed operation.
3. Access is obtained to databases and files of the authorised user through weak places in security systems. This gives an opportunity to read and examine information stored in the system and copy it.
4. Mixed methods also include using of bugs in programs and files. The program is called "breaking" and malefactor inputs of certain commands that help to perform new unplanned functions making this program runnable. Thus, one may transfer money to false accounts, obtain information on real estate, identities etc.
5. Hackers may obtain passwords, keys, IDs and penetrate in computer system as authorised users. Systems with no authorised authentic identification (fingerprints, eye retina, and voice) are especially invulnerable in this relation.

The changing nature of modus operandi which keeps evolving with technological advancements is a continuous challenge for controlling cybercrimes.

2.3.7. Data Crime

Data Interception: An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream. Unlike some other data leakage attacks, the attacker is observing explicit data channels (e.g. network traffic) and reading the content. This differs from attacks that collect more qualitative information, such as communication volume, not explicitly communicated via a data stream. Data Modification Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites. In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. An example of this is changing the dollar amount of a banking transaction from $100 to $10,000. In a replay attack, an entire set of valid data is repeatedly interjected onto the network. An example would be to repeat, one thousand times, a valid $100 bank account transfer transaction.

Data Theft is the term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or

other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law.

2.3.8. Network Crime: Network Interferences

Network Interfering with the functioning of a computer Network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Network data. Network Sabotage 'Network Sabotage' or incompetent managers trying to do the jobs of the people they normally are in charge of. It could be the above alone, or a combination of things. But if Verizon is using the help of the children in hindering first responders' line then they might be using network problems as an excuse to get the federal government to intervene in the interest of public safety. Unions and strikes anyway go in vain if the federal government forces these people back to work.

2.3.9. Access Crime: Unauthorized Access

"Unauthorized Access" is an insider‘s view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality. Virus Dissemination Malicious software that attaches itself to other software. (Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim.

2.3.10. Related Crimes: Aiding and Abetting Cyber Crimes

There are three elements to most aiding and abetting charges against an individual. The first is that another person committed the crime. Second, the individual being charged had knowledge of the crime or the principals' intent. Third, the individual provided some form of assistance to the principal. An accessory in legal terms is typically defined as a person who assists in the commission of a crime committed by another or others. In most cases, a person charged with aiding and abetting or accessory has knowledge of the crime either before or after its occurrence. A person who is aware of a crime before it occurs, and who gives some form of aid to those committing the crime, is known in legal terms as an "accessory before the fact." He or she may assist through advice, actions, or monetary support. A person who is unaware of the crime before it takes place, but who helps in the aftermath of the crime, is referred to as an "accessory after the fact". Computer-Related Forgery and Fraud Computer forgery and computer-related fraud constitute computer-related offenses. Content-Related Crimes Cybersex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses. The total cost to pay by victims against these attacks is in millions of millions Dollar per year which is a significant amount to change the state of un-developed or underdeveloped countries to developed countries.

2.3.11. Common Types of Cyber Attacks

Cybercriminals use a number of attack vectors to carry out their cyberattacks and are constantly seeking new methods and techniques for achieving their goals, while avoiding detection and arrest. Here are common types of attacks cybercriminals have been known to use:

Distributed DoS attacks (DDoS) are often used to shut down systems and networks. This type of attack uses a network's own communications protocol against it by overwhelming its ability to respond to connection requests. DoS attacks are sometimes carried out simply for malicious reasons or as part of a cyberextortion scheme, but they may also be used to distract the victim's organization from some other attack or exploit carried out at the same time.

- Infecting systems and networks with malware are used to damage the system or harm users by, for example, damaging the system, software or data stored on the system. Ransomware attacks are similar, but the malware acts by encrypting or shutting down victim systems until a ransom is paid.
- Phishing campaigns are used to infiltrate corporate networks by sending fraudulent email to users in an organization, enticing them to download attachments or click on links that then spread viruses or malware to their systems and through their systems to their company's networks.
- Credentials attacks, where the cybercriminal aims to steal or guess user IDs and passwords for the victim's systems or personal accounts, can be carried out through the use of brute force attacks by installing key sniffer software or by exploiting vulnerabilities in software or hardware that can expose the victim's credentials.
- Cybercriminals may also attempt to hijack a website to change or delete content or to access or modify databases without authorization. For example, an attacker may use an SQL injection exploit to insert malicious code into a website, which can then be used to exploit vulnerabilities in the website's database, enabling a hacker to access and tamper with records or gain unauthorized access to data, such as customer passwords, credit card numbers, personally identifiable information (PII), trade secrets, intellectual property and other sensitive information.

Cybercriminals often carry out their activities using malware and other types of software, but social engineering is often an important component for executing most types of cybercrime. Phishing email is an important component to many types of cybercrime, but especially so for targeted attacks, like business email compromise (BEC), in which the attacker attempts to impersonate, via email, a business owner in order to convince employees to pay out bogus invoices.

2.4. SUMMARY

In traditional crimes, actus rea and mens rea are two essentials of any crime with certain exceptions in few cases. Actus rea in these types of offences is generally determinable. But the difficulty arises when it comes to the cybercrimes. The modus operandi of criminal in cybercrimes is always different from a normal and conventional crime. Due to rapid growth of technology, absence of territorial limits and any physical surroundings and modus operandi of changing methods adopted by the cyber criminals it becomes a great challenge for law enforcement agencies to control and curb these illegal activities.

2.5. SAQS

1. Short Answer Questions

a. Write a short note on 'Mens Rea' in case of cyber-crimes.

b. What are the different ways of indirect access to certain computer or information system via computer networks from the computer located at certain distance.

2. Fill in the blanks

a. The fundamental difference between a cyber crime and a traditional crime is that in cyber crime a ……is used.

b. The path or tool through which an attack came to the system is called……

3.True or False

a. The Data Theft is the term used to describe when information is illegally copied or taken from a business or other individual

b. A front end server which hides the IP address or the domain name in a front-end address in the network is called Proxy Server.

2.6. REFERENCES

Prevention of Cyber Crimes and Fraud Management by Indian Institute of Banking and Finance, Mumbai, 2017.

Cybercrimes by Talat Fatima, Eastern Book Company, Lucknow, 2011.

Cyber Law in India by Dr. Farooq Ahmad, New Era Law Publications, 2008.

2.7. SUGGESTED READINGS

Cyber Law by Anirudh Rastogi, LexisNexis, Gurgaon, 2014.

Textbook on Cyber Law by Pavan Duggal, Universal Law Publishing Co., New Delhi, 2014.

2.8. TERMINAL QUESTIONS AND MODEL QUESTIONS

a. Write a detailed note on Modus Operandi of criminals in cybercrimes.

b. What are the essentials of cybercrime? Discuss various types of cyber attacks with the help of relevant examples.

Answers

1. a. refer 2.3.5. & 2.3.6. b. refer 2.3.7.2.

2. a. Computer or such an electronic device b. Threat Vector

3. a. true b. true

TERMINAL QUESTIONS AND MODEL QUESTIONS

a. refer 2.3.7.

b. refer 2.3.4., 2.3.6. & 2.3.12.

UNIT–3

TYPES OF CRIME IN INTERNET

3.1. INTRODUCTION

Internet has grown at a rapid pace paving way to new opportunities in various fields like education, business, entertainment, sports etc. In today's scenario the internet serves as a great mediator of our lives. A statistical data infers that nearly 3, 405518,376 people surf net in a day all-round the globe. This swift growth of technology has its own merits and demerits. One such major disadvantage is cybercrime, a latest and perhaps the most complicated issue in cyber world. Deceits who are experts in the field use the technology for erroneous purpose for personal benefits. Cybercrimes have become a great threat of the hour and can be committed even from a remote location single handedly and does not require the physical presence of the criminal who is involved in the act. Progress in the field of e-commerce and online transactions and increased use of plastic money are now being exploited by cyber criminals.

3.2. OBJECTIVES

The study of this chapter will enhance the student's comprehension on

- The various categories of cyber crime
- Kinds of Cyber crimes
- Impact of cyber crime

3.3. STRUCTURE

3.3.1. Categories of cyber crime

Cybercrimes can be classified under three major categories namely

Cyber-crimes against individual

Cyber -crimes against property

Cyber -crimes against government

3.3.1.1 Cyber-crimes against individual

Cyber-crime against an individual is where an individual is targeted in the form of cyber stalking, trafficking or distributing pornography. In current scenario cyber-crime against an individual is taken seriously and measures like implementation of stringent laws and creating awareness on cyber law amidst the masses and strict action against the perpetrators is being exercised.

3.3.1.2. Cyber -crimes against property

As Criminals in real world involve in theft and robbery, here in cyberworld criminals indulge in activities like vandalism of computers, online threatening, intellectual property crime, siphon of money or misuse of credit cards etc. Just as delinquents harm property in the real world,

here malicious software is used to gain access to an organization's website or to intrude into their confidential data.

3.3.1.3. Cyber -crimes against government

Unlike other categories, cybercrime against a government is very uncommon and is termed as cyber terrorism. This is a heinous crime which can disrupt and create panic in the life of civilian population. In this case the criminals hack government websites, military websites or circulate propagandas against the government. These perpetrators can be under the cover of unfriendly government agencies from other nations or terrorists.

3.3.2. Kinds of cybercrime

3.3.2.1. Hacking or unauthorized access

Trespassing in real world simply means entering into property owned by others without his or her permission. Similarly, hacking means unauthorized access to a computer system with an intent to know or cause wrongful loss or damage to the public or any individual. This is an illegal intrusion or breaking into a computer network done for personal monetary benefits where information related to credit cards or bank accounts are hacked. Unauthorized hackers attempt to gain access to vital information system or possess a desire to destruct the system. Hacking is a crime even if there is no visible damage to the system, as it is an invasion into the privacy of data. Hackers are again of different classes, where *White Hat Hackers* just hack to exhibit their expertise, whereas *Black Hat hackers* cause damage after intrusion by inserting viruses or modifying the data. Another class of hackers called *Grey Hat Hackers* are typically ethical but occasionally violate hacker ethics.

3.3.2.2. Web Hijacking

In the case of web hijacking there is a forceful control of others websites and the individual lose control over his website and its content. Here the attacker creates a fake website and when the victim opens the link a new page appears with an information requesting to click another link. Once clicked they will be redirected to a fake page and this is done to get control over the site of another.

3.3.2.3. Pornography/Child Pornography

Pornography means screening sexual acts to induce sexual excitement in an individual. Pornography includes pornographic websites, pornographic magazines produced using an internet pornography delivered over mobile phones. Children are an easy prey in the cybercrime as Internet is being highly used as a medium to cause sexual abuse. Pedophiles trap children using false identity and lure them by offering monetary benefits or falsely promising them for a better life opportunity. They create videos depicting children engaged in sexually explicit act or picturing them in obscene or indecent manner. Later on, these pedophiles exploit the children by using them as sexual objects or sell the pornographic pictures over the internet.

3.3.2.4. Cyber Stalking

The term 'Stalking' means repeated acts of harassment where the victim is followed or receives harassing phone calls or vandalizing the victim's property or even extends to cause physical harm to the individual. Similarly in Cyber Stalking the victim is repeatedly harassed or threatened by the cybercriminal through any means of internet services. Here the personal information like name, phone numbers of residence and workplace, date of birth etc., of the victim is gathered through various sources which the victim have filled in while creating an account in e-mail or any other social sites. At times this information is subscribed to innumerable pornographic and sex sites where the victim is constantly harassed by unsolicited e- mails and prank calls. Stalkers contact their victims through e-mails or telephone to threaten or harass them.

3.3.2.5. Virus attacks

Viruses are malicious programs that can gain access to other electronic device without the permission of the victim and interrupt the smooth functioning of other programs. They disrupt the smooth functioning of the data on a computer either by altering or deleting it. Programs that multiply and spread from one computer to the other are called as worms. Virus, worms, Trojan horse, Time bomb, Logic bomb, Rabbit and Bacterium are malicious. Trojan horse is one of the common but the most dangerous program that acts to be legitimate but ends up doing things that are quiet damping. Trojans come in two types as a Client part and a Server part. When a victim unknowingly uses this server, the attacker uses the client to connect to the server and start using the Trojan. The usual protocols used for communications are TCP/IP and UDP.

Denial of Service attack is another issue in which the victim's e-mail box is filled with spams depriving him of the services he is entitled to. In this kind of attack the network is flooded with useless traffic leading to its crash.

3.3.2.6. Logic Bombs

Generally, viruses are to be activated to perform the desired destructive action. A Logic bomb is a consciously inserted code of application to perform the security-comprising actions and makes the system unusable. A virus may remain dormant when untouched, but becomes active when they receive the required push. Such viruses which activate at a desired time and date are called time bombs and that which is stimulated on happening of some events are called logic bombs. This is sometimes used by vendors to ensure payment as the system will not work unless the bomb is deactivated. Logic bomb is similar to other viruses, except that it goes off at the will of the person.

3.3.2.7. Software Piracy

Software piracy is illegal copying or unauthorized distribution of software intended to pass

for the original. These types of crimes come under trademark violations, copyright infringement, patent violations, theft of computer source code etc. Some common types of software piracy include counterfeit software, Hard-Disk loading, Internet software piracy, etc. Domain names are also trademarks protected by ICANN domain dispute resolution policy and also under trademark laws. Cyber criminals create a domain name identical to popular service providers name to attract maximum number of uses and gain profit out of it.

3.3.2.8. Salami Attacks

Salami attacks, otherwise called as Salami slicing is where attackers use an online database to acquire the customer's information like bank details, credit card details etc. Here the alteration is done in such an insignificant way that when done once it can completely go unnoticed. For example, where the attacker deduces a very minimum amount from the account over a period of time. In this kind of attack the hacker remains free from detection as the clients are even unaware of the slicing.

3.3.2.9. Phishing

Phishing is the act of sending an e-mail to a user projecting to be a legitimate enterprise in a venture to scam the user into surrendering private information that will be used for identity theft. An e-mail is sent to the user where he/she is directed to update personal information like passwords, credit card, social security, bank account number details etc. Such bogus websites are used to steal information and siphon money in a fraudulent way.

3.3.2.10. Cyber defamation

Cyber defamation is where a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to his friends and acquaintances. It is an individuals' right to protect his reputation. A public right to freedom of speech and expression guaranteed under Article 19(1) (a) of the Constitution of India makes enforcement of our private right a challenge. The law of defamation has been designed to protect the reputation of an injured person and provide such balance between private and public rights by giving him the right to sue for damages. Defamation comprises of both libel (defamation by means of writing) and slander (defamation by speaking). With the advent of information technology and the internet libel has become much more common and of course, easier. There are two types of defamation like online and offline, where online defamation is said to be more quantitative and vigorous.

3.3.2.11. Email bombing

This is a type of net abuse where huge number of emails are sent to an email address in-order to flood the mail box or to flood the server where the email address is leading to its crash.

Theft of information and Internet time

Theft of information includes stealing personal details of an individual from a computer hard disk, or any removable storage device. Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.

3.3.2.12. Breach of Privacy

Breach of privacy means unauthorized use or distribution or disclosure of personal information. Privacy refers to the right of an individual to determine when, how and to what extent his or her personal data will be shared with others. Confidentiality means non-disclosure of information to unauthorized or unwanted persons. In addition to Personal information some

other type of information which is useful for business and leakage of such information to other persons may cause damage to business or person and such information should be protected.

3.3.2.13. Data diddling

This computer crime relates to operation security and can be minimized by building strong internal security controls. This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed. This is a simple and common computer related crime which involves changing data prior to or during input process in a computer. Data can be changed by anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transporting computer data.

3.3.2.14. E- commerce frauds

An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. This type of fraud includes misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

3.3.2.15. Cyber Terrorism

Cyber terrorism is an attractive option for modern terrorists for several reasons. It is cheaper than traditional terrorist methods. Cyber terrorism is more anonymous than traditional terrorist methods. The variety and number of targets are enormous. Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc. Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists. Cyber terrorism has the potential to affect directly a larger number of people.

3.4. Measures to tackle cyber Crime

It has been seen that most cyber criminals have a loose network wherein they collaborate and cooperate with one another. Unlike the real world, these criminals do not fight one another for supremacy or control. Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals. While law enforcement agencies are trying to keep pace with cyber criminals, it is proving to be a Herculean task.

Below mentioned security guidelines could be adopted to minimize the security risk of cybercrime:

3.4.1 Updating the computers

Computers should be updated with latest patches to keep attackers away. While keeping your computer up-to-date will not protect you from all attacks, it makes it much more difficult for hackers to gain access to your system, blocks many basic and automated attacks completely,

and might be enough to discourage a less-determined attacker to look for a more vulnerable computer elsewhere. Choose strong passwords and keep them safe.

3.4.2 Safeguarding Personal information

Be cautious while sharing personal information such as one's name, home address, phone number, and email address online. In order to avail many online services, it is inevitable to provide personal information in order to handle billing and shipping of purchased goods.

Since not divulging any personal information is rarely possible, the following list contains some suggestions for how to share personal information safely online.

No entertainment of phony email messages. Things that indicate a message may be fraudulent are misspellings, poor grammar, odd phrasings, Web site addresses with strange extensions, Web site addresses that are entirely numbers where there are normally words, and anything else out of the ordinary.

No response to email messages that ask for personal information. Genuine organizations will not use email messages to ask for your personal information. When in doubt, contact the company by phone or by typing in the company Web address into your Web browser. Don't click on the links in these messages as they may take you to fraudulent, malicious Web sites.

Pay attention to privacy policies on Web sites and in software. It is important to understand how an organization might collect and use your personal information before you share it with them.

Guarding email address. Spammers and phishers sometimes send millions of messages to email addresses that may or may not exist in hopes of finding a potential victim. Responding to these messages or even downloading images ensures you will be added to their lists for more of the same messages in the future. Also be careful when posting your email address online in newsgroups, blogs or online communities.

The first step toward keeping passwords secure and away from the wrong hands is to create strong passwords having eight characters or more and use a combination of letters, numbers and symbols (e.g., # $ % ! ?). Avoid using any of the following as your password: your login name, anything based on your personal information such as your last name, and words that can be found in the dictionary. Try to select especially strong, unique passwords for protecting activities like online banking. Change passwords on a regular basis, at least every 90 days. This can limit the damage caused by someone who has already gained access to your account. If you notice something suspicious with one of your online accounts, one of the first steps you can take is to change your password.

Protect your computer with security software like firewall and antivirus programs which are necessary for basic online security. These software monitors all online activities such as email messages and Web browsing and protects an individual from viruses, worms, Trojan horse and other types of malicious programs. The antivirus and antispyware software you install should be configured to update itself, and it should do so every time you connect to the Internet.

Bank and credit card statements should be reviewed on a regular basis. The impact of identity theft and online crimes can be greatly reduced if user can catch it shortly after their data is stolen or when user gets symptoms.

3.5 Cyber Crime in current scenario

Cybercrime such as credit card thefts and online money-laundering is on a high rise and has thrown light on the hazards of e-commerce and online shopping. Cyber terrorism, hate-mail cases, Zenophobia are some of the prominent cybercrimes prevailing across the globe. Unauthorized hacking, online infringement of music, videos, Fake escrow scams and software also play a prominent role in Cybercrime.

Cyber security being one of the biggest challenges in today's scenario, majority of big crimes today like counterfeiting, terrorism, piracy, privacy etc. are somewhere connected to the cyberspace in one way or the other. India also is very vulnerable and exposed to the cyber-attacks in recent times. The reason behind this are the inherent vulnerabilities that are difficult to be removed, innumerable entry points on the internet, misdirected attribution to the third parties and the fact that attack technology which is consistently outpacing the defence technology.

India is trying to implement the Digital India project to the best of its capabilities. The success of Digital India project would depend upon maximum connectivity with minimum cyber security risks. This can be a challenge for India as India has a poor track record of cyber security.

3.6 Impact of Cybercrime on businesses

Nearly all businesses are operating online as it is very easy to grab customers through digital marketing and hence are vulnerable to devious criminal practices that takes place online.

Due to technological advance which grows at a rapid pace, almost any size of company takes the advantage of Internet. In this scenario it is very vital to fight cyber-crime though it is expensive. The cyber security which we use should be an updated one suiting to evolving threats and methods that emerge.

The objective behind an electronic breakthrough can be to steal any vital information related to the company's business, to monitor the company's online activity or to track down customer details etc. In order to be impervious to cybercrime it is a must to keep our software updated and run security checks on a regular basis. Such practices can improve the longevity and success of our business.

3.7. Cybercrime Prevention strategies

Cybercrime is considered to be one of the most dangerous threats in recent days, as it has a serious impact on every aspect of the growth of a country. Cyber criminals are focused on easy money-making means and target any Government, private or non-profit organizations. Creating awareness and adopting basic security precautions could be the best defense against cybercriminal activities.

Some measures to mitigate the risks of cybercrime:

- The windows or browsers used should be closed completely by using the "sign out" or "log out" button. Never click on the option 'remember' username or password.
- Backup of all important personal and professional details should be created.
- Create strong passwords with combinations of upper case, lowercase, numbers and special characters. Passwords should be changed frequently.
- No exposure personal information on Social Networking sites.
- Personal computers should be preferred for any kind of online transactions.
- Internet security software should be installed mandatorily.
- Not to open any links sent to your mail as cybercriminals use e-mail as the prominent target to gather personal information. However, that website could be accessed by typing the address in the menu bar.
- There should be strict guidelines and notifications issued by the IT department to keep a check on criminal activities related to cyberspace.

3.8. SUMMARY

Cybercrime has become a great menace in the life of mankind. Unlike ordinary crimes these cybercrimes could be committed even from a remote locality by any individual. There must be a constant evolution in cyber law to match the dynamism of technology. Protection or adopting a latest and proliferate security measures and implementing stringent laws is vital for the security aspect of a country. Academic institutions play a major role in creating awareness about the legislation and policy development, delivery of technical assistance among the internet users.

3.9. SAQS

1. Short Answer Questions
   a) What can be the different categories of cybercrime?
   b) Write a short note on cyber terrorism.
2. Fill in the Blanks
   a) _____is illegal copying or unauthorized distribution of software intended to pass for the original.
   b) _____is where a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to his friends and acquaintances.
3. True or False
   a) It is essential to create a backup of all important personal and professional information.
   b) Denial of Service attack is an issue in which the victim's e-mail box is filled with spams depriving him of the services he is entitled to.

3.10. REFERENCES

Prevention of Cyber Crimes and Fraud Management by Indian Institute of Banking and Finance, Mumbai, 2017.
Cybercrimes by Talat Fatima, Eastern Book Company, Lucknow, 2011.
Cyber Law in India by Dr. Farooq Ahmad, New Era Law Publications, 2008.

3.11. SUGGESTED READINGS

Textbook on Cyber Law by Pavan Duggal, Universal Law Publishing Co., New Delhi, 2014.
Cyber Law by Anirudh Rastogi, LexisNexis, Gurgaon, 2014.

3.12.TERMINAL QUESTIONS AND MODEL QUESTIONS

a) Briefly discuss any five kinds of Cyber-crimes.
b) Discuss the impact of Cybercrime on business.

ANSWERS

1. a. refer 3.3.1 b. refer 3.3.2.14
2. a. Software piracy b. Cyber defamation
3. 3. a. true b. true

TERMINAL QUESTIONS AND MODEL QUESTIONS

a. Refer 3.3.2 b. 3.6

UNIT-4

COMPUTING DAMAGE IN INTERNET CRIME

4.1. INTRODUCTION

Cybercrimes are of various types as discussed in previous units. The Modus operandi differs according to the type. It also depends on the capability of the criminal circumstances of the case, vulnerabilities in the system i.e. opportunities provided by the system itself. A computer system or a computer network may be harmed by the attacker by using certain techniques. The

advancement in the field of cybercrime has made administrators take serious steps to protect the system from unauthorized access or virus attacks.

4.2. OBJECTIVES

The study of this chapter will make students understand

- The concept of computing
- the methods and kinds of computing
- Classification of virus and worms.

4.3.1. Definition of Computing

Computing Is where a task is accomplished by using computer technology. This can be a computer hardware or a computer software, but must involve some form of a computer system. Computing is used on a daily basis for day-to-day activities without even the individual realizing it. We use computing in the form of sending an e-mail, using credit cards, online payments using debit cards, using of cell phones etc.

4.3.2. Software related Crimes

In software related crimes the system as well as the application software are corrupted by some means. This is highly sophisticated means of crime where the existing program in a computer is changed by inserting new programs and is difficult to detect. This is usually carried out by system analysts and other experts who are involved in commissioning or making alterations in the software. These are new crimes created with the internet itself. Such as hacking, and planting viruses. Software-related crime could be perpetrated by using various techniques like computer viruses, computer worms, Trojan horse, trap door, super zapping, wire-trapping, time bombs, logic bombs, and salami attacks etc.

4.3.3. Computer as a target

A computer or a computer network becomes a victim when it is targeted and the computer's confidentiality, integrity, or accessibility is attacked. Here the victim is crippled when the information stored or the service provided by the victim is stolen or damaged. This includes disrupting the functioning of the computer, theft or disturb data or information; corrupt the operating systems and programmes; intellectual property violations and blackmail using personal information hacked from computer systems. This is done by spreading of viruses.

4.3.4. Computing Platform

A platform is a group of technologies that are used as a base upon which other applications, processes or technologies are developed. A computing platform is a digital platform where a software is executed. It may include a hardware, an operating system (OS), web browser and associated application programming interfaces. A computing platform is a stage on which a computer program is operated. They provide computational capabilities to apply methods and models to geographic data. Depending upon the needs and data-processing workloads of the user, the price and capability varies from mobile devices to advanced supercomputers and from

standalone computers to complex networked infrastructure. A desktop computer with Microsoft Windows installed on it can be an example for a computer platform.

4.3.5. Types of Computing

4.3.5. 1. Cloud Computing

Cloud computing is a computing paradigm shift where computing is moved away from a desktop or a personal computer of an individual to an application server or a 'cloud' of computers. This method of computing is done through pooling of all computer resources together and is being managed by a software rather than a human.

4.3.5. 2. Grid Computing

They are multiple independent computing clusters which act like a grid because they are composed of resource nodes not located within a single administrative domain. It offers online computation or storage as a metered commercial service, known as utility computing, computing on demand or cloud computing.

4.3.5. 3. Utility Computing

Utility computing is a conventional internet hosting services which have the capability to quickly arrange for the rental of individual servers. This usually envisions some form of virtualization in which the storage or computing power available is considerably larger than that of a single time sharing.

4.3.5. 4. Distributed Computing

In this method of computer processing different parts of a program are run simultaneously on two or more computers that are communicating with each other over a network. Each computer has one more processor and other resources connected to local computer so that the user can access resources on the remote computers via network. World Wide Web is an example for this.

4.3.5. 5. Cluster Computing

Cluster computing is a set of processors in parallel configurations where resources are allocated by centralised resource manager and scheduling system. The objective of using cluster computing is to achieve high performance, reliability or high computing throughout by a set of interconnected computers.

4.3.5. 6. Parallel Computing

Parallel computing or parallel processing is a process where multiple processors are used at the same time to execute a single program. This can be executed only when the program is split into many pieces so that each function is performed by a single CPU. A single computer having multiple CPUs can be utilised for solving computing-intensive problems and is used in the field of biology, airspace and semiconductor design etc.

4.3.6. Concept of Computer Virus/ Creation

VIRUS stands for - Vital Information Resources under Siege. A computer virus is a computer program that can spread across computers and networks by making copies of itself, usually without the user's knowledge. 'Virus' is actually a generic term for software that is harmful to your system. All computer viruses are manmade and here the person has to write the code and test it to make sure it spreads properly before releasing it. Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. A simple virus is dangerous because it will quickly use all available memory and bring the system down. Some viruses display symptoms, and some viruses' damage files and computer systems, but neither symptoms nor damage is essential in the definition of a virus; a non-damaging virus is still a virus. There are computer viruses written for several operating systems including DOS, Windows, Macintosh, UNIX, and others. The first subroutine, infect-executable, is responsible for finding available executable files and infecting them by copying its code into them. The subroutine do-damage and is also known as the payload of the virus which is the code responsible for delivering the malicious part of the virus. A well-written virus contains code to infect programs and will not cause any damage to our system. The last subroutine, trigger-pulled checks if the desired conditions are met in order to deliver its payload Generally, the destructive part of a virus is programmed to execute when certain conditions are met, usually a certain date, day, time, or number of infections.

4.3.7. Stages of Virus

On the basis of function and working methodology stages of viruses are structured under four phases. The first stage is the creation stage where virus is created by hackers or programmers with a malefic intention. Second stage is the replication stage, a technique used to spread viruses, where viruses create so many copies of itself or they are reproduced via nature and it regenerate themselves from one computer to another device. Next is the activation stage where a virus has to be activated to cause damage, otherwise they stay dormant and create hindrance only by stealing storage area. Viruses perform the function they have been targeted only when certain circumstances are met. This is followed by the discovery stage, which is a vital stage in the life of a virus. Discovery usually grasp minimal place, year before the virus power have become a threat to the computing association. Next in the assimilation stage the virus is detected and its activity is being vetoed. Lastly it ends up in the eradication stage where the user installs up-to date virus defence software and any virus can be erased out.

4.3.8. Integration of virus in a computer system

A virus is a small piece of code embedded in a larger, proper or regular program. Any virus is designed to run first when the proper or regular program gets executed. The virus loads itself into memory and looks around to see if it can find any other programs on the disk. If it can find one, it modifies it to add the virus's code to the unsuspecting program. Then the virus launches the "real program." It becomes very difficult for the user to know that the virus ever ran. Unfortunately, the virus has now reproduced itself, so two programs are infected. The next time either of those programs gets executed, they infect other program and the cycle continues. If one of the infected programs is given to another person on a floppy disk, or if it is uploaded to a web, then other programs get infected. This is how the virus spreads and gets assimilated into a computer system.

4.3.9. Classification of computer virus/Malware

Computer viruses are just a type of malicious software called Malware. Malware are designed to infiltrate damage and/or prevent the normal use of a computer system. They are commonly divided into number of classes, depending on the way in which it is introduced into the target system and the sort of policy breach which it is intended to cause. As it is hard to define malware in a proper way, it can also be difficult to classify malware into distinct categories. Malware is constantly evolving and is also combining different ideas and techniques. Payload is a collective term for the actions that a malware attack performs on the computer once it has been infected.

4.3.10. Worms

A worm is a type of virus and has properties similar to it. This is an independent computer program which multiplies itself to different computers on a network with the help of network. It means a worm is a self-carried and they don't want another program to circulate them. Computer worms are very dangerous as they pose a serious threat to the computer and its network security by reducing the speed and blocking the network. In system they also reduce the storage space in available memory. Computer viruses are similar to biological pathogens with respect to propagating and infecting and its technique. Worms have traditionally been categorized according to their dissemination medium. This kind of virus is proficient in quickly spreading across a Local Area Network (LAN) or even over the Internet. Usually, it spreads through shared resources, such as shared drives and folders. Once it infects a new system, it searches for potential targets by searching the network for other vulnerable systems. Once a new vulnerable system is found, the network virus infects the other system, and thus spreads over the network. Mobiles are affected mostly due to Network virus, because of increasing use of Bluetooth, infrared and internet. Network worms gets into mainstream only with emergence of high-speed network including cable-modems and large corporate networks with many often-unpacked PCs. Network worms are more difficult to disinfect as infections are often distributed among multiple sites and expose gross blunders in design of the network and/or configuration of desktops. Network worms are probably the most complex type of worms to fight and they often cause considerable panic in corporate environments.

Worms are of six types:

(i.) E-Mail worm

An e-mail worm spreads by using an e-mail message as the delivery vehicle. Here the worm's main executable file is included as an infected attachment to the e-mail, or it may be embedded as an object or script in the e-mail message. Once the e-mail worm has installed itself on the computer, it will typically use the infected system's local e-mail client to send out copies of the worm to other victims. Often, the people that the worm sends its copies to are those whose e-mail addresses are saved on the infected computer, in a data file or in the local e-mail client.

(ii.) Instance Messaging Worm

Similar to an e-mail worm, an IM-Worm uses instant messaging applications installed on the infected machine to send a message to everyone listed on the contact list. The message will usually contain a link to a site that will infect users who visit it. More rarely, the message may also include an infectious attachment. Instant Messaging is becoming a very popular form of communication both for personal use and business use. Due to the popularity and convenience of Instant Messaging applications, many platforms for using this type of application have become available for PCs and mobile devices. While this is convenient for the users of IM, it also increases the possibilities for malicious attacks and security breaches.

(iii.) Internet Worm

Internet-worms can transmit themselves from a remote location on the Internet directly onto a computer. These worms are designed to exploit vulnerability in a
Computer system that allows them to gain entry. To find their victims, these worms scan the Internet for vulnerable machines. Once found, the worm can then simply download itself onto the computer, and then continue finding and infecting other victims.

(iv.) File sharing and peer-to-peer worm

Internet worms that use P2P vulnerabilities to propagate themselves in the network are called P2P worms. In P2P networks, the worm copies itself with multiple file names into the share directory of the infected host, thereby increasing the chance of being downloaded by the next victim which is now available in multiple file names. When the file is downloaded by the next victim the process of destruction is continued.

(v.) Flash worm

Flash worms are vulnerable hosts and that could possibly infect the whole vulnerable population in a few seconds. Flash worms follow a recomputed spread tree using prior knowledge of all systems vulnerable to the worm's exploit. Flash worm is supposed to have the list of all the possible targets prepared in advance so that no scan during the worm spreading time is necessary. Creation of such a worm requires considerable preparation efforts. Thus, the whole Internet has to be scanned in some way and the list of best initial targets is constructed. While this preparation procedure is quite expensive it can easily be accomplished by a government scale organization by a brute force scanning via a fast Internet link. This method, however, has a big limitation. Hosts behind firewalls cannot be scanned effectively.

(vi.) Hoaxes

Hoaxes are not viruses, but are usually deliberate or unintentional e-messages, warning people about a virus or other malicious software programs. Some hoaxes give as much trouble, the same as viruses, by causing massive amounts of unnecessary emails. Hoaxes can be as disruptive and costly as a genuine virus. If a user forwards a hoax warning to all their friends and colleagues, there can be a flood of email. This can overload mail servers and make them crash. The effect is the same as that of the real virus, but the hoaxer hasn't even had to write any computer code. Hoaxes can be remarkably persistent too

4.3.11. Trojan Horse

A Trojan horse program, or Trojan, is a program that performs actions which are unknown to and/or unauthorized by the user. Trojans take their name from the Trojan Horse of Greek mythology and just like the wooden horse in the story; a Trojan program 'disguises' itself to appear desirable or harmless, but secretly carries a dangerous payload. Any program that performs an action that hasn't been authorized by a user is called as a Trojan. A Trojan horse modifies and opens network connections, Install and run other programs on the computer, and Connect to and communicate with another computer or server. A legitimate program that performs a harmful action because of a bug in its coding or flaw in its design may also be considered a Trojan, at least until the problem is fixed.

4.3.12. Dangerous Virus attack

Virus attacks are not shocking news anymore. But here is the list of the worst of those attacks which shocked many at that time in history. The history of computer virus attack is as follow;

(A.) Jerusalem [1998] - This was the first MS-DOS virus that caused enormous destructions, affecting many countries, universities and company worldwide.

(B.) Morris [1998] - This computer virus infected over 6,000 computer systems in the United States, including the famous NASA research Institute, which for some time remained completely paralyzed.

(C.) Solar Sunrise [1998] – In 1998 using a computer virus, hackers, , penetrated and took control of over 500 computers systems that belonged to the army, government and private sector of the United States.

(D.) CIH [1998] - Unleashed from Taiwan in June of 1998, CIH is recognized as one of the most dangerous and destructive virus ever. The virus infected Windows 95, 98, and ME executable files and was able to remain resident in a PC‘s memory, where it continued to infect other executable.

(E.) Melissa [1999] - It was created by David L. Smith in 1999 and is based on a Microsoft Word macro. He intended to spread the virus through e-mail messages. The virus prompts the recipient to open a document and by doing so the virus gets activated.

(F.) ILOVEYOUILOVEYOU [2000] - It was a standalone program which was capable of replicating itself. The virus initially travelled through the e-mail, same way as Melissa virus. The email had a subject which says that the message was a love letter from the secret admirer. Attachment with this e-mail caused all the trouble.

(G.) Code Red and Code Red II [2001] – It was exploited operating system vulnerability found in Windows 2000 and Windows NT machines. A buffer overflow problem was the vulnerability. Due to this if the operating system receives more information than its buffers handling capacity; the adjacent memory will be overwritten. The original worm initiated a distributed denial of service attack to the White House website.

(H.) Nimda [2001] - It was spread through the Internet rapidly and became one of the fastest propagating computer virus. The Nimda worms aimed on the Internet servers and its real purpose was to slow down the Internet traffic.

(I.) The Klez Virus [2001] – It was appeared in late 2001 and infected a victim's computer through an e-mail message. The virus replicated itself and was sent itself to all the contacts in the victim's address book.

(J.) SQL Slammer / Sapphire SQL [2003] – It caused a damage of affected networks included Bank of America's ATM service, Continental Airlines etc. A few minutes after the infection of the first Internet server, the number of victims of the Slammer virus doubled every few seconds.

(K.) Sasser and Netsky [2003] - The Sasser worm exploited Microsoft Windows vulnerability. The infected system will look for other vulnerable systems and instruct those systems to download the virus. A random scan of the IP addresses was done to find potential victims.

(L.) Blaster [2003] – The summer of 2003 was a rough time for businesses running PCs. Blaster, also known as Lovsan or MS Blast, was the first to hit. The virus was spread rapidly, peaking in just two days. Transmitted via network and Internet traffic, this worm exploited vulnerability in Windows 2000 and Windows XP, and when activated, presented the PC user with a menacing dialog box indicating that a system shutdown was imminent.

(M.) Sobig.F [2003] – The Sobig worm hit right on the heels of Blaster, making August 2003 a miserable month for corporate and home PC users. The most destructive variant was Sobig.F, which spread so rapidly that it set a record, generating over 1 million copies of itself in its first 24 hours. The virus infected host computers via innocuously named e-mail attachments such as application resulting in massive amount of Internet traffic.

(N.) Bagle [2004] – Bagle, a classic but sophisticated worm, made its debut on January 18, 2004. The malicious code infected users 'systems via the traditional mechanism — an e-mail attachment — and then scoured Windows files for e-mail addresses it could use to replicate itself.

(O.) Sasser [2004] - Sasser began spreading on April 30, 2004, and was destructive enough to shut down the satellite communications for some French news agencies. It also resulted in the cancellation of several Delta airline flights and the shutdown of numerous companies' systems worldwide.

(P.) Leap-A/Oompa-A [2004] - Oompa-A was one of the viruses which aimed at Mac systems. The viruses used the iChat instant messaging program for its propagation among vulnerable Mac computers. The Leap-A virus was not able to cause much harm to computers, but showed that even a Mac computer can be affected by malicious software.

(Q.) Storm Worm [2004] - The Storm Worm got this particular name because of the fact that the e-mail messages which carry the virus carried a subject ―230 dead as storm batters Europe. Some versions of this Worm turn computers into bots or Zombies.

(R.) MyDoom [2004] - It was created by a backdoor in the OS of the victim's computer. The MyDoom virus had two triggers, which targeted several search engine companies. Such a type of attack slowed down search engine services and caused some website crash.

(S.) Downadup [2009]–The latest dangerous virus is the "downadup" worm, which was also called "Conficker". Downadup was successful in spreading across the Web due to the fact that it used a flaw that Microsoft patched in October in order to distantly compromise computers that ran unmatched versions of Microsoft's operating system.

4.3.13. SUMMARY

Discussing on computer security, the virus is a leading threat. It can destroy a single program or the whole operating system. There are certain other threats affecting the computer security, but not technically called virus. But they also have the same damaging effects as virus. This includes worms, adware, malware, trojan, ransomware etc. It is a robust task to protect computing system from such threats for the law enforcement agencies.

4.3.14. SAQS

1. Short Answer Questions

a) What is Computing?

b) Write a short note on software related crimes.

2. Fill in the Blanks

a) A computer or a computer network becomes a _____when it is targeted and the computer's confidentiality, integrity, or accessibility is attacked.

b) A _____ is a group of technologies that are used as a base upon which other applications, processes or technologies are developed.

3. True or False

a) Similar to an e-mail worm, an IM-Worm uses instant messaging applications installed on the infected machine to send a message to everyone listed on the contact list.

b) VIRUS stands for - Vital Information Resources under Siege.

4.3.15. REFERENCES

Cyber Law by Anirudh Rastogi, LexisNexis, Gurgaon, 2014.

Textbook on Cyber Law by Pavan Duggal, Universal Law Publishing Co., New Delhi, 2014.

Cyber Law in India by Dr. Farooq Ahmad, New Era Law Publications, 2008.

4.3.16. Suggested Readings

Prevention of Cyber Crimes and Fraud Management by Indian Institute of Banking and Finance, Mumbai, 2017.

Cybercrimes by Talat Fatima, Eastern Book Company, Lucknow, 2011.

4.3.17. Terminal Questions and Model Questions

a) Explain the different types of Computing

b) Briefly discuss the various dangerous virus attacks.

ANSWERS

4. a. refer 4.3.1 b. refer 4.3.2.
5. a. victim b. platform
6. 3. a. true b. true

TERMINAL QUESTIONS AND MODEL QUESTIONS

b. Refer 4.3.5 b. 4.3.12.

UNIT- 5
FRAUD, HACKING, MISCHEF

5.1 INTRODUCTION

Criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all are subject to the Indian Penal Code, can involve cybercrime also. Unauthorized access, damage to property, theft, fraud, mischief and the publication of obscene and indecent material are all familiar crimes.

Criminal tendency of human mind to develop new ingenuous and unforeseen deceptive methods to make profit and gain wrongfully causing loss or injury to another, may be the reason why a comprehensive definition to fraud is not attempted under Indian Criminal law. Indian Penal Code envisages of confining and dealing with the offence of fraud on the intention to 'defraud'. According to Web Crime Statistics, fraud on Internet constitutes one third of all cybercrimes.

Unauthorised access to another computer system is commonly known as offence of "hacking". In terms of India Panel Code (IPC), the provision that comes close to describing hacking is

'criminal trespasses. Hacking is made a crime punishable under the Information Technology (IT) Act, 2000.

Mischief is both civil as well as criminal offence. In Civil Law, a person who suffered physical injury due to the Negligence of another person could allege mischief in a lawsuit in tort. Chapter XVII of the Indian Penal Code explains about the offences against property, of them Sections 425 to 440 explain about Mischief. A charge of criminal mischief can encompass a wide range of activities and offenses against a property. Though it does not involve theft, it does involve damage or destruction.

In the present unit we discuss about offences of Fraud, Hacking and Mischief in the light of Indian Penal Code and Cyber law i.e. IT Act, 2000.

5.2 OBJECTIVES

After reading this unit you are able to understand the following:

- What is fraud;
- Definition of fraud under various Indian law;
- Definition of fraud under IPC;
- Punishment for offence of fraud;
- What is hacking;
- Hacking under traditional law;
- Hacking under cyber law;
- Who are hackers;
- Hackers and their technique;
- What is mischief;
- Offence of mischief under civil law;
- Act of mischief under IPC;

5.3 SUBJECT

5.3.1 Fraud

Fraud indeed, in the sense of a Court of Equity, properly includes all acts, omissions and concealments which involve a breach of legal or equitable duty, trust or confidence, justly reposed, and are injurious to another, or by which an undue and unconscientious advantage is taken to another.[1]

In Concise Oxford dictionary Fraud is defined as, "criminal deception, use of false representation to gain unjust advantage; dishonest artifice or trick"

5.3.1.1 'Fraud' Under Indian Law

[1] Story's Equity Jurisprudence, 14th Edition, Vol. 1;

The word 'Fraud' is not defined under Indian Penal Code. However it is defined under section 17 of Indian Contract Act.[2] Under chapter XI of the IT Act, 2000, it is said that, "the word — 'fraudulently' shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860)."[3] In this unit we shall discuss the meaning of fraud in the relevance of Indian Penal Code only. The section 25 of the IPC reads as follows:

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

It is clear from the above definition that the act of fraud implies following two elements-

(i) To do a thing fraudulently; and

(ii) Intention of defraud

The word 'defraud' also not defined under the IPC. "Dishonestly " is defined by section 24 of IPC, which provides that 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; and the meaning of the expression wrongful gain and wrongful loss is made clear by section 23[4].

The word "fraudulently" is used in sections 471 and 464 together with the word "dishonestly" and presumably in a sense not covered by the latter word.

Section 463 defines the "forgery" in the following words-

"Whoever makes any false document or false electronic record or part of a document or electronic record, with intent to cause damage or injury[5], to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery."

Thus we see that section 463 defines the offence of forgery, and in so doing prescribes the intents necessary to that offence.

"Making a false document"- describe in the next section i.e. in section 464 with detailed illustrations. It clears the 'making of false document or false electronic record' in the following words-

"A person is said to make a false document or false electronic record—

First.—who dishonestly or fraudulently—

---

[2] 'Fraud' means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract:— —'Fraud' means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent1, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract:—

(1) the suggestion, as a fact, of that which is not true, by one who does not believe it to be true;
(2) the active concealment of a fact by one having knowledge or belief of the fact;
(3) a promise made without any intention of performing it;
(4) any other act fitted to deceive;
(5) any such act or omission as the law specially declares to be fraudulent. Explanation.—Mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud, unless the circumstances of the case are such that, regard being had to them, it is the duty of the person keeping silence to speak2, or unless his silence, is, in itself, equivalent to speech.

[3] Section 66(b) of IT Act, 2000

[4] "Wrongful gain" is gain by unlawful means of property to which the person gaining is not legally entitled. "Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled.

[5] The word 'electronic record' was inserted by amendment in 2000 for dealing with the challenge of cyber-crime.

(a) makes, signs, seals or executes a document or part of a document;

(b) Makes or transmits any electronic record or part of any electronic record;

(c) affixes any electronic signature on any electronic record;

(d) makes any mark denoting the execution of a document or the authenticity of the electronic signature,

with the intention of causing it to be believed that such document or part of document, electronic record or electronic signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly.—Who without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with electronic signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly.—Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his electronic signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alteration.

Illustrations:

(a) A has a letter of credit upon B for rupees 10,000, written by Z. A, in order to defraud B, adds cipher to the 10,000, and makes the sum 1, 00,000 intending that it may be believed by B that Z so wrote the letter. A has committed forgery.

(b) A, without Z's authority, affixes Z's seal to a document purporting to be a conveyance of an estate from Z to A, with the intention of selling the estate to B and thereby of obtaining from B the purchase-money. A has committed forgery.

(c) A picks up a cheque on a banker signed by B, payable to bearer, but without any sum having been inserted in the cheque. A fraudulently fills up the cheque by inserting the sum of ten thousand rupees. A commits forgery.

(d) A leaves with B, his agent, a cheque on a banker, signed by A, without inserting the sum payable and authorizes B to fill up the cheque by inserting a sum not exceeding ten thousand rupees for the purpose of making certain payments. B fraudulently fills up the cheque by inserting the sum of twenty thousand rupees. B commits forgery.

(e) A draws a bill of exchange on himself in the name of B without B's authority, intending to discount it as a genuine bill with a banker and intending to take up the bill on its maturity. Here, as A draws the bill with intent to deceive the banker by leading him to suppose that he had the security of B, and thereby to discount the bill, A is guilty of forgery.

(f) Z's will contains these words—"I direct that all my remaining property be equally divided between A, B and C." A dishonestly scratches out B's name, intending that it may be believed that the whole was left to himself and C. A has committed forgery.

(g) A endorses a Government promissory note and makes it payable to Z or his order by writing on the bill the words "Pay to Z or his order" and signing the endorsement. B dishonestly erases the words "Pay to Z or his order", and thereby converts the special endorsement into a blank endorsement. B commits forgery.

(h) A sells and conveys an estate to Z. A afterwards, in order to defraud Z of his estate, executes a conveyance of the same estate to B, dated six months earlier than the date of the conveyance to Z, intending it to be believed that he had conveyed the estate to B before he conveyed it to Z. A has committed forgery.
(i) Z dictates his will to A. A intentionally writes down a different legatee named by Z, and by representing to Z that he has prepared the will according to his instructions, induces Z to sign the will. A has committed forgery.
(j) A writes a letter and signs it with B's name without B's authority, certifying that A is a man of good character and in distressed circumstances from unforeseen misfortune, intending by means of such letter to obtain alms from Z and other persons. Here, as A made a false document in order to induce Z to part with property, A has committed forgery.
(k) A without B's authority writes a letter and signs it in B's name certifying to A's character, intending thereby to obtain employment under Z. A has committed forgery inasmuch as he intended to deceive Z by the forged certificate, and thereby to induce Z to enter into an express or implied contract for service.

Explanation 1.—a man's signature of his own name may amount to forgery.
Illustrations:
(a) A signs his own name to a bill of exchange, intending that it may be believed that the bill was drawn by another person of the same name. A has committed forgery.
(b) A writes the word "accepted" on a piece of paper and signs it with Z's name, in order that B may afterwards write on the paper a bill of exchange drawn by B upon Z, and negotiate the bill as though it had been accepted by Z. A is guilty of forgery; and if B, knowing the fact, draws the bill upon the paper pursuant to A's intention, B is also guilty of forgery.
(c) A picks up a bill of exchange payable to the order of a different person of the same name. A endorses the bill in his own name, intending to cause it to be believed that it was endorsed by the person to whose order it was payable; here A has committed forgery.
(d) A purchases an estate sold under execution of a decree against B. B, after the seizure of the estate, in collusion with Z, executes a lease of the estate, to Z at a nominal rent and for a long period and dates the lease six months prior to the seizure, with intent to defraud A, and to cause it to be believed that the lease was granted before the seizure. B, though he executes the lease in his own name, commits forgery by antedating it.
(e) A, a trader, in anticipation of insolvency, lodges effects with B for A's benefit, and with intent to defraud his creditors; and in order to give a colour to the transaction, writes a promissory note binding himself to pay to B a sum for value received, and antedates the note, intending that it may be believed to have been made before A was on the point of insolvency. A has committed forgery under the first head of the definition.

Explanation 2.—The making of a false document in the name of a fictious person, intending it to be believed that the document was made by a real person, or in the name of a deceased person, intending it to be believed that the document was made by the person in his lifetime, may amount to forgery.
Illustration-

A draws a bill of exchange upon a fictious person, and fraudulently accepts the bill in the name of such fictitious person with intent to negotiate it. A commits forgery.

Explanation 3.—For the purposes of this section, the expression "affixing electronic signature" shall have the meaning assigned to it in clause (d) of sub-section (1) of section 2 of the Information Technology Act, 2000 (21 of 2000).
Clause (d) of sub-section (1) of section 2 of the Information Technology Act, 2000 reads as follows:
"Affixing electronic signature with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature."
Punishment for forgery.—whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

5.3.1.2 Essential Ingredients Of The Offence Of Fraud

As section 25 says, the two main ingredients to constitute any fraudulently act are deceit or an intention to deceit and either actual injury or possible injury or intent to expose some person to actual or possible injury.
Forgery is defines in section 463 and what amount to making a false document is given in section 464.
Fraud is proven when it is shown that a false representation has been made, (i) knowingly, or (ii) without belief in its truth, or (iii) recklessly, careless whether it be true or false". But "fraud" in public law is not the same as "fraud" in private law. Nor can the ingredients, which establish "fraud" in commercial transaction, be of assistance in determining fraud in Administrative Law.[6]
The Apex Court in a case[7], dilating upon the words "with intent to deceive" has observed that it does not indicate a bare intent to deceive, but an intent to cause a person to act, or omit to act, on account of deception practised upon him, to his advantage. The words ' but not otherwise' after the words 'with intent to deceive' in the definition of 'fraudulently'- it clearly show, "…..that the words intent to defraud are not synonymous with intent to deceive and requires some action resulting in some disadvantage which but for the deception, the person deceived would have avoided". So, under the Indian law a penal offence of fraud, demands for successful prosecution the twin elements of 'intent to defraud' of the offender -- (i) an intent to deceive another and (ii) an intent to cause, by that deception, injury to some person.
In determining whether the deception was fraudulent or not the question is :Did the author of deceit drive any advantage from it which he could not have had if the truth had been known : if so, it is hardly possible that advantage should not have had an equivalent in loss or risk of loss, to someone else; and if so there was fraud[8].

[6] Derry and Ors vs. Peek(1886-90) All ER 1
[7] Dr. S.Dutt v. State of Uttar Pradesh (AIR 1966 SC 523)
[8] Ramchandra gujar, (1937) 39 Bom. L.R. 1184 *per sir James Stephen;* Indian Penal Code by Prof. S. N. Mishra, page 91;

In another case the Supreme Court observed that, fraud and deception are synonyms. The court said, "*A fraudulent misrepresentation is called deceit and consist in leading a man into damage by wilfully or recklessly causing him to believe in action falsehood. It is a fraud in law if a party makes representation, which he knows to be false, and injury ensures therefrom although the motive from which the representation proceeded may not have been bad. An act of fraud on court always viewed seriously. Fraud and deception are synonymous. Although in a given case a deception may not amount to fraud, fraud is anathema to all equitable principles and any affair tainted with fraud cannot be perpetuated or saved by application on any equitable doctrine including res-judicata.*"[9]

In another case the Supreme Court said that, "*Since fraud affect the solemnity, regularity and orderliness of the proceedings of the Court and also amount to an abuse of process of Court, the Courts have been held to have inherent power to set aside an order obtained by fraud practised upon the Court.*"[10]

5.3.2 Hacking

In simple words hacking is an act of unauthorised access of a computer without the permission of the owner of that computer. Hacking may be constructive and destructive, which depends on the intention of the hacker. In fact a "hacker" is very intelligent and skilful personal. They are basically computer programmers, who have advanced understanding of computers. The real tangible threat of 'hacking' comes in when an unauthorized access to a system is done with an intention of committing further crimes like fraud, misrepresentation, downloading data, in order to commit infringement of copyright, accessing sensitive and top secret data from defence sites, etc. Some of the most common types of fraud as committed on the net include bogus online investment newsletters, which give a biased and untrue advice on stocks and securities thereby fictionally giving a pull to the share value of bogus companies, etc.

5.3.2.1 Hacking Under Indian Law

In terms of India Panel Code (IPC), the provision that comes close to describing hacking is 'criminal trespass'. But to prove criminal trespass under Section 441 of the IPC[11], the ingredients of "unauthorized entry into or upon property against the will of the person in possession" and/or "lawfully obtained entry but wrongfully remaining thereon" must be satisfied. In applying the section to hacking on the Internet, the prime question that needs to be answered is as to whether website is a 'property'. For this it is imperative to consider the computer or the virtual area of the net as a 'property'. In order to do this, we must consider the common jargon used to describe the world of Internet including '*site',' home page', 'visiting a site'* and *'traveling on the super highway'* are just a few examples. Thus, as trespass

[9] Ram Chandra singh vs. Savitri devi (2003) 8 SCC 319;

[10] Indian Bank vs. Satyam fibers (India) Pvt. Ltd.{1996 (5) SCC 550}

[11] Criminal trespass.—Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit "criminal trespass".

actions are grounded in the idea of protecting the owners control over real property, there is no inherent reason as to why the owners control over websites could not be considered as species of property subject to trespass.[12] It is for this reason that hacking is made a crime punishable under the Information Technology (IT) Act, 2000.

Section 43 and section 66 of the IT Act cover the civil and criminal offenses of data theft or hacking respectively. Hacking earlier used to refer to a crime under section 43 of the IT Act but at the same time, ethical hacking or better known as white collar hacking was considered legal. Ethical hacking is also being taught by various professionals at schools and colleges. So a need was felt to differentiate between good and bad i.e. constructive and destructive hacking. Under the amendment IT Act in 2008, the word 'hacker was removed from the act.

Section 43 of Information Technology Act, 2000 says about- Penalty and compensation for damage to computer, computer system, etc. in the following words-

"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;

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;

(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;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

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

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

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

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

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any 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;

(j) steal, conceal, 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;

[12] "Technical notes on Cyber Crime"
https://www.niscair.res.in/ScienceCommunication/ResearchJournals/rejour/jipr/Fulltextsearch/2004/January%202004/JIPR-vol%209-January%202004-pp%2051-56.htm

he shall be liable to pay damages by way of compensation to the person so affected.
Explanation.–For the purposes of this section,–
(i) "computer contaminant" means any set of computer instructions that are designed–

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

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

(ii) "computer data-base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.
(v) "computer source code" means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.

Thus above section describe all the acts, falls under the ambit of crime, done after hacked any computer with malicious intention. In fact above acts are done by **"crackers"** and not by **"hackers"**, because hackers are skilful personals and are constructive but crackers are made unauthorised access in others PCs with bad intention, although crackers are also skilled personalities but they use their intelligence in negative ways to harm others, which constitutes crime.
Section 43A of the IT Act deals with the civil liability of "cracking". This section introduced by amendment act in 2009.The section deals with the compensation that should be made for failure of protection of the date.
Section 43A reads as follows-
"**43A. 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."

It is noteworthy to mention here that, Under the ITA 2000, the maximum cap for compensation was fine at Rs. One crore. However in the amendment made in 2009, this ceiling was removed.

Penal liability of cracking arises when the intention or the liability of the cracker to harm the system or steal any important information gets established. If the cracker only trespasses the system without any intention to harm, it only remains a form of civil liability under section 43A. Like criminal trespass, cyber theft can be punishable under section 378 of Indian Penal Code, which define the theft.

As we mention above that, Section 43A of the IT Act deals with the civil liability of "cracking", section 66 of IT Act deals with the criminal offence of "hacking" (in other words cracking). This section reads as follows-
"**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 (45 of 1860);
(b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860)."
We have already discussed the meaning of word "fraudulently" (under section 25 of the Indian Penal Code) above.
The meaning word "fraudulently" as assigned in section 25 of the Indian Penal Code reads as follows,-
"Dishonestly".—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".[13]
Again the meaning of "wrongful gain" and "wrongful loss" is given in the section 23 of the Indian Penal Code, which reads as follows,-
"Wrongful gain".—"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

[13] section 24 of the Indian Penal Code (45 of 1860);

to lose wrongfully when such person is wrongfully kept out of any property, as well as when such person is wrongfully deprived of property.[14]

Thus section 66 of IT Act, 2000 describe the punishment done against any act referred to in section 43 of IT Act, 2000. Malicious intention or bad intention is the essential ingredients of hacking under section 66 of IT Act, 2000.

Section 66B of IT Act, 2000 covers the punishment for dishonestly receiving stolen computer resource or communication device. The punishment includes imprisonment of for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Similarly under section 66A, punishment for sending offensive messages through communication service, etc. are given as follows,–

"Any person who sends, by means of a computer resource or a communication device,–

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.–For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.[15]

Section 66A explain the another form of hacking with bad intentions. *Mens rea* is an essential ingredient under this section i.e. the person is well aware of his/her act and also its consequences.

5.3.2.2 Hackers and Their Technique

Generally hackers may be categorised through their motives-

- **Pranksters:** These hackers are the mischief-makers of the bunch whose intention is merely to be a nuisance.
- **Fame seekers:** This group hacks seeking attention or notoriety.
- **Educational:** Students justify hacking into systems by saying that they are honing their programming skills.

[14] section 23 of the Indian Penal Code (45 of 1860);

[15] Section 66A has been struck down by Supreme Court's Order dated 24th March, 2015 in the Shreya Singhal vs. Union of India, AIR 2015 SC. 1523.

- **Criminals:** Those who involved in computer fraud and many other acts. Their acts consists of both a mental and physical element of crime i.e. *mens rea* and *actus reus*.

Various techniques used by hackers are following-

SQL injections- SQL is a **standardized query language** for requesting information from a database. SQL is a popular way to get information out of relational **database** systems. An SQL injection is a technique that allows hackers to play upon the security vulnerabilities of the software that runs a website. It can be used to attack any type of unprotected or improperly protected SQL database.

Theft or FPT passwords - FTP stands for File Transfer Protocol. **FTP** is a standard network protocol used to transfer files between computers (a client and server) over a TCP/IP network. This is a very common way to tamper with the websites. Many webmasters store their website login information on their poorly protected PCs and the FTP password hacking takes advantage of this fact. The thief searches the victim's system for FTP login details and then relays them to his own remote computer. He then logs into the website via the remote computer and modifies the web pages as he/she pleases.

Cross site scripting - Cross-site scripting (**XSS**) is a type of computer security vulnerability typically found in web applications. **XSS** enables attackers to inject client-side scripts into web pages viewed by other users. A**cross-site scripting** vulnerability may be used by attackers to bypass access controls such as the same-origin policy. This is a very easy way of circumventing a security system.

5.3.3 Mischief

Generally mischief refer to behaviour, especially a child's that is slightly bad but is not intended to cause serious harm or damage. We can say that mischief is a specific injury or damage caused by another person's action or inaction. In Civil Law, a person who suffered physical injury due to the Negligence of another person could allege mischief in a lawsuit in tort.

A charge of criminal mischief can encompass a wide range of activities and offenses against a property. Though it does not involve theft, it does involve damage or destruction. It can also include road rage and other activities that have to do with disputes or revenge. If the action are either intentional or reckless and cause another person or entity to suffer monetary or property loss, it generally constitutes criminal mischief.

5.3.3.1 Mischief Under Indian Law

In Civil Law, a person who suffered physical injury due to the Negligence of another person could allege mischief in a lawsuit in tort. It is distinct from malicious mischief, which is a criminal act usually involving reckless or intentional behaviour such as Vandalism. In tort law, strict liability is the imposition of liability on a party without a finding of fault (such as negligence or tortious intent). The claimant need only prove that the tort occurred and that the defendant was responsible. The law imputes strict liability to situations it considers to be

inherently dangerous. Under the rule in *Rylands v. Fletcher*[16], a person who allows a dangerous element on their land which, if it escapes and damages a neighbour, is liable on a strict liability basis - it is not necessary to prove negligence on the part of the landowner from which has escaped the dangerous substance. *Rylands v Fletcher* was a decision by the House of Lords[17] which established a new area of English Tort Law.

The Supreme Court of India in *MC Mehta v. Union of India*[18] evolved a more stringent rule of strict liability than the Rylands v. Fletcher rule. In this case, which involved the leakage of and the harm caused by Oleum gas from one of the units of Shriram industries in Delhi, the court held that keeping in mind the needs and demands of a modern society with highly advanced scientific knowledge and technology where for the sake of development programme, it was necessary to carry out inherently dangerous or hazardous industry, a new rule had to be laid down to adequately deal with the problems arising in a highly industrialised economy.

Under Criminal Law, the various act comes under the definition of mischief and their punishment are described from section 425 to 440 of IPC.

The word "Mischief" is defined under section 425 of Indian Penal Code in the following words:

425. Mischief.—Whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits "mischief".

Explanation 1.—It is not essential to the offence of mischief that the offender should intend to cause loss or damage to the owner of the property injured or destroyed. It is sufficient if he intends to cause, or knows that he is likely to cause, wrongful loss or damage to any person by injuring any property, whether it belongs to that person or not.

Explanation 2.—Mischief may be committed by an act affecting property belonging to the person who commits the act, or to that person and others jointly.

Some illustrations are given in the section to make clear the definition.

Illustrations:

(a) A voluntarily burns a valuable security belonging to Z intending to cause wrongful loss to Z. A has committed mischief.

(b) A introduces water in to an ice-house belonging to Z and thus causes the ice to melt, intending wrongful loss to Z. A has committed mischief.

(c) A voluntarily throws into a river a ring belonging to Z, with the intention of thereby causing wrongful loss to Z. A has committed mischief.

(d) A, knowing that his effects are about to be taken in execution in order to satisfy a debt due from him to Z, destroys those effects, with the intention of thereby preventing Z from obtaining satisfaction of the debt, and of thus causing damage to Z. A has committed mischief.

(e) A having insured a ship, voluntarily causes the same to be cast away, with the intention of causing damage to the underwriters. A has committed mischief.

---

[16] (1868) UKHL 1; https://en.wikipedia.org/wiki/Rylands_v_Fletcher

[17] The House of Lords of the United Kingdom, in addition to having a legislative function, historically also had a judicial function. It functioned as a court of first instance for the trials of peers, for impeachment cases, and as a court of last resort within the United Kingdom.

[18] 1987 SCR (1) 819, AIR 1987 965;

(f) A causes a ship to be cast away, intending thereby to cause damage to Z who has lent money on bottomry on the ship. A has committed mischief.
(g) A, having joint property with Z in a horse, shoots the horse, intending thereby to cause wrongful loss to Z. A has committed mischief.
(h) A causes cattle to enter upon a field belonging to Z, intending to cause and knowing that he is likely to cause damage to Z's crop. A has committed mischief.

Punishment for mischief.—
Whoever commits mischief shall be punished with imprisonment of either description for a term which may extend to three months, or with fine, or with both.[19]
Further section 427 provided the punishment for Mischief causing damage to the amount of fifty rupees. It says, "Whoever commits mischief and thereby causes loss or damage to the amount of fifty rupees or upwards, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both."
It is noteworthy to mention here that the offence under these Section are non-cognizable, bailable, compoundable, and triable by any Magistrate.

Punishment for committing mischief with animals:
Section 428 prevents cruelty to animals and consequent loss to the owner. According to this section, "Whoever commits mischief by killing, poisoning, maiming or rendering useless any animal or animals of the value of the ten rupees or upwards, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both."
Again section 429 punishes severely if the animal is of greater value. This section reads as, "Whoever commits mischief by killing, poisoning, maiming or rendering useless, any elephant, camel, horse, mule, buffalo, bull, cow or ox, whatever may be the value thereof, or any other animal of the value of fifty rupees or upwards, shall be punished with imprisonment of either description for a term which may extend to five years, or with fine, or with both."
The offence under above Sections are cognizable, bailable, compoundable with permission of the Court before which any prosecution of such offence is pending, and triable by any Magistrate.

Mischief by injury to works of irrigation or by wrongfully diverting water.—
Section 430 deals with when the water supply to agriculture purposes is in any way decreased by accused illegally so as to infringe any person's right. According to the section, the person commits such mischief shall be punished with imprisonment of either description for a term which may extend to five years, or with fine, or with both. The offence under this Section is also cognizable, bailable, compoundable with permission of the Court before which any prosecution of such offence is pending, and triable by any Magistrate.

Mischief by injury to public road, bridge, river or channel.—

[19] Section 426 of IPC (45 of 1860);

Section 431 says, "Whoever commits mischief by doing any act which renders or which he knows to be likely to render any public road, bridge, navigable river or navigable channel, natural or artificial, impassable or less safe for travelling or conveying property, shall be punished with imprisonment of either description for a term which may extend to five years, or with fine, or with both.

Mischief by causing inundation or obstruction to public drainage attended with damage.—

According to the section 432, "Whoever commits mischief by doing any act which causes or which he knows to be likely to cause an inundation or an obstruction to any public drainage attended with injury or damage, shall be punished with imprisonment of either description for a term which may extend to five years, or with fine, or with both."

Mischief by destroying, moving or rendering less useful a light-house or sea-mark.—

Section 433 reads as, "Whoever commits mischief by destroying or moving any light-house or other light used as a sea-mark, or any sea- mark or buoy or other thing placed as a guide for navigators, or by any act which renders any such light-house, sea-mark, buoy or other such thing as aforesaid less useful as a guide for navigators, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both."

Punishment for **mischief by destroying or moving any land-mark fixed by the authority** shall be, with imprisonment of either description for a term which may extend to one year, or with fine, or with both.[20]

Mischief by fire or explosive substance with intent to cause damage to amount of one hundred or (in case of agricultural produce) ten rupees, shall be punished with imprisonment of either description for a term which may extend to seven years and shall also be liable to fine.[21]

Mischief by fire or explosive substance with intent to destroy house, etc., shall be punished with imprisonment for life, or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.[22] This section contemplates the destruction of a building and a building is not necessarily a finished structure.[23]

Punishment for **Mischief with intent to destroy or make unsafe a decked vessel or one of twenty tons burden** shall be, with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.[24] This section (i.e. 437) excludes all kinds of small crafts.

Punishment for the **mischief described in section 437 committed by fire or explosive substance** shall be, with imprisonment for life or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.[25] This section proposes higher penalty due to dangerous nature of means used to commit mischief crime.

[20] Section 434 of IPC (45 of 1860);
[21] Section 435 of IPC (45 of 1860);
[22] Section 436 of IPC (45 of 1860);
[23] Manning, (1871) L.R. 1 C.C.R. 338; Indian Penal Code by Prof. S.N. Sharma, page 712;
[24] Section 437 of IPC (45 of 1860);
[25] Section 438 of IPC (45 of 1860);

Punishment for intentionally running vessel aground or ashore with intent to commit theft, etc. shall be, with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.[26]

Mischief committed after preparation made for causing death or hurt.— Whoever commits mischief, having made preparation for causing to any person death, or hurt, or wrongful restraint, or fear of death, or of hurt, or of wrongful restraint, shall be punished with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.[27]

5.3.3.2 Essential Ingredients For The Offence Of Mischief

Following essentials would be satisfied to constitute the offence of mischief:

- Mens rea is one of the essential ingredients of mischief. The accused shall have intention or knowledge of likelihood to cause wrongful loss or damage to the public or to any person.
- Destruction of property, or any change in the property, which may destroy or diminish the value of the property.
- Any wrongful loss or damage to the public or to any person by any of the above mentioned acts.
- By doing the wrongful acts of mischief, the accused need not personally benefitted.

For the default of payment or any illegal acts, disconnection of water supply, sewerage supply, electricity supply, telephone connection, etc., by the concerned departments do not come under the purview of "Mischief", as such acts are legally done.

If one compares cybercrimes with traditional land based crimes, it can be found that it has posed number of new challenges to the global legal community. Since it is difficult for the law enforcement agencies to combat cybercrimes, it is not only the job of government, but it is also the responsibility of the global virtual community to put there all efforts to curb this menace.

Indian legislatures while enacting IT Act had used broad terminology. Thus the word "computer damage" and "computer contaminant" as defined in S. 43 (see above)[28] are would enough to including even Hacking within its ambit.[29]

5.4 SUMMARY

A crime consists of both a mental and physical element i.e. *mens reas* and *actus reus*. The Indian Penal Code is the official criminal code of India.

Unauthorized access, damage to property, theft, fraud, mischief and the publication of obscene and indecent material all familiar crimes are traditional in nature. These all are subject to the

[26] Section 439 of IPC (45 of 1860);
[27] Section 440 of IPC (45 of 1860);
[28] See 1.3.2.1 HACKING UNDER INDIAN LAW

[29] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf

Indian Penal Code, can involve cyber-crime also. According to Web Crime Statistics, fraud on Internet constitutes one third of all cybercrimes.

The section 25 of the IPC define fraud as, "A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise." The word 'defraud' is not defined under the IPC. the two main ingredients to constitute any fraudulently act are deceit or an intention to deceit and either actual injury or possible injury or intent to expose some person to actual or possible injury.

Hacking is an act of unauthorised access of a computer without the permission of the owner of that computer. In terms of India Panel Code (IPC), the provision that comes close to describing hacking is 'criminal trespass'. Hacking is made a crime punishable under the Information Technology (IT) Act, 2000. Section 43 and section 66 of the IT Act cover the civil and criminal offenses of data theft or hacking respectively. Section 66 of IT Act, 2000 describe the punishment done against any act referred to in section 43 of IT Act, 2000. Malicious intention or bad intention is the essential ingredients of hacking under section 66 of IT Act, 2000.

Section 66B of IT Act, 2000 covers the punishment for dishonestly receiving stolen computer resource or communication device.

Mischief is a specific injury or damage caused by another person's action or inaction. In Civil Law, a person who suffered physical injury due to the Negligence of another person could allege mischief in a lawsuit in tort.

The word "Mischief" is defined under section 425 of Indian Penal Code as "Whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits "mischief"." Section 426 provided the punishment for Mischief.

Section 428 prevents cruelty to animals and consequent loss to the owner. Section 429 to section 440 of IPC describes various types of act of mischief and their punishment.

5.5 GLOSSARY

IPC : The Indian Penal Code is the official criminal code of India. It is a comprehensive code intended to cover all substantive aspects of criminal law; enacted on 6 October 1860.

IT Act, 2000 : The Information Technology Act, 2000 is an Act of the Indian Parliament notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce.

Mens rea: a fundamental law of Criminal Law is that a crime consists of both a mental and physical element. *Mens rea*, a person's awareness of the fact that his or her conduct is criminal, is the mental element and *actus reus*, the act itself is the physical element.

TCP/IP : TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private network (an intranet or an extranet).

5.6 SAQS

I. Short Answer Question

1. In which section of Indian Contract Act, the word 'fraud' is define?
2. Which provision of IPC is close to describing offence of hacking.
3. Is ethical hacking considered legal?
4. If a body corporate proves for failure to protect data. Shall it be liable to pay damages by way of compensation to the person so affected?
5. What is maximum cap for compensation, under the IT Act?

II. Fill In The Blanks

1. ……..are basically computer programmers, who have advanced understanding of computers.
2. Section …… of IT Act, 2000 covers the punishment for dishonestly receiving stolen computer resource or communication device.
3. Punishment for sending offensive messages through communication service, etc. are given under section ……..
4. The word "Mischief" is defined under section …… of Indian Penal Code.

III. True And False Statement

1. A "hacker" is very intelligent and skilful personal. (true/false) 5.3.2
2. Hacking is an act of unauthorised access of a computer without the permission of the owner of that computer. (true/false)
3. Section 428 of IPC prevents cruelty to animals and consequent loss to the owner.

5.7 REFERENCE

1. http://voice4india.org/judgments-supreme-court-fraud-deceit/7020/
2. https://blog.ipleaders.in/laws-hacking-india/
3. https://www.livelaw.in/offences-fruad-need-new-perspective/
4. http://www.shareyouressays.com/knowledge/legal-provisions-regarding-mischief-section-425-of-ipc/115802
5. https://en.wikipedia.org/wiki/Rylands_v_Fletcher
6. https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
7. Indian Penal code
8. https://www.niscair.res.in/ScienceCommunication/ResearchJournals/rejour/jipr/Fulltextsearch/2004/January%202004/JIPR-vol%209-January%202004-pp%2051-56.htm
9. Indian Technology Act, 2000

5.8 SUGGESTED READINGS

1. Indian Penal code

2. Indian Technology Act, 2000
3. Indian Penal Code by Prof. S.N. Sharma,

5.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. Describe the provision for fraud under IPC.
2. Describe the reason for hacking is made a crime punishable under the Information Technology (IT) Act, 2000.
3. What is good and bad hacking? Explain.
4. Describe in brief the provision for hacking under IPC.
5. Write short notes on the following:

(i) Essential ingredients of the offence of fraud.
(ii) Difference between 'hackers' and 'crackers'.
(iii) Hackers and their technique.
(iv) Essential ingredients for the offence of mischief.
(v) *Mens reas* and *actus reus.*

6. What is civil and criminal mischief?
7. What are the provisions regarding offence of mischief under IPC? Explain.

5.10 ANSWER SAQS

I. SHORT ANSWER QUESTION

1. Section 17; see 5.3.1.1; 2. Criminal trespass; see 5.3.2.1; 3. Yes; see 5.3.2.1; 4. Yes; see 5.3.2.1; 5. Previously it was Rs. One crore, however in the amendment made in 2009, this ceiling was removed; see 5.3.2.1;

II. FILL IN THE BLANKS

1. Hackers; see 5.3.2; 2. 66B; see 5.3.2.1; 3. 66A; see 5.3.2.1; 4. 425; see 5.3.3.1

III. TRUE AND FALSE STATEMENT

4. True; see 5.3.2; 2. True; see 5.3.2; 3. True; see 5.3.3.1;

TERMINAL QUESTIONS AND MODEL QUESTIONS

1. See 5.3.1.1;
2. See 5.3.2.1;
3. See 5.3.2.1;
4. See 5.3.2.1;
5. (i) See 5.3.1.2; (ii) See 5.3.2.1; (iii) See 5.3.2.2; (iv) See 5.3.3.2;
6. See 5.3.2, 5.3.2.1;
7. See 5.3.2.1;

UNIT- 6
TRESSPASS, DEFAMATION, STALKING, SPAM

STRUCTURE

6.1 INTRODUCTION

Unauthorized access, damage to property, theft, fraud, mischief, defamation, stalking and the publication of obscene and indecent material are all familiar crimes. The expression 'crime' is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act.

The world of Internet today has become a parallel form of life and living because with the availability of artificial intelligence and new technologies, we are now capable of doing things, which were not even imaginable few years ago. The advent of the computer has been a boon to students, lawyers, businessmen, teachers, doctors, researchers and also, of course, to the criminals. A person with access to a computer and the Internet might be participating, attempting or planning a criminal act anywhere in the world.

The Indian Penal Code clearly says that, 'Any person liable, by any Indian law, to be tried for an offence committed beyond India shall be dealt with according to the provisions of this Code for any act committed beyond India in the same manner as if such act had been committed within India.

In the previous unit we discuss about offences of Fraud, Hacking and Mischief in the light of Indian Penal Code and Cyber law i.e. IT Act, 2000.

In the present unit we discuss some other crimes like trespass, defamation, stalking and spam in the light of IPC and IT Act.

6.2 OBJECTIVES

After reading this unit you are able to understand the following:

- Civil as well as criminal trespassing;
- Provisions regarding offence of trespass under Indian law;
- Definition of assault , battery and false imprisonment;
- Trespass to goods;
- Trespass to land;
- What are essential elements to constitutes the offence of trespass;
- Punishment for the offence of trespassing;
- What is defamation;
- Provisions for the offence of defamation under penal code;
- The elements, that are necessary to constitutes the offence of defamation;
- Punishment provided by law for the crime of various types of defamation;
- Offence of stalking, definition and provision for punishment for stalking;
- What is spam;
- Meaning and ingredients, that constitutes the offence of spamming;
- Punishment and compensation for various types of spamming;

6.3 SUBJECT

6.3.1 Trespass

In broad term Trespass is entering another person's property without permission of the owner or legal authority. Offence of trespass may be civil or criminal in nature.
The tort of trespass can be defined as an unjustifiable physical interference of land in possession of one party by another. Under English common law where these principles of torts emanate, trespass does not form a criminal act but in the Indian Penal Code it has been given recognition.

6.3.1.1 Trespass Under Indian Law

Trespass is broadly divided into three groups:

- trespass to a person;
- trespass to chattel; and
- Trespass to land.

6.3.1.1.1 Trespass to a Person

Trespass to a person included assault, battery and false imprisonment.
Assault is an attempt or offer to apply force to the person of another directly or indirectly. Battery consist of touching another person hostilely or against his will. The force[30] (defined in the section 349 of IPC) becomes criminal force when -

(i) it is used in order to the committing of the offence and is used without consent; and
(ii) It is intentionally used to cause injury, fear or annoyance to some other person.[31]

The term '**Battery**' is not defined under Indian law. Battery is a term of English Law, which included "criminal force"[32]. The criminal force may be very slight as not amounting to an offence as per section 95[33].The aim of battery is to cause grievous hurt to other person. But if two or more meet in a narrow passage and without any violence or design of harm, the one touches the other, gently, it will be no battery. If any of them use violence against the other, to force his way in a rude manner, it will be a battery. Any struggle about the passage to that degree as may do hurt, will be a battery. Hence in case of battery intention must necessarily be considered.
False imprisonment means total restraint of a person's liberty without any legal justification for imprisonment.
Assault is defined under section 351 of IPC in the following words:
Assault.—Whoever makes any gesture, or any preparation intending or knowing it to be likely that such gesture or preparation will cause any person present to apprehend that he who makes

[30] See glossary
[31] See Section 350 of the Indian Penal Code (45 of 1860);
[32] Ibid.
[33] Act causing slight harm.—nothing is an offence by reason that it causes, or that it is intended to cause, or that it is known to be likely to cause, any harm, if that harm is so slight that no person of ordinary sense and temper would complain of such harm.

that gesture or preparation is about to use criminal force to that person, is said to commit an assault.

***Explanation.*—**Mere words do not amount to an assault. But the words which a person uses may give to his gestures or preparation such a meaning as may make those gestures or preparations amount to an assault.

Some illustrations are given in the section to make clear the offence of assault:

(a) A shakes his fist at Z, intending or knowing it to be likely that he may thereby cause Z to believe that A is about to strike Z. A has committed an assault.

(b) A begins to unloose the muzzle of a ferocious dog, intending or knowing it to be likely that he may thereby cause Z to believe that he is about to cause the dog to attack Z. A has committed an assault upon Z.

(c) A takes up a stick, saying to Z, "I will give you a beating". Here, though the words used by A could in no case amount to an assault, and though the mere gesture, unaccompanied by any other circumstances, might not amount to an assault, the gesture explained by the words may amount to an assault.

Punishment for assault or criminal force otherwise than on grave provocation.—Whoever assaults or uses criminal force to any person otherwise than on grave and sudden provocation given by that person, shall be punished with imprisonment of either description for a term which may extend to three months, or with fine which may extend to five hundred rupees, or with both.[34]

It is make clear under this section that, 'Grave and sudden provocation will not mitigate the punishment for an offence under this section', but 'Whether the provocation was grave and sudden enough to mitigate the offence, is a question of fact.'[35]

Section 353 says that, 'Assault or criminal force to deter public servant from discharge of his duty shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.'

Assault or criminal force to woman with intent to outrage her modesty shall be punished with imprisonment of either description for a term which shall not be less than one year but which may extend to five years, and shall also be liable to fine.[36]

Sexual harassment also comes under the ambit of criminal assault. In this regards section 354A says,-

"(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.

[34] Section 352 of the Indian Penal Code (45 of 1860);
[35] Explanation of Section 352 of the Indian Penal Code (45 of 1860);
[36] Section 354 of the Indian Penal Code (45 of 1860);

(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."

It is noted here that, not only, try to make an attempt of physical contact but demand or request for sexual favours or showing pornography against the will of women and even making sexually coloured remarks, shall be guilty of the offence of sexual harassment and punishes accordingly. Again, showing pornography is itself constitutes a cybercrime.

Further section 354B says that, "Any man who assaults or uses criminal force to any woman or abets such act with the intention of disrobing or compelling her to be naked, shall be punished 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."

Thus assault and battery against modesty of any women is made a serious crime under law.

Assault or criminal force with intent to dishonour person, otherwise than on grave provocation. —Whoever assaults or uses criminal force to any person, intending thereby to dishonour that person, otherwise than on grave and sudden provocation given by that person, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.[37]

Assault or criminal force in attempt to commit theft of property carried by a person.— Whoever assaults or uses criminal force to any person, in attempting to commit theft on any property which that person is then wearing or carrying, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.[38]

Assault or criminal force in attempt wrongfully to confine a person.—Whoever assaults or uses criminal force to any person, in attempting wrongfully to confine that person, shall be punished with imprisonment of either description for a term which may extend to one year, or with fine which may extend to one thousand rupees, or with both.[39]

Assault or criminal force on grave provocation.—whoever assaults or uses criminal force to any person on grave and sudden provocation given by that person, shall be punished with simple imprisonment for a term which may extend to one month, or with fine which may extend to two hundred rupees, or with both.

Explanation.—Grave and sudden provocation will not mitigate the punishment for an offence under this section, if the provocation is sought or voluntarily provoked by the offender as an excuse for the offence, or

if the provocation is given by anything done in obedience to the law, or by a public servant, in the lawful exercise of the powers of such public servant, or

[37] See Section 355 of the Indian Penal Code (45 of 1860);
[38] See Section 356 of the Indian Penal Code (45 of 1860);
[39] See Section 357 of the Indian Penal Code (45 of 1860);

if the provocation is given by anything done in the lawful exercise of the right of private defence. Whether the provocation was grave and sudden enough to mitigate the offence, is a question of fact.[40]

In simple words **"False imprisonment"** is restraining a person in a bounded area without justification or consent. False imprisonment is a crime as well as a tort. It applies private as well as governmental detention. The victim of false imprisonment file the suit against the offence in civil and also in criminal court. It is also a matter of fundamental right given by the Indian Constitution under Article 20 and 21. Article 20 gives protection in respect of conviction for offences. Article 21 gives the right to life, personal liberty and the right to die with dignity. The proving of false imprisonment is sufficient to obtain a writ[41] of Habeus Corpus. A writ of habeas corpus (which literally means to "produce the body") is a court order demanding that a public official deliver an imprisoned individual to the court and show a valid reason for that person's detention.

Under Indian Penal Code sections 339 to 348 deals with the offence of false imprisonment. Section 340 of IPC says about "wrongful confinement" in the following words,-

Wrongful confinement.—whoever wrongfully restrains any person in such a manner as to prevent that person from proceedings beyond certain circumscribing limits, is said "wrongfully to confine" that person.

When any person voluntarily obstructs any other so as to prevent that person from proceeding in any direction in which that person has a right to proceed, is said wrongfully to restrain that person.[42] For example, 'A obstructs a path along which Z has a right to pass, A not believing in good faith that he has a right to stop the path. Z is thereby prevented from passing. A wrongfully restrains Z. punishment for wrongfully restrains any person shall be, with simple imprisonment for a term which may extend to one month, or with fine which may extend to five hundred rupees, or with both.[43]

Example of wrongful confinement-

(a) A causes Z to go within a walled space, and locks Z in Z is thus prevented from proceeding in any direction beyond the circumscribing line of wall. A wrongfully confines Z.

(b) A places men with firearms at the outlets of a building, and tells Z that they will fire at Z if Z attempts leave the building. A wrongfully confines Z.

Punishment for wrongfully confines any person will be, with imprisonment of either description for a term which may extend to one year, or with fine which may extend to one thousand rupees, or with both.[44]

If period of wrongful confinement is three or more days the imprisonment may extend to two years or punishes with fine or both.[45] Similarly if period of wrongful confinement is ten or

[40] See Section 358 of the Indian Penal Code (45 of 1860);
[41] It is a constitutional remedy available to all the people of India. The Supreme Court and High Court has power to issues writs under Article 36 and 226 respectively.
[42] Section 339 of the Indian Penal Code (45 of 1860);
[43] Section 341 of the Indian Penal Code (45 of 1860);
[44] Section 342 of the Indian Penal Code (45 of 1860);
[45] Section 343 of the Indian Penal Code (45 of 1860);

more days the punishment of imprison may extend to three years and shall also be liable to fine.[46]

Wrongful confinement of person for whose liberation writ has been issued.—Whoever keeps any person in wrongful confinement, knowing that a writ for the liberation of that person has been duly issued, shall be punished with imprisonment of either description for a term which may extend to two years in addition to any term of imprisonment to which he may be liable under any other section of this Chapter.[47]

Wrongful confinement in secret.—Whoever wrongfully confines any person in such manner as to indicate an intention that the confinement of such person may not be known to any person interested in the person so confined, or to any public servant, or that the place of such confinement may not be known to or discovered by any such person or public servant as hereinbefore mentioned, shall be punished with imprisonment of either description for a term which may extend to two years in addition to any other punishment to which he may be liable for such wrongful confinement.[48]

Section 347 of IPC says about **wrongful confinement to extort property, or constrain to illegal act.** This section reads as, "Whoever wrongfully confines any person for the purpose of extorting from the person confined, or from any person interested in the person confined, any property or valuable security or of constraining the person confined or any person interested in such person to do anything illegal or to give any information which may facilitate the commission of an offence, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine."

Section 348 defines **wrongful confinement to extort confession, or compel restoration of property** and punishment for such offence. According to this section, "Whoever wrongfully confines any person for the purpose of extorting from the person confined or any person interested in the person confined any confession or any information which may lead to the detection of an offence or misconduct, or for the purpose of constraining the person confined or any person interested in the person confined to restore or to cause the restoration of any property or valuable security or to satisfy any claim or demand, or to give information which may lead to the restoration of any property or valuable security, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine."

6.3.1.1.1.1 Essential Ingredients To Be Constitutes The Offence Of Trespass To A Person

From the above discussion it is now clear that following ingredients are necessarily included in the offence of trespass to a person:

(i) Intentional use of force to any person;

[46] Section 344 of the Indian Penal Code (45 of 1860);
[47] Section 345 of the Indian Penal Code (45 of 1860);
[48] Section 346 of the Indian Penal Code (45 of 1860);

(ii) Such force to be used without the consent of other person i.e. victim;
(iii) The force must have been used to commit an offence. In other words with the intention to cause injury, fear or annoyance to the victim.[49]

Causing of some actual hurt is not necessary for constituting assault. Mere threat may constitute assault[50]. *Mens rea* is a necessary ingredient under the offence of assault. In other words an intention to cause harm to other is necessary to constitute the offence of assault. Another essential ingredient to make the offence of assault as per section 351 is, making gesture or preparation by a person in the presence of another.

During false imprisonment a person apply voluntary obstruction to prevent other from proceeding in any direction in which the other person has right to proceed. There is total restraint of the personal liberty of a person. In this offence period of confinement is immaterial but becomes material in determining the extent of punishment. Malice is not an essential element in the offence of wrongful confinement. Also physical force or actual conflict is not an essential requirement. Detention through moral force is sufficient to constitute wrongful confinement. An arrest made by the police officer without warrant, for a non-cognizable offence was amounted to wrong confinement.[51]

There is no requirement that the plaintiff alleging false imprisonment was aware of the restraint on his freedom at the time of his confinement, If the person is confined in a room, with one of the entries known to the plaintiff closed, and the room has more than one entry-exit door, but the plaintiff has no knowledge about the same, the defendant will still be held liable. To constitute the wrong, there may be no actual imprisonment in the ordinary sense. Any confinement in the ordinary sense whether be it prison or any place used temporarily for the purpose of confinement constitutes false imprisonment.[52]

Hence it is the crime against the legal right of a person given by constitution. The tort of false imprisonment is one of the most severe forms of human rights violation.

6.3.1.1.2 Trespass To A Chatteles

Trespass to chattels, also known as trespass to goods or trespass to personal property, is defined as "an intentional interference with the possession of personal property. **Trespass to goods** is defined as "wrongful physical interference with goods that are in the possession of another", and is covered not only by the common law, but also by the Torts (Interference with Goods) Act 1977.

The trespass can be as little as touching or moving the goods, given the right circumstances. It differs from trespass to land in one important aspect that wrongful intention or negligence is not necessary for trespass to goods. A challenge to ownership of goods amounts to conversion which is different from trespass to goods, which can be elucidated by an example of the damage of goods given by the plaintiff in a cloak room of railways but personnel there instead of giving it, threw it and damaged it.

[49] Indian Penal Code by Prof. S.N. Sharma;
[50] *Rupabati vs. Shyama.* AIR 1958 Cut. 710; Indian Penal Code by Prof. S.N. Sharma, page 585;
[51] *Gopal Naidu vs. Madras State* (1922)46 Mad.605; Indian Penal Code by Prof. S.N. Sharma, page 581;
[52] https://www.lawctopus.com/academike/law-of-false-imprisonment-in-india/

Remedies for trespass to chattel include damages, liability for conversion, and injunction, depending on the nature of the interference.

In recent years, trespass to chattels has been expanded in the United States to cover intangible property, including combating the proliferation of unsolicited bulk emails as well as virtual property interests in online worlds. In the late 1990s, American courts enlarged trespass to chattels, first to include the unauthorized use of long distance telephone lines,[53] and later to include unsolicited bulk email.

6.3.1.1.2.1 Essential Elements For Trespass Of Chattele Or Goods

Generally, trespass to chattels possesses following three elements:

1. The interference with the property must be non-consensual. A claim does not lie if, in acquiring the property, the purchaser consents contractually to certain access by the seller. "[A]ny use exceeding the consent" authorized by the contract, should it cause harm, gives rise to a cause for action.
2. The interference with the property must result in actual harm. The threshold for actual harm varies by jurisdiction. In California, for instance, an electronic message may constitute a trespass if the message interferes with the functioning of the computer hardware, but the plaintiff must prove that this interference caused actual hardware damage or actual impaired functioning.
3. The interference must be intentional. What constitutes intention varies by jurisdiction, however, the Restatement (Second) of Torts indicates that "intention is present when an act is done for the purpose of using or otherwise intermeddling with a chattel or with knowledge that such an intermeddling will, to a substantial certainty, result from the act", and continues: "[i]t is not necessary that the actor should know or have reason to know that such intermeddling is a violation of the possessory rights of another".

6.3.1.1.3 Trespass To Land

Trespassing is the legal term for the situation in which one person enters onto the land of another without permission or the legal right to be there. Depending on the circumstances and the law in place where the act occurs, trespassing may be considered a crime, a civil wrong (called a "tort"), or both.

In modern law the word *trespass* is used most commonly to describe the intentional and wrongful invasion of another's real property. Under English law trespass does not form a criminal act? The tort of trespass requires essentially only the possession of land by the plaintiff and jut encroachment by some way by the defendant. There requires no force, unlawful intention or damage nor the breaking of an enclosure.

The **criminal trespass** is define under section 441 in IPC. Section 441 says,-

[53] "[T]he electronic signals generated by the [defendants'] activities were sufficiently tangible to support a trespass cause of action." *Thrifty-Tel v. Bezenek*, 46 Cal.App.4th 1559, n. 6 54 Cal.Rptr.2d 468 (1996); https://en.wikipedia.org/wiki/Trespass

"Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit "criminal trespass"."

In this section, if any person enters upon the property of another lawfully but unlawfully remains there with intent to insult or annoy such person, he is guilty of an offence of criminal trespass.

Punishment for criminal trespass.—Whoever commits criminal trespass shall be punished with imprisonment of either description for a term which may extend to three months, or with fine which may extend to five hundred rupees, or with both.[54]

House trespass- Section 442 of IPC prescribes a particular criminal trespass in the nature of house trespass in the following-

"Whoever commits criminal trespass by entering into or remaining in any building, tent or vessel used as a human dwelling or any building used as a place for worship, or as a place for the custody of property, is said to commit "house-trespass".

Explanation.—the introduction of any part of the criminal trespasser's body is entering sufficient to constitute house-trespass."

Building is defined as a structure intended for affording some sort of protection to the persons dwelling inside in or for the property placed therein for custody.[55] School and railway waiting room is also a building in this sense.

Punishment for house-trespass.—Whoever commits house-trespass shall be punished with imprisonment of either description for a term which may extend to one year, or with fine which may extend to one thousand rupees, or with both.[56]

If any person commits house-trespass in order to the committing of any offence, which is punishable with death. In that case the trespasser shall be punished with imprisonment for life, or with rigorous imprisonment for a term not exceeding ten years, and shall also be liable to fine.[57]

Moreover if anyone commits house-trespass in order to the committing of any offence punishable with imprisonment for life, shall be punished with imprisonment of either description for a term not exceeding ten years, and shall also be liable to fine.[58]

Further section 451 says that, "Whoever commits house-trespass in order to the committing of any offence punishable with imprisonment, shall be punished with imprisonment of either description for a term which may extend to two years, and shall also be liable to fine; and if the offence intended to be committed is theft, the term of the imprisonment may be extended to seven years."

[54] Section 447 of the Indian Penal Code (45 of 1860);
[55] *Lakshman Koundes*, A.I.R. 1927 Mad. 543; Indian Penal Code by Prof. S.N. Sharma, page 715;
[56] Section 448 of the Indian Penal Code (45 of 1860);
[57] Section 449 of the Indian Penal Code (45 of 1860);
[58] Section 450 of the Indian Penal Code (45 of 1860);

Trespassing made in surreptitious manner is deal under the section 443 of IPC. This section reads as follows:

Lurking house-trespass.—Whoever commits house-trespass having taken precautions to conceal such house-trespass from some person who has a right to exclude or eject the trespasser from the building, tent or vessel which is the subject of the trespass, is said to commit "lurking house-trespass".

Above section deals with further aggravation trespass due to its lurking nature.

Lurking house-trespass by night.—whoever commits lurking house-trespass after sunset and before sunrise, is said to commit "lurking house-trespass by night".

Trespassing in a house through breaking it or any part of it is address in detail under section 445 of IPC. This section says,

House-breaking.—A person is said to commit "house-breaking" who commits house-trespass if he effects his entrance into the house or any part of it in any of the six ways hereinafter described; or if, being in the house or any part of it for the purpose of committing an offence, or having committed an offence therein, he quits the house or any part of it in any of such six ways, that is to say:—

First.—If he enters or quits through a passage made by himself, or by any abettor of the house trespass, in order to the committing of the house-trespass.

Secondly.—If he enters or quits through any passage not intended by any person, other than himself or an abettor of the offence, for human entrance; or through any passage to which he has obtained access by scaling or climbing over any wall or building.

Thirdly.—If he enters or quits through any passage which he or any abettor of the house-trespass has opened, in order to the committing of the house-trespass by any means by which that passage was not intended by the occupier of the house to be opened.

Fourthly.—if he enters or quits by opening any lock in order to the committing of the house-trespass, or in order to the quitting of the house after a house-trespass.

Fifthly.—if he effects his entrance or departure by using criminal force or committing an assault, or by threatening any person with assault.

Sixthly.—if he enters or quits by any passage which he knows to have been fastened against such entrance or departure, and to have been unfastened by himself or by an abettor of the house-trespass.

Explanation.—any out-house or building occupied with a house, and between which and such house there is an immediate internal communication, is part of the house within the meaning of this section.

Above section describe six ways for house breaking. Further, to make clear this following illustrations are given under this section:

(a) A commits house-trespass by making a hole through the wall of Z's house, and putting his hand through the aperture. This is house- breaking.

(b) A commits house-trespass by creeping into a ship at a port- hole between decks. This is house-breaking.

(c) A commits house-trespass by entering Z's house through a window. This is house-breaking.

(d) A commits house-trespass by entering Z's house through the door, having opened a door which was fastened. This is house-breaking.
(e) A commits house-trespass by entering Z's house through the door, having lifted a latch by putting a wire through a hole in the door. This is house-breaking.
(f) A finds the key of Z's house door, which Z had lost, and commits house-trespass by entering Z's house, having opened the door with that key. This is house-breaking.
(g) Z is standing in his doorway. A forces a passage by knocking Z down, and commits house-trespass by entering the house. This is house-breaking.
(h) Z, the door-keeper of Y, is standing in Y's doorway. A commits house-trespass by entering the house, having deterred Z from opposing him by threatening to beat him. This is house-breaking.
It is important to mention here that, where a hole was made by housebreaker in the wall of a house but their way was blocked by presence of a beam on the other side of the wall, the offence committed was an attempt to house-breaking and not actual house-breaking as given under Illustration (a).[59]

House-breaking by night.—whoever commits house-breaking after sunset and before sunrise, is said to commit "house-breaking by night".[60]

Punishment for lurking house-trespass or house-breaking.—whoever commits lurking house-trespass or house-breaking, shall be punished with imprisonment of either description for a term which may extend to two years, and shall also be liable to fine.[61]
Similarly if anyone commits lurking house-trespass or house-breaking, in order to the committing of any offence punishable with imprisonment, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and if the offence intended to be committed is theft, the term of the imprisonment may be extended to ten years.[62]

Punishment for lurking house-trespass or house-breaking by night.—According to section 456 of IPC**: "**Whoever commits lurking house-trespass by night, or house-breaking by night, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine."
Moreover if any person commits lurking house-trespass by night, or house-breaking by night, in order to the committing of any offence punishable with imprisonment, shall be punished with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine; and, if the offence intended to be committed is theft, the term of the imprisonment may be extended to fourteen years.[63]
If any trespasser whilst committing lurking house-trespass or house-breaking, causes grievous hurt to any person or attempts to cause death or grievous hurt to any person, shall be punished

[59] Indian Penal Code by Prof. S.N. Sharma;
[60] Section 446 of the Indian Penal Code (45 of 1860);
[61] Section 453 of the Indian Penal Code (45 of 1860);
[62] Section 454 of the Indian Penal Code (45 of 1860);
[63] Section 457 of the Indian Penal Code (45 of 1860);

with imprisonment for life, or imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.[64]
The co-extensive and constructive liability of persons jointly concerned in committing 'lurking house-trespass' and house-breaking at night' is address under section 460 and during the course of which death or grievous hurt to any person, every person is caused. Every accused person is punished for the act of any one of them. Such punishment shall be with imprisonment for life, or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

6.3.1.1.3.1 Criminal Trespass With Hurt, Assault Or Wrongful Restrain

Where house trespass is committed in order to cause **hurt,** or to **assault** or to **wrongfully restrain** any person, then section 452 of IPC provided higher punishment for this offence. Section 452 says,-
"Whoever commits house-trespass, having made preparation for causing hurt to any person or for assaulting any person, or for wrongfully restraining any person, or for putting and person in fear of hurt, or of assault, or of wrongful restraint, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine."

Similarly section 455 is applicable to the house-breaker who actually has himself made preparation for causing **hurt, assault** or wrongful **restrain any person.** This section reads as follows-
"Whoever commits lurking house-trespass, or house-breaking, having made preparation for causing hurt to any person, or for assaulting any person, or for wrongfully restraining any person, or for putting any person in fear of hurt or of assault or of wrongful restraint, shall be punished with imprisonment of either description or a term which may extend to ten years, and shall also be liable to fine."

6.3.1.1.3.2 Criminal Trespass With Intent To Commit Mischief

Section 461 and 462 of IPC dealt with the offence of criminal trespassing committed dishonestly or with the intent to commit mischief.
According to section 461, "Whoever dishonestly or with intent to commit mischief, breaks open or unfastens any closed receptacle which contains or which he believes to contain property, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both."
And section 462 says, "Whoever, being entrusted with any closed receptacle which contains or which he believes to contain property, without having authority to open the same, dishonestly, or with intent to commit mischief, breaks open or unfastens that receptacle, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both."

[64] Section 459 of the Indian Penal Code (45 of 1860);

6.3.1.1.3.3 Essential Elements For Tresspass To Land

Every unlawful entry onto another's property is trespass, even if no harm is done to the property. Any person who enters upon the property of another with intent to commit offence etc. is criminal trespass. Following elements are essential to commit an offence of 'criminal trespasses-

(1) Entry into or upon immovable property in the possession of another. If such entry is lawful, then unlawfully remaining upon such property.
(2) An intent to commit an offence or to intimidate, insult or annoy such person, who has lawful possession of that property.

It is noteworthy to mention here that criminal trespass depends on the intention and not the nature of the act.

In the offence of house trespassing and lurking house trespassing following ingredients must be added with the above mentioned elements, i.e.-

(3) Entry into or remaining in any building i.e. building used as human dwelling, not necessarily as a place of permanent residence viz. a school or a railway waiting room.
(4) In case of lurking house-trespass the house included building, tent or vessel and the entry must be made in a surreptitious manner.
(5) Time of offence is also an element define in separate sections i.e. If lurking house-trespass occur at night, section 444 is also applied otherwise offence committed is U/S 443 only.

In case of house breaking in addition to above mentioned elements following ingredients should be satisfied to commit an offence of house breaking-

(6) Making entry into a house through any means-
    (i) through the passage made by the accused himself or his accomplice of the house trespass;
    (ii) through any passage not meant for human entrance other than himself or an abettor of the offence;
    (iii) through any passage opened by himself or by any of the abettors of the house-trespass;
    (iv) by opening any lock to seek entry into, or exit from, the house;
    (v) by using criminal force to seek entry into, or depart from, the house; and
    (vi) by entering or quitting through any passage fastened against such entrance or exit.

(7) Time of offence is also an element define in separate sections. Element of time is added u/s 446.

Hence we see that in all house-breaking, there must be house-trespass and in all house-trespass there must be criminal-trespass. To constitute the offence of house-breaking and house-trespass there must be an intent to commit criminal trespass.

The term 'house' in Section 445 has been used in the same sense as a 'building used as a human dwelling or any building used as a place for worship or as a place for the custody of property within the meaning of Section 442. The explanation extends the meaning of the term 'house'

by including therein any out-house or building if it is connected therewith by an immediate internal communication.

6.3.2 Defamation

Defamation is a general term for a legal claim involving injury to one's reputation caused by a false statement made by another. The false statement must include a fact and it may be libel or slander i.e. in the form of written or spoken. In India, defamation is both civil and criminal offence**.** The remedy for civil defamation is covered under the Law of Torts. In a civil defamation case, a person who is defamed can move either High Court or subordinate courts and seek damages in the form of monetary compensation from the accused. The standard of proof is also different in a criminal case than a civil case. Crimes must generally be proved "beyond a reasonable doubt", whereas civil cases are proved by lower standards of proof such as "the preponderance of the evidence".[65]
Under IPC sections 499 and 500 address the criminal defamation. Defamation laws may come into tension with freedom of speech, leading to censorship where publishers fear lawsuits. Freedom of speech for individual and for media is guaranteed under the article 19 of the Constitution of India. There are many demands to make defamation only as a civil wrong. However, the Supreme Court in his recent judgment uphold the validity of Sections 499 and 500 of the IPC.

6.3.2.1 Defamation Under Indian Penal Law

Defamation is injury to the person's reputation. Human are lives in society and any intentional false communication, either written or spoken, that harms reputation of a person, decreases the respect, regard or confidence in which a person is held and induced disparaging, hostile or disagreeable opinions or feeling against a person, is called defamation.

Section 499 of IPC defines the 'defamation' in the following words-
"Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.
Explanation 1.—it may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the fellings of his family or other near relatives.
Explanation 2.—it may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.
Explanation 3.—an imputation in the form of an alternative or expressed ironically, may amount to defamation.

[65] https://www.clearias.com/defamation-freedom-speech/

Explanation 4.—No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful.

Some illustrations are given to clear the definition-

Illustrations

(a) A says, "Z is an honest man; he never stole B's watch"; intending to cause it to be believed that Z did steal B's watch. This is defamation, unless it fall within one of the exceptions.

(b) A is asked who stole B's watch. A points to Z, intending to cause it to be believed that Z stole B's watch. This is defamation, unless it fall within one of the exceptions.

(c) A draws a picture of Z running away with B's watch, intending it to be believed that Z stole B's watch. This is defamation, unless it fall within one of the exceptions.

There are ten exceptions in this section-

First Exception.—Imputation of truth which public good requires to be made or published.—It is not defamation to impute anything which is true concerning any person, if it be for the public good that the imputation should be made or published. Whether or not it is for the public good is a question of fact.

Second Exception.—Public conduct of public servants.—It is not defamation to express in good faith any opinion whatever respecting the conduct of a public servant in the discharge of his public functions, or respecting his character, so far as his character appears in that conduct, and no further.

Third Exception.—Conduct of any person touching any public question.—It is not defamation to express in good faith any opinion whatever respecting the conduct of any person touching any public question, and respecting his character, so far as his character appears in that conduct, and no further.

Following illustration is given to make clear above exceptions-

"It is not defamation in A to express in good faith any opinion whatever resepting Z's conduct in petitioning Government on a public question, in signing a requisition for a meeting on a public question, in presiding or attending at such meeting, in forming or joining any society which invites the public support, in voting or canvassing for a particular candidate for any situation in the efficient discharge of the duties of which the public is interested."

Fourth Exception.—Publication of reports of proceedings of courts.—It is not defamation to publish substantially true report of the proceedings of a Court of Justice, or of the result of any such proceedings.

Explanation.—A Justice of the Peace or other officer holding an enquiry in open Court preliminary to a trial in a Court of Justice, is a Court within the meaning of the above section.

Fifth Exception.—Merits of case decided in Court or conduct of witnesses and others concerned.—It is not defamation to express in good faith any opinion whatever respecting the merits of any case, civil or criminal, which has been decided by a Court of Justice, or respecting the conduct of any person as a party, witness or agent, in any such case, or respecting the character of such person, as far as his character appears in that conduct, and no further.

Following ***illustrations*** are given to make clear the meaning of fifth exception-

(a) A says—"I think Z's evidence on that trial is so contradictory that he must be stupid or dishonest." A is within this exception if he says this in good faith, inasmuch as the opinion which he expresses respects Z's character as it appears in Z's conduct as a witness, and no farther.

(b) But if A says—"I do not believe what Z asserted at that trial because I know him to be a man without veracity"; A is not within this exception, inasmuch as the opinion which express of Z's character, is an opinion not founded on Z's conduct as a witness.

Sixth Exception.—Merits of public performance.—it is not defamation to express in good faith any opinion respecting the merits of any performance which its author has submitted to the judgment of the public, or respecting the character of the author so far as his character appears in such performance, and no further.

Explanation.—A performance may be submitted to the judgment of the public expressly or by acts on the part of the author which imply such submission to the judgment of the public.

Illustrations

(a) A person who publishes a book, submits that book to the judgment of the public.

(b) A person who makes a speech in public, submits that speech to the judgment of the public.

(c) An actor or singer who appears on a public stage, submits his acting or singing to the judgment of the public.

(d) A says of a book published by Z—"Z's book is foolish; Z must be a weak man. Z's book is indecent; Z must be a man of impure mind." A is within the exception, if he says this in good faith, inasmuch as the opinion which he expresses of Z respects Z's character only so far as it appears in Z's book, and no further.

(e) But if A says "I am not surprised that Z's book is foolish and indecent, for he is a weak man and a libertine." A is not within this exception, inasmuch as the opinion which he expresses of Z's character is an opinion not founded on Z's book.

Seventh Exception.—Censure passed in good faith by person having lawful authority over another.—It is not defamation in a person having over another any authority, either conferred by law or arising out of a lawful contract made with that other, to pass in good faith any censure on the conduct of that other in matters to which such lawful authority relates.

Illustration

A Judge censuring in good faith the conduct of a witness, or of an officer of the Court; a head of a department censuring in good faith those who are under his orders, a parent censuring in good faith a child in the presence of other children; a schoolmaster, whose authority is derived from a parent, censuring in good faith a pupil in the presence of other pupils; a master censuring a servant in good faith for remissness in service; a banker censuring in good faith the cashier of his bank for the conduct of such cashier as such cashier- are within this exception.

Eighth Exception.—Accusation preferred in good faith to authorised person.—It is not defamation to prefer in good faith an accusation against any person to any of those who have lawful authority over that person with respect to the subject-matter of accusation.

Illustration

If A in good faith accuses Z before a Magistrate; if A in good faith complains of the conduct of Z, a servant, to Z's master; if A in good faith complains of the conduct of Z, a child, to Z's father- A is within this exception.

Ninth Exception.—Imputation made in good faith by person for protection of his or other's interests.—It is not defamation to make an imputation on the character of another provided that the imputation be made in good faith for the protection of the interests of the person making it, or of any other person, or for the public good.

Illustrations

(a) A, a shopkeeper, says to B, who manages his business—"Sell nothing to Z unless he pays you ready money, for I have no opinion of his honesty." A is within the exception, if he has made this imputation on Z in good faith for the protection of his own interests.

(b) A, a Magistrate, in making a report to his own superior officer, casts an imputation on the character of Z. Here, if the imputation is made in good faith, and for the public good, A is within the exception.

Tenth Exception.—Caution intended for good of person to whom conveyed or for public good. — It is not defamation to convey a caution, in good faith, to one person against another, provided that such caution be intended for the good of the person to whom it is conveyed, or of some person in whom that person is interested, or for the public good."

It is clear to above description that definition of 'defamation' is thoroughly describe in the IPC with clear exceptions. For the offence of defamation the defamatory matter must be communicated to some person other than the person to whom it concerns. In other words publication of defamatory matter is essential. A publisher shall be strictly responsible for publishing a defamatory matter irrespective of the fact weather he is the originator of the libel or is merely repeating it.[66]

The requirement of exception 1 and 4 is that the imputation must be true. While according to other exceptions that the imputation should be made in good faith. The position of some personal and lawful authority's u/s 499 are as follows:

- The court generally presumes that the defamatory matter was published in good faith and made on instructions. The **advocate** are protected under the exception if there is absence of direct malice or private motive.
- As regard of statement made by a **witness,** he has no absolute privilege. But only qualified privilege under exception 1 and 9.[67]

[66] *Harbhajan singh,* A.I.R. 1961 Punj. 215; Indian Penal Code by Prof. S.N. Sharma, page 765;
[67] *E.P. Reddi,* A.I.R. 1932 Mad. 165; Indian Penal Code by Prof. S.N. Sharma, page 772;

- If the statement is bona fide and made with a view to protect their interest, **parties** will be entitled to protection under exception 9.[68]
- **Judges** are protected for their acts done when discharging their duty as judge u/s 77 of IPC.
- Under exception 9 the committee member of a **social club** are given protection, even if wrong. But for this exception it is impossible for such body to function.
- The **report** of an officer in the execution of his duty under his superior's order, in which defamatory imputations against others, does not appear to have recklessly or unjustifiably are protected. But a report based on totally false allegations will not protected.
- **Legislators** enjoys absolute privileges to their speeches made on the floor of house either of Parliament or State Legislature.

Punishment for defamation: Section 500 of IPC provided punishment for the offence done u/s 499 as follows:
"Whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both."
Hence the quantum of punishment may extend to two years, weather with or without fine.

Printing or engraving matter known to be defamatory.—Whoever prints or engraves any matter, knowing or having good reason to believe that such matter is defamatory of any person, shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.[69]

Sale of printed or engraved substance containing defamatory matter.—Whoever sells or offers for sale any printed or engraved substance containing defamatory matter, knowing that it contains such matter, shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.[70]
If any person printed or engraved a defamatory matter and he/she know or has reason to believe that such matter is defamatory then punishes u/s 501. A seller of such defamatory matter is punishable u/s 502.

6.3.2.2 Essential Ingredients For Offence Of Defamation

As we mention earlier that defamation is a civil wrong as well as offence under Indian Penal Code also. In English law there is distinction has been maintained between libel and slender form of defamation, but under Indian law no such distinction has be seen.
Defamation laws protect the reputations of individuals and other entities (such as businesses) from untrue and damaging statements.

[68] *Sayed Ali,* A.I.R. 1925 Rang. 360;
[69] Section 501 of the Indian Penal Code (45 of 1860);
[70] Section 502 of the Indian Penal Code (45 of 1860);

It is now clear from above discussion, that following ingredients are essential for an offence of defamation:

(1) There is a statement (imputation) of fact, which must be about another person;
(2) such imputation must have been made by-
   (i) words, either spoken or intended to be read; or
   (ii) signs; or
   (iii) Visible representations.
(3) The statement should be published to a third party, who cannot also be the person who is being defamed;
(4) The statement caused injury
(5) The statement must be false. ...

The ***Explanation 1*** will come into operation when, the imputation made by any person would hurt the deceased person's reputation and it would have also hurt the feelings of deceased's family and relatives.

If any statement defamed the reputation of any company and affect it trade or business, the ***Explanation 2*** will come into operation. It also covers any collection of persons but such collection of persons must be identifiable in the sense that one could with certainly say that this group of particular people has been defamed as distinguished from the rest of community.

Ironic Statements are used to emphasise a point using the opposite (or deeper) meaning of something. If any imputation made through ironically statement, then it constitutes defamation according under ***Explanation 3.***

Explanation 4 makes it clear that, the term referred to in the explanation has reference to imputation on a man's character made to lower him in the estimation of others and not of himself.[71]

As describe earlier there are 10 exceptions given with the definition of defamation under section 499 0f IPC.

The requirement of ***Exception 1*** are- first, the statement into question must be true and second, its publication is for public good.

Under ***Exception 2*** the statement made against a public servant in the discharge of his public functions, must be based on true facts and honest expression made in good faith and for public good.

Exception 3 is apply on the conduct of publicists who take part in politics or other matters concerning the public can be commented on in good faith.

Exception 4 requires that the report of proceedings of a court of justice should be without malice, fair an accurate. **Good faith is not a requisites of this exception.**

Under ***Exception 5*** the free comment on the judgement of court, the verdict of jury, the conduct of parties and the witness is necessary. A journalist must discharge his duty fairly.

Exception 6 deals with the literary criticism of public performance submitted to its judgement. The criticism should be fair and made in good faith.

Exception 7 allow a person under whose authority other have been placed by their consent or by law to censure in good faith, those who are so placed under his authority so far as regard matters to which that authority relates.

[71] *Amar Singh*, (1962) 2 Cr. L.J. 698; Indian Penal Code by Prof. S.N. Sharma, page 768;

It is necessary for application of ***Exception 8*** that the complaint is *bona fide* and not made with the intention to injure any one.
Where a defamatory statement is made in good faith for the protection of the interest of the person making it, ***Exception 9*** will come into operation.
It is noteworthy to mention here that, under exception 8, the person to whom the complaint is made must have lawful authority to deal with the subject matter of the complaint, while in exception 9 no such requirement is need.
For applying the ***Exception 10*** it must be proved that the caution is intended to be given to the person to whom it is needed. The imputation must be made in good faith.
Thus it is clear from above discussion that Justification of truth, fair comment and privilege are the prime defences to the action of defamation.
We have also found that the essence of defamation lies in the injury to the reputation of a person. And for this injury, he can very much sue the defendants.

6.3.3 Stalking

Stalking is a repetitive pattern of unwanted, harassing or threatening behaviour committed by one person against another. Acts include: telephone harassment, being followed, receiving unwanted gifts, and other similar forms of intrusive behaviour. In digital age harassing or threatening through social sites, internet and other digital means also come under this preview. It is known as cyber stalking.
Stalking is often dismissed as an harmless and innocent act, but it is an alarming and harrowing for the victim. It is the victim who ultimately has to bear the grunt, move to a different place, change jobs, and sometimes even their identity to evade the stalker.

6.3.3.1 Stalking Under Indian Law

In present times, physical stalking has become secondary to online stalking due to the increased reach and easily available information which can be effortlessly manipulated by someone. Regardless of their gravity, these crimes are considered as minor crimes. The Indian cyber laws do not address the issue of cyber stalking.
Under Section 354 of the IPC, whoever assaults a woman knowing that it would outrage her modesty is liable to be punished under the law. The essence of a woman's modesty is her sex. The ultimate test to be seen if a woman's modesty is outraged is to see if the act or assault would amount to shocking the sense of decency of a woman.
In fact, the Magistrates did not always take cognizance of cases under sexual harassment until in *Rupan Deol Bajaj vs. Kanwar Pal Singh Gill* (1995) the Supreme Court unambiguously directed the Magistrate to take cognizance of the complaint under Section 354 read with Section 509.
After the multitude of offences against women and the increasing violence, in 2013, the Criminal Law Amendment Act was introduced through the Justice Verma Committee. Stalking, both online and offline, was recognized as an offence under Section 354D. This section reads as follows:

Stalking.—(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) (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.

Punishment for the offence of stalking:

"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.[72]

Though the Act has made stalking a crime now, it has been criticised for its loopholes and lack of a coherent definition. The first offence of stalking is "bailable", implying the accused need not be produced before court for seeking bail and can walk to freedom from police station itself. There is an evident presumption that women do not stalk as it only protects women from stalking when the stalker is a man. Gender bias is one of the biggest lacunas of Indian criminal laws, and laws on stalking continue to insinuate this. Further Stalking laws are relatively young laws which are still unknown to the majority. Establishing a dedicated machinery, sensitising the enforcement authorities and creating a quick redressal mechanism is required to deal with the problem of stalking, both physical and virtual. [73]

6.3.3.2 Crime Of Stalking

According to a victim of stalking "Stalking is rather a precursor to much more serious crime."[74]

The crime of stalking is not a standalone crime and is of a nature where many other offences in the law are interlinked. A woman who is stalked, is not only being mentally harassed, she may be sexually harassed, eve teased and her modesty may also be outraged.

The victim can also additionally file a case of defamation (Section 499, IPC) against the offender.

Section 354A of IPC punishes offence of sexual harassment with 3 years of imprisonment and/or fine.

Section 354C criminalises the offence of Voyeurism. It is defined as the act of capturing the image of a woman engaging in a private act, and/or disseminating said image, without her

[72] Section 354D (2) of the Indian Penal Code (45 of 1860);

[73] https://www.myadvo.in/blog/the-unavailing-laws-on-stalking-in-india/

[74] Varnika Kundu; see Chandigarh staking case;

consent. The section prescribes 3 years of imprisonment for the first conviction and 7 years of imprisonment on second conviction along with fine.
Section 507 punishes criminal intimidation by an anonymous communication with a term which may extend to two years of imprisonment. Vengeful posting of images or videos of rape victims is punishable with imprisonment which may extend to two years and fine under section 228a of IPC.

6.3.3.3 Essential Ingredients For The Offence Of Stalking

Stalking is the act of following someone or something very closely and watching its every move. Following ingredients are involves in the offence of stalking:

(1) following a woman by any man
(2) contacting, or attempting to contact, by any means,
(3) there must be a clear indication of disinterest by such woman;

(4) monitoring the use by a woman of the internet, email or any other form of electronic communication,
(5) loitering in any place (whether public or private),

There are giving some conditions in the section 354D that will not amount to the stalking. These conditions are as follows:

(1) the man following a woman for the purpose of preventing or detecting crime and that responsibility to the man is entrusted by state
(2) the woman is persuaded by man under any law or to comply with any condition or requirement imposed by any person under any law;
(3) Such conduct was reasonable and justified in the particular circumstances.

The effect of stalking is to curtail a victim's freedom, leaving them feeling that they constantly have to be careful. In many cases, the conduct might appear innocent, but when carried out repeatedly so as to amount to a course of conduct, it may then cause significant alarm, harassment or distress to the victim.

6.3.4 Spam

Spam is any message or posting, regardless of its content, that is sent to multiple recipient who have not specifically requested the message. Generally unsolicited bulk messages are sent to a large number of users, indiscriminately.
The first show of email spam dates back as far as 1978, when Indian are unknown to computers, and, although spam began in earnest in 1994, the recent history of spam “trouble” actually began about 2002. In early 2002, spam presented about 16% of all the email sent over internet. By early 2008, spam present between 87% and 95% of all emails.[75]
Opening links given in spam mails may lead the user to phishing web sites hosting malware. Spam mails also have infected files as attachments. Emails spamming worsen when the

[75] Wikipedia;

recipient replies to the email causing all the original addressees to receive the reply. Spamming collect email addresses from customers lists, news groups, chat-rooms, web sites and viruses which harvest user's address books, and sell them to other spammers as well.
In 2002, the first hostile virus targeted at Pakistan was released by a group of Indian hackers and spread worldwide - a worm called "Yaha"[76], which was sent out as spam that pretended to offer you a free screensaver, and would rebroadcast itself from infected machines. Pakistani government websites and the Karachi stock exchange were severely affected by DoS attacks triggered by this worm,
Email spamming may be combined with email spoofing, so that it is very difficult to determine the actual originating email address of the sender. "Email spoofing" refers to email that appears to have been originated from one source when it was actually sent from another source. Individuals, who are sending "junk" email or "SPAM", typically want the email to appear to be from an email address that may not exist. This way the email cannot be traced back to the originator.

6.3.4.1 Spam Under Indian Law

Spammers are violating the privacy of mail account holder by forcing to receive useless mails. Many aspects of spam are unlawful and other consumer protection statutes dealing with unfair and deceptive business practices. Many services and products promoted via spam, like get-rich-quick schemes and quack medical remedies, are already illegal under existing laws. Spammers use many technical tricks to hijack e-mail servers are unlawful. Internet service providers (ISPs) have also successfully sued spammers under laws relating to trademark misuse and the private-property rights of network owners.

Developed countries like USA and EUROPIAN country are already enacted law against spam but India has no direct law against spam under IPC or IT Act.
The Information Technology Act, a law based primarily on the UNCITRAL Model Law on Electronic Commerce was passed by the Indian legislature in 2000. While that statute had no provisions directly relating to spam, it did have provisions on hacking[77] and on 'damage to computer, computer system, etc.' that were remarkably broad. These provisions, which could potentially be stretched to include spam, have never, at the time of writing, been tested against spam.
An 'Expert Committee' was constituted, in August 2005 to proposed amendments to the Information Technology Act over various cybercrimes. The committee did not propose any amendments specifically on spam, despite their having been software industry representation on the committee. The Parliamentary Standing Committee reviewing that bill amending the Information Technology Act, noted that:

[76] Wikidot Definition of Yaha.

[77] See previous unit, unit-5: Fraud, hacking, Mischief;

"While examining the Information Technology (Amendment) Bill, 2006, the Committee were apprised by the industry representatives/legal experts that 'spam' or the issue of receiving unwanted and unwarranted e-mails have not been addressed under the proposed amendments. In the above context, the Committee asked whether it would not be prudent to incorporate specific provisions in the proposed law to protect the e-mail account holders from unwarranted mails. In reply, the Department of Information Technology stated that Sub-Section (b) of Section 66A and Clause (i) of Section 43 of the IT Act addressed the issues pertaining to spam."[78]

Section 43 of IT Act, says about **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 not exceeding one crore rupees to the person so affected."[79]

And section 66A provided punishment for sending offensive massage through communication service, etc. in following way:

Punishment for sending offensive messages through communication service, etc.–"Any person who sends, by means of a computer resource or a communication device,–

…(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;

(c) Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.–For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message."[80]

The Telecom Regulatory Authority of India (TRAI) has sought to tackle SMS spam and unsolicited telemarketing through its regulatory powers, rather than using the Information Technology Act. TRAI has used multiple means to deter SMS spam and unsolicited telemarketing, including mandatory registration for telemarketing and SMS marketing – which includes provisions requiring marketers to respect a nationwide "Do Not Call" list, the Telecom Commercial Communications Customer Preference Portal (NCCP)[81]. TRAI additionally approaches this from a pricing perspective, levying higher termination charges for

[78] http://cybersummit.info/sites/cybersummit.info/files/srs-ewi-paper-final.pdf

[79] For detail see unit-5: Fraud, hacking, Mischief;

[80] Ibid;

[81] Telecom Commercial Communications Customer Preference Portal;

'transactional SMSes' to raise the costs of bulk SMS and make it uneconomical to send unsolicited SMS campaigns.

Recent TRAI regulations[82] provide strong disincentives to all players in the unsolicited telemarketing and bulk SMS ecosystem, from telecom operators who structure bulk SMS plans that are heavily abused by marketers, to telemarketers as well as the advertisers who hire them for spam campaigns. TRAI will, going forward, levy a fine of five thousand rupees per complaint, for successive incidents of spam SMS originating from bulk SMS plans allotted to unregistered telemarketers. In addition, all telephone numbers allocated to both the telemarketer as well as the advertiser that hired the telemarketer are subject to disconnection, in an attempt to target the widespread use of throwaway prepaid phone numbers in telemarketing and SMS campaigns.

TRAI earlier attempted to enforce a blanket limit the number of SMSes that could be sent each day, which was halted by the courts stepping in to disallow such a restriction.[83]

While the telecom regulator has, over a period of years, been able to come upon a reasonably functional solution against SMS spam, there still continue to be no useful legislative or regulatory provisions against email spam, and substantial work is required on enforcement against other forms of cybercrime.

6.4 SUMMARY

The fundamental principle of criminal liability is laid down in the maxim - *'actus non facit reum nisi mens sit rea*'. It means that, 'an act by itself will not amount to offence unless it is done with guilty intention'

All from the conventional crimes are treated by the Indian Penal code. With the advent of computer and internet the world face a new threat in the form of cyber-crime. When the IPC was drafted, there was nothing like computer. Hence it not defined cyber-crime. To face this problem the Information Technology Act was enacted. Still the provisions of IPC are applicable where the IT Act is silent to a particular offence.

Trespass is of mainly three types- trespass to a person, trespass to chattel and trespass to land. Trespass to a person included assault, battery and false imprisonment. Different types of assault are address under section 351 to section 358 of IPC. The term 'Battery' is not defined under Indian law. Battery is a term of English Law, which included "criminal force". Sections 339 to 348 deals with the offence of false imprisonment under Indian Penal Code.

Trespass to chattels is defined as "an intentional interference with the possession of personal property. It is also known as trespass to goods or trespass to personal property.

Trespass to land or criminal trespass is define under section 441 in IPC. Different offences related criminal trespass and their punishment are address under section 442 to 460 of IPC. Where house trespass is committed in order to cause hurt, or to assault or to wrongfully restrain any person, then section 452 and 455 of IPC provided higher punishment for this offence.

[82] Agrawal, Rajeev. TRAI releases "The Telecom Commercial Communications Customer Preference (Thirteenth Amendment) Regulations, 2013," TRAI, 22 August 2013,

[83] "Convention on Cybercrime," Council of Europe,

Section 461 and 462 of IPC dealt with the offence of criminal trespassing committed dishonestly or with the intent to commit mischief.

Defamation is a civil wrong as well as offence under Indian Penal Code also. Defamation is injury to the person's reputation, caused by a false statement made by another. Sections 499 and 500 of IPC address the criminal defamation.

Stalking is a repetitive pattern of unwanted, harassing or threatening behaviour committed by one person against another. In present times, physical stalking has become secondary to online stalking due to the increased reach and easily available information which can be effortlessly manipulated by someone. Which is known as cyber stalking. The Criminal Law (Amendment) Act, 2013 amended the Indian Penal Code and inserted 'stalking' as a crime under Section 354D(1)(1). Both online and offline stalking was recognized as an offence under Section 354D. The crime of stalking is not a standalone crime and is of a nature where many other offences in the law are interlinked.

Stalking becomes a serious crime against women. The fallout of the #MeToo movement promises to initiate an open dialogue on all forms of sexual harassment being faced by women in India. The narrative must also consider seriously, the problem of online stalking to safeguard the right of women to be free from harassment in the cyberspace.

Spam is any message or posting, regardless of its content, that is sent to multiple recipient who have not specifically requested the message. Spammers are violating the privacy of mail account holder by forcing to receive useless mails. Developed countries like USA and EUROPIAN country are already enacted law against spam but India has no direct law against spam under IPC or IT Act. Sub-Section (b) of Section 66A and Clause (i) of Section 43 of the IT Act addressed the issues pertaining to spam.

6.5 GLOSSARY

Mens rea : *Mens rea*, is mental element, i.e. a person's awareness of the fact that his or her conduct is criminal.

Tort: A tort, in common law jurisdictions, is a civil wrong that causes a claimant to suffer loss or harm resulting in legal liability for the person who commits the tortious act. The person suffer loss is liable to obtain damage for his loss.

Force: A person is said to use force to another if he causes motion, change of motion, or cessation of motion to that other, or if he causes to any substance such motion, or change of motion, or cessation of motion as brings that substance into contact with any part of that other's body, or with anything which that other is wearing or carrying, or with anything so situated that such contact affects that other's sense of feeling:

Provided that the person causing the motion, or change of motion, or cessation of motion, causes that motion, change of motion, or cessation of motion in one of the three ways hereinafter described:

First.—by his own bodily power.

Secondly.—By disposing any substance in such a manner that the motion or change or cessation of motion takes place without any further act on his part, or on the part of any other person.

Thirdly.—by inducing any animal to move, to change its motion, or to cease to move.[84]
U/S – Under section.
Preponderance of the evidence: The greater weight of the evidence required in a civil (non-criminal) lawsuit for the trier of fact (jury or judge without a jury) to decide in favor of one side or the other. This preponderance is based on the more convincing evidence and its probable truth or accuracy, and not on the amount of evidence. Prosecutors in criminal cases must prove meet the burden of proving that the defendant is guilty beyond a reasonable doubt, whereas plaintiffs in a civil case, such as for personal injury, must prove their case by a preponderance of the evidence.
Loathsome: Extremely unpleasant or disgusting
Resepting (resept): an idea formed by the repetition of similar percepts, as successive percepts of the same object
Veracity: The quality of being true or correct; the habit of telling the truth.
Censuring: To tell somebody in a strong and formal way, that he/ she has done something wrong.
Bona fide: Authentic; genuine; without intention to deceive.
Malware: it is a software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
Phishing: It is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
Viruses: A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions. It can self-replicate, inserting itself onto other programs or files, infecting them in the process. Not all computer viruses are destructive though.

6.6 SAQS

I. SHORT ANSWER QUESTION

6. Under which section the assault is make a criminal offence?
7. A takes up a stick, saying to Z, “I will give you a beating”. Will it amount to an assault?
8. Name the writ, which is obtained against the false imprisonment.
9. If a person enters upon the property of another lawfully but unlawfully remains there with intent to insult or annoy such person. Does he/she guilty of an offence of criminal trespass?
10. A commits house-trespass by making a hole through the wall of Z's house, and putting his hand through the aperture. Does he commit house-breaking?
11. Is defamation both civil and criminal offence?
12. How many exceptions are given with the definition of defamation under section 499 0f IPC.

[84] Section 349 of the Indian Penal Code (45 of 1860);

IV. FILL IN THE BLANKS

5. An arrest made by the police officer without warrant, for a non-cognizable offence was amounted to …….. .
6. Publication of true reports of proceedings of courts, if hurt a person's reputation. It does not amount to …….. .
7. Judges are protected against the defamation charges for their acts done when discharging their duty as judge under section ……. of IPC.
8. Sale of printed or engraved substance containing defamatory matter, knowing that it contains such matter, is offence under section ……. of IPC.
9. Stalking, both online and offline, was recognized as an offence under Section ……. .
10. The victim of stalking can also additionally file a case of …….. Against the offender.
11. In 2002, the first hostile virus targeted at Pakistan was released by a group of Indian hackers and spread worldwide - a worm called …….. .

V. TRUE AND FALSE STATEMENT

5. Mere words do amount to an assault. (True/False)
6. Showing pornography is constitutes a cybercrime. (True/False)
7. Causing of some actual hurt is not necessary for constituting assault. Mere threat may constitute assault. (True/False)
8. Detention through moral force is sufficient to constitute wrongful confinement. (True/False)
9. To prove the trespass to chattel there must be some actual harm. (True/False)
10. To constitute the offence of house trespass, it is necessary to enter trespasser whole body. (True/False)
11. A finds the key of Z's house door, which Z had lost, and commits house-trespass by entering Z's house, having opened the door with that key. This is not amount to house-breaking. (True/False)
12. Every unlawful entry onto another's property is trespass, even if no harm is done to the property. (True/False)
13. Public good or good faith is a good defense in the case of defamation. (True/False)
14. Cyber-stalking also address under IPC. (True/False)
15. Section 345D of IPC only protects women from stalking not man. (True/False)
16. Section 66A (b) and of Section 43 (i) of the IT Act addressed the issues pertaining to spam. (True/False)

6.7 REFERENCE

1. https://en.wikipedia.org/wiki/Trespass
2. http://www.legalservicesindia.com/article/202/Trespass:-Tortious-Liability.html
3. https://www.lawctopus.com/academike/law-of-false-imprisonment-in-india/
4. Indian Penal Code by Prof. S.N. Sharma

5. Indian Penal Code; https://www.iitk.ac.in/wc/data/IPC_186045.pdf
6. https://blog.ipleaders.in/trespass-meaning-nature-types-defenses-case-laws/
7. https://www.clearias.com/defamation-freedom-speech/
8. https://barandbench.com/me-too-law-protects-you-stalking/
9. https://www.myadvo.in/blog/the-unavailing-laws-on-stalking-in-india/
10. http://cybersummit.info/sites/cybersummit.info/files/srs-ewi-paper-final.pdf
11. Indian Technology Act, 2000
12. Constitution of India

6.8 SUGGESTED READINGS

1. Indian Penal Code by Prof. S.N. Sharma
2. Indian Penal Code
3. Constitution of India
4. Indian Technology Act, 2000

6.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. Define the offence of assault. Does Sexual harassment come under the ambit of criminal assault? Explain.
2. False imprisonment is also a matter of fundamental right given by the Indian Constitution under Article 20 and 21. Article 20. Comment.
3. Write short note on 'wrongful confinement'.
4. What do you mean by trespass to chattel?
5. write short notes on the following:

(i) Criminal trespass.
(ii) House trespass.
(iii) Lurking house trespass.
(iv) House breaking.
(v) Criminal trespass with intent to commit mischief.
(vi) Essential ingredients for offence of defamation.
(vii) Offline and online stalking.
(viii) Voyeurism.
(ix) Email spoofing.

6. What punishment given to the person who commit criminal trespass with assault, hurt or wrongful restrain.
7. "Defamation laws generally come into tension with freedom of speech." Give your opinion.
8. Defamation law applies to deceased person also. Comment.
9. Explain the exceptions in the section 499.
10. "Stalking is rather a precursor to much more serious crime." Comment.

11. Give a brief account of essential ingredients of the offence of stalking.
12. Describe the position of offence under Indian law.

6.10 ANSWER SAQS

I. SHORT ANSWER QUESTION

1. Section 351; see 6.3.1.1.1; 2. Yes; see 6.3.1.1.1; 3. Habeus Corpus; 6.3.1.1.1; 4. Yes; see 6.3.1.1.3; 5. Yes; see 6.3.1.1.3; 6. Yes; 6.3.2; 7. 10; see 6.3.2.1

III. FILL IN THE BLANKS

1. Wrong confinement; see 6.1.1.1.1; 2. Defamation; see 6.3.2.1; 3. 77; see 6.3.2.1;
13. 502; see 6.3.2.1; 5. 354D; see 6.3.3.1; 6. Defamation; see 6.3.3.2; 7. "Yaha"; see 6.3.4;

III. TRUE AND FALSE STATEMENT

1. False; see 6.3.1.1.1; 2. True; see 6.3.1.1.1; 3. True; see 6.3.1.1.1.1; 4. True; see 6.3.1.1.1.1; 5. True; see 6.1.1.2.1; 6. False; see 6.3.1.1.3; 7. False; 6.3.1.1.3; 8. True; see 6.3.1.1.3.3; 9. True; see 6.3.2.1; 10. True; 6.3.3.1; 11. True; see 6.3.3.1; 12. True; see 6.3.4.1;

TERMINAL QUESTIONS AND MODEL QUESTIONS

1. See 6.3.1.1.1;
2. See 6.3.1.1.1. 6.3.1.1.1.1;
3. See 6.3.1.1.1, 6.3.1.1.1.1;
4. See 6.1.1.2, 6.1.1.2.1;
5. (i) to (iv) See 6.3.1.1.3, 6.3.1.1.3.3; (v) See 6.3.1.1.3.2; (vi) See 6.3.2.2; (vii) See 6.3.3, 6.3.3.1, 6.3.3.2; (viii) See 6.3.3.2; (ix) See 6.3.4;
6. See 6.3.1.1.3.1;
7. See 6.3.2, 6.3.2.1;
8. See 6.3.2.1;
9. See 6.3.2.1;
10. See 6.3.3.1, 6.3.3.2;
11. See 6.3.3.3;
12. See 6.3.4.1

UNIT- 7
PENALTIES AND OFFENCES UNDER THE IT ACT

STRUCTURE

7.1 INTRODUCTION

The Information Technology Act, 2000 (ACT NO. 21 OF 2000) was enacted on 9th June 2000, to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies.[85]

The Information Technology Act, 2000 applies also to any offence or contravention thereunder committed outside India by any person.

The 'offence' is defined in the code of criminal procedure to mean as an act or omission made punishable by any law for the time being in force. With the emergence of Internet, the traditional crimes have assumed new dimensions. Any criminal wrong related to cyber world is loosely spoken as "Cybercrime".

The first well publicized instance in India of the potential damage caused by cybercrime was in 1998, when members of an anti-nuclear collective of hackers called milw0rm[86] compromised servers belonging to the Bhabha Atomic Research Centre (BARC), and downloaded classified documents about India's nuclear weapons program.

The Information Technology Act provides for and punishes only certain Cyber offences and is not exhaustive of all cyber-crimes. For offence where IT Act is silent, but the commission of the offence includes the use of Internet it will attract the provisions of Indian Penal Code and the act will be called cyber-crime. Though the IT Act 2000 defines and punishes only a few cyber-crimes, it recognizes that there are other crimes which can be committed via Internet and there the provisions of Indian Penal Code 1860 will be applicable.

7.2 OBJECTIVES

After reading this unit you are able to understand the following:

- Penalties and offences provided under the Information Technology Act, 2000;
- Compensation for damaging computer, computer system etc and failure to protect data;
- Penalty for failure to furnish any document, return or report or any information, books or other documents or maintain books of account or records etc.;
- Provision about residuary penalty and Recovery of penalty or compensation;
- Provisions about offence of tampering with the computer source documents,
- Offences relating to Hacking with computer system, cyber fraud and cyber terrorism;
- Offence of Publishing of information which is obscene in electronic form and pornography;

[85] Objective, Information Technology Act, 2000 (ACT NO. 21 OF 2000)
[86] https://en.wikipedia.org/wiki/Milw0rm

- What is the Power of Controller to give directions to subordinates and issue orders for interception or monitoring or decryption and penalty if any one fails to comply with them;
- Who are intermediary, their responsibility and punishment for contravention of their duty;
- Power of Central Government to issue directions for blocking for public access of any information through any computer resource in the various national interest;
- Provisions which gives power to Central Government for enhancing cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country;
- Power of appropriate government to declare any computer, computer system or computer network, to be a protected system;
- Provisions for national nodal agency, computer emergency response team (CERT) etc.;
- Penalty for misrepresentation or suppression of material facts during obtaining of any licence or electronic signature;
- Penalty for breach of confidentiality and privacy;
- Applicability of IT Act on offence or contravention committed outside India;
- Provisions for compounding of offences;
- Punishment for abetment and attempt to commit offences;
- Offences relating to company;

7.3 SUBJECT

7.3.1 Penalties Under It Act

The fast growing technology converted the whole world in to a global village. The world-wide connectivity also developed numerous online crime called cyber-crime. These increased offences need law to protect innocents. The Indian Parliament enacted the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.
For the violation of rules and regulations various penalties has been prescribes under chapter IX of the IT Act, 2000. These are describe below.

7.3.1.1 Penalty And Compensation For Damage To Computer, Computer System, Etc.

The anonymous nature of the Net has made Netizens more vulnerable to the cyber-crimes. Breaking into the computer systems has become common.

According to section 43 of IT Act, where a person without the permission of owner or any other person-in-charge damage the Computer, or Computer System, or Computer Network, the he shall be liable for Penalty and Compensation to such person so affected. This section reads as follows:

"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;
(*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;
(*c*) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
(*d*) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
(*e*) disrupts or causes disruption of any computer, computer system or computer network;
(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
(*g*) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
(*h*) charges the services availed of by a person to the account of another person by tampering with or manipulating any 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;
(*j*) steal, conceal, 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.

Explanation.–For the purposes of this section,–
(*i*) "computer contaminant" means any set of computer instructions that are designed–
(*a*) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
(*b*) by any means to usurp the normal operation of the computer, computer system, or computer network;
(*ii*) "computer data-base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
(*iii*) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
(*iv*) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

(*v*) "computer source code" means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.

Penalty : According to above section if any person does any of the aforesaid act(s), he/she shall liable to pay compensation, not exceeding one crore rupees to the affected person.

7.3.1.2 Compensation for Failure to Protect Data

Network security has become a major concern with the birth of Internet and its unprecedented growth. Private confidential information has become available to the public. Confidential information can reside in two states on the network. It can reside on the physical stored media, such as hard drive or memory or it can reside in the transit across the physical network wire in the form of packets. Since these network packets are not encrypted they can be processed and understood by any application that can pick them off the network and process them. A third party can easily interpret the network packets and develop a packet sniffer[87]. A packet sniffer can provide its users with meaningful and often sensitive information.
Section 43A of IT Act provided compensation for failure to protect sensitive personal data or information. This section says:

"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."

[87] A packet sniffer is software that uses a network adapter card in a promiscuous mode to capture all network packets that are sent across a local network.

< https://shodhganga.inflibnet.ac.in/bitstream/10603/58938/8/08_chapter%203.pdf >

7.3.1.3 Penalty for Failure to Furnish Information, Return, Etc

Section 44 prescribes the penalty for failure to furnish any document, return or report which is required to be submitted to the Controller or the Certifying Authority under the IT Act or any of its rules and regulations. The person shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure. Further if the person so required under the Act or its regulations fails to file any return or furnish any information, books or other documents within the time specified in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day of the failure. Further if the person fails to maintain books of account or records as required under the IT Act or its rules or regulations, he shall be liable to a penalty not exceeding ten thousand rupees for every day of the failure. This section reads as follows:

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

(*a*) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
(*b*) file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
(*c*) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Penalty : Any person who fails to furnish any document, return or report under section 44. He shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure. Further if he fails to file any return or furnish any information, books or other documents within the time specified, shall be liable to a penalty up to five thousand rupees for every day during which such failure continues. Again in failure to maintain books of account or records, he shall be liable to a penalty up to ten thousand rupees for every day during which the failure continues.

7.3.1.4 Residuary Penalty

Section 45 of IT Act provided provision for the act(s), in contravention of rules and regulation mention under the information technology act, for which no penalty has been separately provided. This section reads as:
"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."[88]

[88] Section 45; IT Act, 2000;

Penalty: On contravention of any rules or regulations made under IT Act, 2000, for which no penalty has been separately provided, the culprit shall be liable to pay a compensation or a penalty up to twenty-five thousand rupees.

7.3.1.5 Recovery of Penalty or Compensation

Any penalty or compensation awarded under the Information technology act, if not paid by the person, to whom it has imposed, may be recovered in the same manner as an arrear of land revenue. Again his licence granted under the section 24[89] of IT Act shall be suspended. Or electronic signature certificate issued under the section 35[90] of IT Act shall be suspended.

Section 64 of IT Act, 2000 made provision in this regard as follows:

"Recovery of penalty or compensation –A penalty imposed or compensation awarded under this Act, if it is not paid, shall he recovered as an arrear of land revenue and the licence or the electronic signature Certificate, as the case may be, shall be suspended till the penalty is paid."

7.3.2 Offences Under It Act

In general terms offences committed via Information Technology is called cyber-crime. we may define cyber-crime as, - a criminal offense that has been created or made possible by the advent of computer technology or a traditional crime, which has been so transformed by the use of a computer that law enforcement investigators need a basic understanding of computers in order to investigate the crime.[91]

As per the objectives of IT Act, the act essentially deals with the issues of -legal recognition of electronic documents, legal recognition of digital signatures, offenses and contraventions and justice dispensation systems for cyber-crimes.

Information Technology Amendment Act 2008 was passed at the end of 2008. It got the President assent on 5 Feb 2009 and was made effective from 27 October 2009. There were Inclusion of some additional cyber-crimes like child pornography and cyber terrorism through this amendment. This amendment made- authorizing an Inspector to investigate cyber offenses (as against the DSP earlier).

On the contrary of traditional criminals, cyber criminals are well educated and very good in information and computer technology. Cyber-crime has no geographical boundaries and operate and affects in no time i.e. very efficiently. In comparison to other traditional crimes the degree of risk in cyber criminality is extremely low. Because cyber-criminal is physically

[89] Section 24- procedure for granting licence; see IT Act 2000;

[90] Section 35- Certifying authority to issue electronic signature Certificate; see IT Act, 2000;

[91] Cyber-crime; < https://shodhganga.inflibnet.ac.in/bitstream/10603/58938/8/08_chapter%203.pdf>

outside the cyberspace and all components of cyber criminality from preparation to execution, takes place in the cyber world. The offence of cyber-crime will cause unimaginable loss.

The offences included in the I.T. Act 2000 under chapter XI, are as follows -

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Power to issue directions for interception or monitoring or decryption of any information through any computer resource.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Let us discuss them under separate headings.

7.3.2.1 Tampering With Computer Source Documents

According to section 65 of IT Act,

"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."

Aforesaid section protect the "intellectual property" invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law. It also applies to a person who intentionally causes another person to do the same.

Mens rea is the main ingredient under this section.

Again 'conceal' meaning to hide or to take away from the view or steal, 'destroy' meaning causing destruction or deletion and 'alter' meaning to make changes. Hence the culprit with *mens rea* shall conceal, destroy or alter any 'computer source code' then it is an offence under

section 65 IT Act. The meaning of 'computer source code' has been make clear in the explanation of the section.

Penalty – Imprisonment of up to three years or a fine of up to two lakh rupees, also both in some cases.
This is cognizable and non-bailable offence.

Related case: In the case of *Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh& Ors 2005CriLJ 4314*, Tata Indicom employees were arrested for manipulation of the electronic 32-bit number (ESN) programmed into cell phones theft, which were exclusively franchised to Reliance Infocomm. The Court held that tampering with source code invokes Section 65 of the Information Technology Act.

7.3.2.2 Computer Related Offences (Hacking With Computer System)

Section 66 of IT Act says:
"If any person, dishonestly or fraudulently, does any act referred to in section 43[92], 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 (45 of 1860);[93]
(*b*) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).[94]

In a brief account of Section 43, we can say that it applies if any person, without the permission of the owner or the person in charge of a computer, system, or network –

- Accesses such computer, network or system.
- Copies, downloads or extracts any data or information from such computer, network or system (this also includes the information or data stored in a removable storage medium).
- Also, introduces or causes any computer containment or virus into such computer, network or system.
- Further, he damages any computer, system or data or any other programs residing in them.
- Disrupts or causes disruption of any such computer, system or network.

[92] For detail see 7.3.1.1 PENALTY AND COMPENSATION FOR DAMAGE TO COMPUTER, COMPUTER SYSTEM, ETC.

[93] "Dishonestly".—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".

[94] "Fraudulently".—A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

- Also, denies or causes the denial of access to an authorized person to such computer, system or network.
- Provides any assistance to anyone to facilitate access to such a computer, system or network contrary to the provisions of the Act and its rules.
- Also, charges the services availed of by one person to the account of another by tampering with such computer, system or network.

Section 66 applies to a person who commits hacking. "Hacking" means unauthorised access to a computer system. It is most common type of cyber-crime. Hacking is when the person intentionally or knowingly causes a wrongful loss or damage to the public or another person or destroys or deletes any information residing in a computer resource or diminishes its utility or value or injures it by any means. *Mens rea* is a necessary element under this section.

Penalty : Any person who contravene the provision of section 66 i.e. does any act referred to in section 43, punishes with imprisonment up to three years or with fine up to five lakh rupees or with both.

7.3.2.2.1 Punishment for Sending Offensive Messages through Communication Service, Etc.

Section 66A of IT Act says that,

"Any person who sends, by means of a computer resource or a communication device,–
(*a*) any information that is grossly offensive or has menacing character[95]; or
(*b*) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;
(*c*) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,
shall be punishable with imprisonment for a term which may extend to three years and with fine.
Explanation.–For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

Penalty: Any person convicted under section 66A shall be punishable with imprisonment for a term which may extend to three years and with fine.

Struck down of Section 66-A by the Hon'ble Supreme Court of India:

[95] Something that is *menacing* is threatening or suggestive of coming danger.

It is noteworthy to mention here that the Supreme Court struck down Section 66A of the Information Technology Act, 2000, relating to restrictions on online speech, unconstitutional on grounds of violating the freedom of speech guaranteed under Article 19(1)(a) of the Constitution of India. The Court further held that the Section was not saved by virtue of being 'reasonable restrictions' on the freedom of speech under Article 19(2). The case was a watershed moment for online free speech in India.

The back ground of the issue is that two girls were arrested by the Mumbai police in 2012 for expressing their displeasure, by posting their remarks over their facebook profiles at the bandh called in the wake of Shiv Sena chief Bal Thackery's death.

Although the police later released the women and dismissed their prosecution, the incident invoked substantial media attention and criticism. The women then filed a petition, challenging the constitutional validity of Section 66A on the ground that it violates the right to freedom of expression.

Dealing with the word "grossly offensive", the bench referred to the judgement cited by the Additional Solicitor General (ASG) and said, "What is grossly offensive to you, may not be grossly offensive to me and it is a vague term." Justice Nariman even gave an example to the court of how the vague definition of 'grossly offensive' could be dangerously twisted.[96]

Alterative provisions and effects of struck down of Section 66-A :

After the verdict of apex court, the question is, if cases are reported attracting the provisions given in 66-A IT Act, what to do. The answer is, relevant sections of IPC cab be apply under such situations. For example, in the case of online stalking and harassment section 354-D of IPC can be invoked. Section 509 of IPC can also be invoked. According to the situation 354-A IPC sexual harassment (making sexually coloured remarks, shall be guilty of the offence of sexual harassment) may also be relevant.[97]

Further, act for communal sensitive remarks and degrading the gods or goddesses of the different religions also invoked the provision of 66A. In that case police may have to look for the provisions 153A[98] and 505(2)[99] that are relevant under Indian Penal Code as per the situation, the contents of the complaint and nature of the offence.

Social networking media refer to the mode of communication among people on the cyber space with use of Internet. These include social media networking sites (Facebook), micro blogging

[96] < https://www.firstpost.com/living/who-defines-grossly-offensive-sc-raises-red-flags-over-draconian-sec-66a-of-it-act-2079081.html>

[97] For detail see previous unit-6 : TRESSPASS, DEFAMATION, STALKING, SPAM

[98] 153A says about, Promoting enmity between different groups on ground of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony. (see glossary)

[99] Section 505(2) of IPC says about, Statements creating or promoting enmity, hatred or ill-will between classes. This section reads as, —"Whoever makes, publishes or circulates any statement or report containing rumour or alarming news with intent to create or promote, or which is likely to create or promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, feelings of enmity, hatred or ill will between different religious, racial, language or regional groups or castes or communities, shall be punished with imprisonment which may extend to three years, or with fine, or with both."

sites (Twitter), video sharing websites (Youtube), wikis (Wikipedia) etc. The following different variants of offences may be reported with regard to the Facebook-[100]

- Creating impersonating profiles with the identities like name, photographs of the victim.
- Sending and posting obscene content.
- Hacking of a profile.
- Sending obscene and derogatory content to a profile.
- Posting material which hurts the feelings and sentiments of a community.

7.3.2.2.2 Punishment for Dishonestly Receiving Stolen Computer Resource or Communication Device

The section tells about the hacking activity. *Mens rea* is a main ingredient under this section also.

Section 66B of IT Act states that,
"Whoever dishonestly receive 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."

In the above section the resource of computer means- software and other content which are computer based. Hence this section does not confine to the physical theft, even if the resource of the computer i.e., software etc. is received by anyone with knowledge of that, it was stolen, then also the section applies. In this way, this section has the relevance for violation of intellectual property rights.
"**Dishonestly**" means "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**"."[101]

Essential ingredients of the section:
1. Whoever does intentionally, anything causing wrongful gain to one person or wrongful loss to another person?
2. Receive stolen software and other content which are computer based; or
3. Retain stolen software and other content which are computerHe must aware of the fact that, above software and other content which are computer based, are stolen.

Penalty: Any person convicted under section 66B shall be punished with imprisonment of a term which may extend to three years or with fine up to rupees one lakh or with both.

[100] <http://cybercrimedetective.com/wp-content/uploads/2017/04/07-Cyber-Stalking-354-D-SOP.pdf>

[101] Section 24 in the Indian Penal Code.

7.3.2.2.3 Punishment for Identity Theft

'Identity theft' means the phenomenon of stealing another person's identity.

Section 66C of IT Act, reads as follows:
"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."

Identity theft occurs when someone steals others identity and pretends to be other to access resources such as credit cards, bank accounts and other benefits in other's name. The imposter may also use other's identity to commit other crimes. "Credit card fraud" is a wide ranging term for crimes involving identity theft where the criminal uses other's credit card to fund his transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is any pre-approved card falling into someone else's hands.
A more serious concern is the use of any one's personal information with the help of stolen or fake documents to open accounts (or even worse, using one's existing account) to take a loan on that name. These unscrupulous people can collect others personal details from mailbox or trash can (remember to shred all sensitive documents). Think of all the important details printed on those receipts, pay stubs and other documents. The victim won't know a thing until the credit card people track him down and tail until he/she clear all his/her dues.
Often people forget to collect their copy of the credit card receipt after eating at restaurants or elsewhere when they pay by credit card. These receipts have their credit card number and signature for anyone to see and use. With only this information, someone can make purchases online or by phone. Also used airline tickets has traveller's information in the form of QR code. If discarded irresponsible manner it will make big problem.

Penalty: A person committing identity theft will be punished with imprisonment up to 3 years or fine up to Rs.1 lakh or with both.

Related case: *CBI vs Arif Azim, 2003/ Sony Sambandh.com case* : The accused Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site. The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code.
Besides being the first conviction in a cybercrime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cyber-crimes which are not covered under the Information Technology Act 2000.

7.3.2.2.4 Punishment for Cheating By Personation by Using Computer Resource

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.[102]

Section 66D of IT Act reads as follows:
"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."

Above section apply when a person who by use of computer resource or computer device cheats another by pretending to be some other person. it is basically cheating by personation through e-mails and other electronic resource taking the names of different reputed organisations, and also pretending as ambassadors, diplomats. For example, the false e-mails (electronic records) with fake certificates in the names reputed organisation like Microsoft, Yahoo etc. are sent as if they are genuine.

Penalty : Punishment for a person who is convicted under this section will be imprisoned up to 3 years and fine up to Rs. 1 lakh.

7.3.2.2.5 Punishment for Violation of Privacy

Section 66E stated for violation of privacy. This section reads as,
"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."

[102] Section 416 of Indian Penal Code;

Privacy rights refer to a person's right to be free from intrusion into their personal life by another individual, business or the government. Right of privacy also granted by Indian Constitution under article 21. The right to privacy exists in some capacity in the following situations:

- At school;
- In hotel rooms and lodges;
- In dressing rooms and bathrooms;
- Searches by law enforcement;
- In an employment setting, especially during off-work hours; and
- When dealing with medical information and reports.

Provisions of section 66E are applicable if someone – Captures, Publishes or Transmits image of a private area of any person without his or her consent, under the circumstances violating the privacy of that person. This section ensuring privacy on an individual at the places where he/she under the normal circumstances expects to be in a private environment.

In an incident a 58-year old man was arrested for installing spy cameras in his house to 'snoop' on his young lady tenants. But it was difficult for law enforcement agencies to book him under the provisions of cyber law as he was neither publishing nor transmitting the obscene material in the electronic form.[103]

Penalty : Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, shall be punished with imprisonment which extent to 3 years or with fine not exceeding Rs 2 lakhs or with both.

Related case: *Sai Priya Vs State rep by Inspector of Police,* Crl.OP No.14209 of 2016
On the complaint lodged by the petitioner, the respondent police have registered a case in Cr.No.5 of 2016 on 30.03.2016 for an offence u/s 498-A IPC against Sathyanarayana, the husband of the petitioner. It is the grievance of the petitioner that her husband took her to Pondicherry for honeymoon and after forcibly making her to consume liquor had taken photos of her in nude position and is blackmailing her. Even in the complaint given by the petitioner, she has made averments in connection with this allegation and it is supported by a SMS message that is said to have been sent by Satyanarayana, wherein he has stated that "I have nude photos of your daughter".
The Court directs the respondent police to take all these factors into consideration and alter the FIR, so as to include the offence under Section 66E of the Information Technology Act, if so advised. With the above direction, this petition is ordered.[104]

7.3.2.2.6 Punishment for Cyber Terrorism

[103] <https://www.chmag.in/articles/legalgyan/section-66e-punishment-for-violation-of-privacy-policy/>

[104] < https://acadpubl.eu/hub/2018-119-17/2/129.pdf>

Cyber terrorism is a criminal act accomplish by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

Section 66F provided provisions on 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 data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base 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.

Intention is a primary ingredient to strike terror in the person's mind or menace to the unity, integrity, security or sovereignty of India, through,

1. denial of access to any person from using any virtual resource which he is authorized for;
2. unauthorized access of computer resource; or
3. introducing or causing to introduce any computer contaminant.

There should be causing or likely to cause

1. death or injury to person or
2. damage or destruction of property or
3. damage or disruption of supplies.

There should be unauthorised penetrating or accessing a computer resource, knowingly or intentionally and obtaining access to restricted information, data or computer database or any protected system declared by appropriate government under section 70 of this Act.

Penalty : Any person who with the intent to threaten the unity, integrity, security or sovereignty of India shall be punished with imprisonment which may extend to imprisonment for life.

Cyber Terrorism can be done by- Data Theft[105] and/or Network Damage and/or Privacy Breach[106] and/or Unauthorized access[107] and/or Distributed Denial Service of Attack.[108]

7.3.2.3 Punishment For Publishing Or Transmitting Obscene Material In Electronic Form

The definition of obscene is "likely to deprave and corrupt" the audience for which it is intended and includes not only sexually explicit material but material relating to violence and drug taking.
Section 67 of IT Act make crime the pornography in electronic form. This section is parallel to 292 IPC which make pornography a crime in form of books, pamphlets, posters etc..

Section 67 reads as:
"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."

Above section is applicable to the pornographic websites, and also for acts of sending, transmitting or circulation of obscene e-mails.
'Lascivious' means something which excites lust in a person. The word 'Prurient interest' here means which is drawn by lustful thoughts. And 'tend to deprave and corrupt' means to draw a person towards becoming immoral or bad morally. Hence anything which is lascivious or appeals to the prurient interest or if its effect tends to deprave and corrupt persons are said to be obscene.[109]
Exception : the provision this section does not apply to any contents in any form if such contents has scientific, literary, artistic value or that has bona fide use for religious purposes.

---

[105] Data theft is the act of stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information.

[106] A *privacy breach* occurs when someone accesses information without permission.

[107] Unauthorized access is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods.

[108] A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource.

[109] < https://blog.ipleaders.in/obscene-material-electronic-form/>

Penalty: On first conviction culprit will punishes with imprisonment of either description for a term which may extend to three years and with fine, may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment may extend to five years and also with fine which may extend to ten lakh rupees.

7.3.2.3.1 Punishment For Publishing Or Transmitting Of Material Containing Sexually Explicit Act, Etc., In Electronic Form

Obscenity under IT Act, is an offense when it is published or transmitted or caused to be published in any electronic form. Published means any information which is distributed and broadcasted formally by issuing and selling copies of the same for general public. And transmission means transfer, pass, communicate, a medium for transmitting, signal etc.

Section 67A of IT Act says:

"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 refer to pornography but does not define what a sexually explicit act is or included.

Penalty : Any person who convicted under this section, on first conviction, 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.
Provision of aforesaid section also does not apply to any contents in any form if such contents has scientific, literary, artistic value or that has bona fide use for religious purposes.

The Internet has made pornography more ubiquitous than traditional media. All kinds of pornography, ranging from materials which depict naked bodies and conventional sexual activities to extreme materials which portray sexual violence, bestiality or necrophilia, are available on the Internet.
It is a bitter truth that, the sexually explicit materials which are produced to sexually stimulate viewers - have an interrelation with new media technologies. In the 21st Century, people can access pornographic materials with ease, requiring only a PC or another mobile Internet device and an Internet connection.

Relevant Case: in the case of *Janhit Manch & Others v. The Union of India*[110], a Public Interest Litigation was filed to seek a complete ban on pornographic websites. The NGO had argued that websites displaying sexually expressive content had an adverse influence, leading youth on a delinquent path.

7.3.2.3.2 Punishment For Publishing Or Transmitting Of Material Depicting Children In Sexually Explicit Act, Etc., In Electronic Form

There is no settled definition of pornography in a multi-national environment such as the Internet and cultural, moral and legal variations all around the world make it difficult to define 'pornographic content' in a global society. However, the production and distribution of child pornography on the Internet is illegal in the US, India and many other countries.

Section 67B of IT Act, states the punishment for publishing or transmitting of material depicting children in sexually explicit act in electronic form. This section reads as follows:

"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 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.

[110] In the High Court of Bombay, PIL NO.155 OF 2009

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

This section provides a great protection to children and prohibits child pornography. As provided in the section browsing, watching pornography within the confines of four walls which can in one's bedroom, cyber café and whatever is an offence.
Bonafide heritage material being printed or distributed for the purpose of education or literature etc are specifically excluded from the coverage of this Section, to ensure that printing and distribution of ancient epics or heritage material or pure academic books on education and medicine are not unduly affected.

Penalty : In case of first conviction imprisonment of either of up to five years and a fine which may extend to ten lakh rupees. For subsequent conviction imprisonment of up to seven years and a fine of up to ten lakh rupees.

7.3.2.3.3 Preservation And Retention Of Information By Intermediaries

"intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, Online-auction sites, online-market places and cyber cafes.[111]

Section 67C of IT Act, says,

"(*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 also be liable to fine."

According to IT Act, intermediary includes;

(1) telecom service providers,
(2) network service providers,
(3) internet service providers,
(4) web-hosting service providers,
(5) search engines,
(6) online payment sites,
(7) online-auction sites,
(8) online-market places and
(9) Cyber cafes.

[111] Section 2(*w*) of IT Act, 2000;

Hence section 67C states that aforesaid intermediary must protect and kept in possession the specified information for a fixed time period and in such method and format as directed by central government.
In the exercise of aforesaid provisions of IT Act, the central government enacted the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.
Digi locker is a secure cloud based platform for storage, issuance and verification of documents & certificates in a digital way. Launched by the Government of India, it is a key initiative under the Digital India Program.

Penalty: Any person who contravene the provision of section 67C) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.

7.3.2.4 POWER OF CONTROLLER TO GIVE DIRECTIONS

"Controller" means the Controller of Certifying Authorities appointed under sub-section (1) of section 17.[112]

Section 68 of IT Act states the provision relating power of controller to give direction. This section says,

"(*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."

According to the provisions of IT Act the Controller of Certifying Authorities (CCA) provides license and regulate the working of Certifying Authorities and also to ensure that none of the provisions of the Act are violated. The Certifying Authorities (CAs) issue Digital Signature Certificates(DSC) for electronic authentication of users.
"Certifying Authority" means a person who has been granted a licence to issue a electronic signature Certificate under section 24.[113]

Penalty : Any person who fails to comply with any order or direction given by the controller under this act, shall be guilty of an offense under section 68 and shall be convicted for a term not less than three years or to a fine exceeding two lakh rupees or to both.

7.3.2.4 Power To Issue Directions For Interception Or Monitoring Or Decryption Of Any Information Through Any Computer Resource

[112] Section 2(*m*) of IT Act, 2000;
[113] Section 2(*g*) of IT Act, 2000;

Section 69 of IT Act, states about power to issue directions for interception[114] or monitoring[115] or decryption[116] of any information through any computer resource. In other words these provisions gives power to government for cyber **-surveillance**.

Section 69 reads as follows:

"(*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.

According to provisions aforesaid, Central or State Government or any of its officers for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause the same to do any information generated, transmitted, received or stored in any computer resource, if satisfied that it is necessary or expedient so-

1. In the interest of the sovereignty or integrity of India or
2. Defense of India or

[114] "Interception" means the action or fact of receiving electronic transmissions before they reach the intended recipient.

[115] "monitoring" includes to view or to inspect or listen to or record information by means of a monitoring device;

[116] "decryption" means the process of conversion of information in non-intelligible form to an intelligible form via a mathematical formula, code, password or algorithm or a combination thereof; section 2(*f*), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

3. Security of the State or
4. Friendly relations with foreign States or
5. To maintain public order or
6. For preventing incitement to the commission of any cognizable offence or
7. For investigation of any offence

The subscriber[117] or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

In the exercise of the powers conferred by aforesaid section of the Information Technology Act, 2000 (21 of 2000), the Central Government makes rules called, the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009. These rules explain the procedure and safeguards subject to which such interception or monitoring or decryption may be carried out.

Penalty : The subscriber or any person who fails to comply the provision of section 69(3) shall be punished, imprisonment up to seven years also be liable to fine.

The recent notification issued by the Ministry of Home Affairs[118] authorises 10 Central government agencies as agencies for the purpose of interception, monitoring and decryption of data in any computer resource.

7.3.2.5.1 Power To Issue Directions For Blocking For Public Access Of Any Information Through Any Computer Resource

In the national interest IT Act, 2000 gives power to the government to issue directions for blocking for public access of any information through any computer resource, under section 69A.

Section 69A of IT Act states that,

(*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.

[117] Subscriber" means a person in whose name the electronic signature Certificate is issued. Section 2(zg) of IT Act, 2000

[118] Dec. 21 2018; < https://www.firstpost.com/tech/news-analysis/mha-notification-authorised-agencies-dont-have-suo-motu-powers-to-issue-interception-monitoring-directions-5772101.html>

(*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 also be liable to fine.

As per the provision, in the exercise of powers conferred under section 69A, with prescribed procedure and safeguard, the Central Government or any of its officers- 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. if satisfied that it is necessary or expedient so-

1. In the interest of the sovereignty or integrity of India or
2. Defense of India or
3. Security of the State or
4. Friendly relations with foreign States or
5. To maintain public order or
6. For preventing incitement to the commission of any cognizable offence or
7. For investigation of any offence

Again the reasons behind the aforesaid order should be recorded in writing.

Government has passed the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 to be read with Sec. 69A (2). These rules explain the procedure and safeguards subject to which such blocking for access by the public may be carried out.[119]

Penalty : The intermediary, who fails to comply with the direction issued under this Section, shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

7.3.2.5.2 Power To Authorise To Monitor And Collect Traffic Data Or Information Through Any Computer Resource For Cyber Security

Section 69B makes provisions for enhancing cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country. According to this section,
(*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 or 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

[119] < https://www.chmag.in/articles/legalgyan/powers-of-government-under-the-information-technology-act-2000/>

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 any 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, data, size, duration or type of underlying service and any other information.

This section gives the power to the Central Government to authorize any agency of the government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource for the purpose of enhancing cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country.

Government has passed Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009, which explains the procedure and safeguards for monitoring and collecting traffic data or information.

Penalty : Any intermediary who intentionally or knowingly contravenes the provisions of this section shall be punished with an imprisonment for a term which any extend to three years and shall also be liable to fine.

"Intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.[120]

Relevant case : In August 2007, Lakshmana Kailash K., a techie from Bangalore was arrested on the suspicion of having posted insulting images of Chhatrapati Shivaji, a major historical figure in the state of Maharashtra, on the social-networking site Orkut. The police identified him based on IP address details obtained from Google and Airtel -Lakshmana's ISP. He was brought to Pune and detained for 50 days before it was discovered that the IP address provided by Airtel was erroneous. The mistake was evidently due to the fact that while requesting information from Airtel, the police had not properly specified whether the suspect had posted the content at 1:15

[120] Section 2(*w*) of IT Act, 2000;

p.m.
Verdict: *Taking cognizance of his plight from newspaper accounts, the State Human Rights Commission subsequently ordered the company to pay Rs 2 lakh to Lakshmana as damages. The incident highlights how minor privacy violations by ISPs and intermediaries could have impacts that gravely undermine other basic human rights.*

7.3.2.6 Protected System

Section 70 grants the power to the appropriate government to declare any computer, computer system or computer network, to be a protected system. Only authorized person has the right to access to protected system. This section reads as follows:

(*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.

As per the provision of above section The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorize the persons who are authorized to access notified protected systems.

Government has passed The Information Security Practices and Procedures for Protected System Rules, 2018 under section 70 of the IT Act 2000. These rules explain the information security practices and procedure for protected system.

"The term "protected system"--
(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof,

software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage." [121]

Penalty : 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 up to ten years and shall also be liable to fine.

7.3.2.6.1 National Nodal Agency

National nodal agency for all measures to protect nation's critical information infrastructure. Protect and deliver advice that aims to reduce the vulnerabilities of critical information infrastructure, against cyber terrorism, cyber warfare and other threats.
Section 70A of IT Act makes provisions for national nodal agency. According to this section,

(*1*) The Central Government may, by notification published in the Official Gazette, designate any organisation of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.
(*2*) The national nodal agency designated under sub-section (*1*) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.
(*3*) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

National Critical Information Infrastructure Protection Centre (NCIIPC) is an organization of the Government of India created under Sec 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on 16th Jan 2014. Based in New Delhi, India, it is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection.
NCIIPC's vision is to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors of the Nation. its team is constantly dealing with challenges in Cyber Security, Information Technology (IT), Operational Technology (OT), Policy, Regulations that target the overall security of Critical Information Infrastructure (CII).

NCIIPC aims to create resilient and robust framework for protection of CII by building collaborative framework among various stake holders and supports stronger communities. The Internship program is designed to be aligned with the Latest Trends and Global Best Practices in ICT Security especially focused towards protection of CII.[122]

[121] < https://definitions.uslegal.com/p/protected-system/>

[122] < https://nciipc.gov.in/NCIIPC_internship.html>

The government passed Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013 to prescribed manner of performing functions and duties of the agency.

7.3.2.6.2 Indian Computer Emergency Response Team To Serve As National Agency For Incident Response

A computer emergency response team (CERT) is a group of experts who respond to cybersecurity incidents. These teams deal with the evolution of malware, viruses and other cyberattacks. It is a statutory organisation under the Department of Electronics and Information Technology, Ministry of Communications and Information Technology. The CERT-In was officially inaugurated on 19th January, 2004. It is generally denoted either as "ICERT" or "CERT-IN".

Section 70B of IT Act, provided provisions relating CERT as follows:

(*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 white papers relating to information security practices, procedures, preventation, 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 centres, body corporate and any other person.
(*7*) Any service provider, intermediaries, data centres, 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*).

In exercise of provision under section 70B (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. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services. CERT-In has been serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents;
- Forecast and alerts of cyber security incidents;
- Emergency measures for handling cyber security incidents;
- Coordination of cyber incident response activities;
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
- Such other functions relating to cyber security as may be prescribed.

For carrying out the aforesaid activities, the CERT-In has been vested with the powers to call for information and give directions to the service provides, intermediaries, data centres, body corporate and any other person. It may be noted that the court can take cognisance of offence under this section only on a complaint made by an officer authorised in this behalf by the CERT-In.[123]

The government passed Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013. It prescribes manner of performing functions and duties of the agency.

Penalty : Failure to provide the requisitioned information is a punishable offence with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both under Section 70B (7).

7.3.2.7 PENALTY FOR MISREPRESENTATION

There are three main types of misrepresentation- fraudulent, negligent, and innocent. Innocence is not amount to offence at all. Negligence is an important legal concept. It's usually defined as the failure to use the care that a normally careful person would in a given situation. Misrepresentation of facts before any government authority is a crime. If the person has knowledge of or reason to believe that the facts presented by him are not true. Again, if any person does not disclosed the facts, it amount the suppression of facts, it also constitutes a crime.

Section 71of IT Act, provided penalty for misrepresentation or suppression of material facts during obtaining of any licence or electronic signature before the controller or certifying authority. This section reads as follows:

[123] <http://www.merinews.com/article/cert-in-to-serve-as-national-agency-for-incident-response/15794566.shtml&cp>

"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 term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."
Any person who obtain any licence or electronic signature Certificate through misrepresentation or surpassing any material fact before the authority. He/she commit a crime under section 70 of IT Act.

Penalty : Imprisonment which may extend to two years or fine may extend to one lakh rupees or with both.

A misrepresentation is a false statement of a material fact made by one party which affects the other party's decision in further activity on its behalf. If the misrepresentation is discovered, that activity made on false facts, be declared void and, depending on the situation, the adversely impacted party may seek damages. Misrepresentation applies only to statements of fact, not to opinions or predictions.

7.3.2.8 Penalty For Breach Of Confidentiality And Privacy

One of the objectives of the enactment of the Information Technology Act, 2000, the Indian Parliament to provide a new legal idiom to data protection and privacy. The meaning of the word confidentiality and privacy are somewhat synonymous. Confidentiality involves a sense of 'expressed or 'implied basis of an independent equitable principle of confidence. Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.[124] Right to privacy is granted by the article 21 of ours Constitution. It also included right to let alone.

Section 72 of IT Act provided penalty for breach of confidentiality and privacy in the following words:
"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."

This section relates to any person who in pursuance of any of the powers conferred by the Act or it allied rules and regulations have secured access to any: Electronic record, books, register, correspondence, information, document, or other material.

[124] <http://www.legalserviceindia.com/article/l288-Breach-of-privacy-&-Confidentiality-.html>

Penalty : Any person who have been conferred powers under this Act, Rules or Regulation made there under, if discloses such information, he will be punished with imprisonment of a term which may extend to two years or fine up to one lakh rupees or with both.

The aforesaid section confines itself to the acts and omissions of those persons, who have been conferred powers under this Act, Rules or Regulation made there under, thus has a limited application only. It would not apply to disclosure of personal information of a person by a website, by his email service provider.

7.3.2.8.1 Punishment For Disclosure Of Information In Breach Of Lawful Contract

From last few years, India is playing crucial role in outsourcing business. Outsourcing has been started with call centres and later on it developed into BPO, KPO, LPO and many other outsourcings forms. These outsourcing companies are becomes an important part of Indian economy. Most of outsourcing companies deal with the foreign client's data i.e. third party information and hence it is necessary for these companies to deal with such third party information very carefully with due diligence so as to avoid misuse of such information. Hence Indian Information Technology Act, 2000 has provisions under sec.72A which was inserted by an amendment made in Information Technology Act in 2009[125].

Section 72A reads as follows:
"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."

The outsourcing companies deal with third party data and personal information of clients, customers etc. as they are having contractual relationship between them. While affording services under the term of their contractual relationship, these intermediaries are permitted to have secured access to clients /any other person's personal information. If the party or the intermediary discloses this information to any other person in default of consent or in breach of their contractual relationship, it amounts to commit an offence under section 72A, which provided punishment for act of discloses information in breach of lawful contract.[126]

[125] w.e.f. 27-10-2009.

[126] <http://www.manupatrafast.com/articles/PopOpenArticle.aspx?ID=31ffaabf-0a2b-4368-81d3-275b7e8c449e&txtsearch=Source:%20www.mightylaws.in>

Penalty : The offender, for breach of lawful contract under IT Act, is punishable with imprisonment for a term which may extend 3 years or fine which may extend to 5 lakh rupees or with both.

7.3.2.9 Penalty For Publishing Electronic Signature Certificate False In Certain Particulars

The traditional signatures are hand written and are uniquely representative of one's identity. The online transaction requires unique and strong protection which is served by electronic signature.

The concept of digital signature was introduced through Information Technology Act 2000 in India, which is enhanced with hybrid concept of electronic signature which is based on UNCITRAL Model Law on Electronic Signatures 2001. The electronic signature is a technologically neutral concept and includes a digital signature. The object and purpose of electronic signature are similar to that of traditional signature. In cyber world electronic signature ensures that the electronic records are authentic and legitimate as electronic signature are safer and cannot be forged and is convenient as the sender himself does not have to be present personally at the place to contract to sign the document. For example a person can sign a contract in India and send it to any part of the world to complete the transaction.[127]

The legal recognition of electronic signature has been provided under section 5 of information technology Act 2000. This section equates electronic signature as traditional handwritten signature.

Digital signature certificate are provided by certifying authority under provisions of Indian Technology Act. "Certifying Authority" means a person who has been granted a licence to issue electronic signature Certificate under section 24.[128] Section 24 provided Procedure for grant or rejection of licence.[129]

An "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35[130] and includes Digital Signature Certificate[131].

While issuing a Digital Signature Certificate, a Certifying Authority shall certify that--[132]

(a) it has complied with the provisions of this Act and the rules and regulations made thereunder.
(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it.
(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate.
(d) the subscriber's public key and private key constitute a functioning key pair.
(e) the information contained in the Digital Signature Certificate is accurate, and

[127] < http://www.legalservicesindia.com/article/1827/Electronic-Signature:-Legal-and-Technical-aspect.html>

[128] Section 2(g) of IT Act, 2000;
[129] See section 24, IT Act, 2000;
[130] Section 35- Certifying authority to issue electronic signature Certificate; Refer IT Act, 2000;

[131] Section 2(tb) of IT Act, 2000;
[132] Section 36 of IT Act, 2000;

(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

According to the IT Act, "subscriber" means a person in whose name the electronic signature Certificate is issued[133].

Digital Signature Certificates contains Public key of the certificate owner, Name of the owner, Validity "from" and "to" dates, Name of the issuing authority, Serial number of the certificate, Digital signature of the issuing authority name of the person, etc.
Publication of electronic signature certificate which is false in certain particulars is an offense under section 73 of the Act.

Section 73 of IT Act, reads as follows:
"(*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 purpose of verifying a electronic signature created prior to such suspension or revocation.

Penalty : 73(*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."

Hence section 73 of IT Act made an offence if any person publish electronic signature certificate with aware of the fact that, the certificate has not issued by the CA listed in the certificate or the person in whose name the electronic signature Certificate is issued, has not accepted it or the certificate has been revoked or suspended by the certification authority. Clause 2 of this section provided punishment for this crime.

The Certifying authority also has right to suspend the Digital Signature Certificate if it is of the opinion that the digital signature certificate should be suspended in public interest.

A digital signature may not be revoked unless the subscriber has been given opportunity of being heard in the matter. On revocation, the Certifying Authority need to communicate the same with the subscriber. Such publication is not an offense, it is the purpose of verifying a digital signature created prior to such suspension or revocation.[134]

[133] Section 2(zg) of IT Act, 2000;
[134] < https://www.lawctopus.com/academike/offences-act-2000/>

Suspension and revocation of digital signature certificate are given under the section 37[135] and 38[136] of the IT Act respectively.

Relevant case : In the case of *Bennett Coleman & Co. v. Union of India* AIR 1973 SC 106, the publication has been stated that 'publication means dissemination and circulation'. In the context of the digital medium, the term publication includes transmission of information or data in electronic form.

7.3.2.10 Publication For Fraudulent Purpose

Fraud is generally defined in the law as an intentional misrepresentation of material existing fact made by one person to another with knowledge of its falsity and for the purpose of inducing the other person to act, and upon which the other person relies with resulting injury or damage. Fraudulent purpose inherent intent to deceive other.

When a person, knowingly creates, publishes or makes available a digital certificate with the intention of fraud. He or she commit crime under section 74 of IT Act.

Section 74 of IT Act reds as follows:
"Whoever knowingly creates, publishes or otherwise makes available a 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."

According to this section following acts come under crime:

- When a person knowingly creating a digital signature certificate for any, fraudulent purpose or unlawful purpose;
- When a person knowingly publishing a digital signature certificate for any fraudulent purpose or unlawful purpose; and
- When a person knowingly making available a digital signature certificate for any fraudulent purpose or unlawful purpose.

Penalty : Anyone who commit under aforesaid section will punishes with imprisonment up to two years or a fine of up to one lakh rupees, or with both.

The growing online transactions and contracts requires stronger protection which is currently fulfilled by digital signature. It would be in the interest of cyber community if the Government allows and initiate multiple method of authentication like the use of fingerprint or Aadhaar card linked with password based online transaction. The multiple methods would permit easy

[135]Section 35- Suspension of Digital Signature Certificate; Refer IT Act, 2000;

[136] Section 35- Revocation of Digital Signature Certificate; Refer IT Act, 2000;

identification of persons which will assist in curbing online frauds and ease online transaction and further enhance online security of users.[137]

7.3.2.11 Act To Apply For Offence Or Contravention Committed Outside India

Cyber-crimes are the most dangerous of all the crimes because the magnitude of loss it is causing goes in billions. It can be committed very easily, without disclosing the identity, from any part of the world. The Internet is analogous to the high seas. No one owns it, yet people of all nationalities use it. The new millennium is witnessing a new form of crime, which can be done through Internet. As Internet is decentralized, person can commit crime from anywhere in the world.
Section 1(*2*) of IT Act says about its applicability outside India, "it applies also to any offence or contravention thereunder committed outside India by any person." Section 75 of Act make provision in this regard.

Section 75 of It Act reads as follows:
(*1*) Subject to the provisions of sub-section (*2*), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
(*2*) For the purposes of sub-section (*1*), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Aforesaid section has a broader perspective including cyber-crime, committed by cyber criminals, of any nationality, any territoriality.
An offence would typically contain these elements, i.e.-

- The victim
- Computer involve in committing offence
- Computer system used to commit the offence
- Computer network used to commit offence
- The computer system affected by offence
- The offender

An act will be categorise as an offence under the purview of Information Technology Act, 2000 if any one of the element aforesaid are located in India.

Relevant case : *R v. Governor of Brixton prison and another* [1969] 2 QB 222, [1969] 2 All ER 347, [1969] 2 WLR 618, 133 JP 407

Facts: In this case the Citibank faced the wrath of a hacker on its cash management system, resulting in illegal transfer of funds from customers account into the accounts of the hacker, later identified as Valdimer Levin and his accomplices. After Levin was arrested he was

[137] <http://www.legalservicesindia.com/article/1827/Electronic-Signature:-Legal-and-Technical-aspect.html>

extradited to the United States. One of the most important issues was the jurisdictional issue, the 'place of origin' of cyber-crime.

Held: The Court held that the real-time nature of the communication link between Levin and Citibank computer meant that Levin's keystrokes were actually occurring on the Citibank computer. It is thus important that in order to resolve the disputes related to jurisdiction, the issue of territoriality and nationality must be placed by much broader criteria embracing principles of reasonableness and fairness to accommodate overlapping or conflicting interests of states, in spirit of universal jurisdiction.[138]

7.3.2.12 Confiscation

Confiscation is a legal form of seizure by a government or other public authority.

Section 76 of IT Act said about confiscation in the following words:
"Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:
Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit."

The aforesaid section provided that all devices whether computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device which helped in the contravention of any provision of this Act, rules, orders, or regulations made under there under liable to be confiscated.
This section made provision for, any digital device which involves in contravention of any rule, orders or regulations made under this act, in other words used in an offence, would be seizure by cyber-crime investigating authority. Hence helps in investigation of digital crime giving power to the investigating authority to seize devices used in crime.

7.3.2.13 Compensation, Penalties Or Confiscation Not To Interfere With Other Punishment

Section 77 of IT Act said that compensation, penalty or confiscation under IT Act, does not interfere with any other punishment given under any other law for the time being in force. The

[138] < https://www.lawctopus.com/academike/offences-act-2000/>

punishment made under IT law provides no excuse for other compensation or imposition of any other penalty or punishment under any other law for the time being in force.

Section 77 reads as follows:
"No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force."

The aforesaid section lays down a mandatory condition, which states the Penalties or confiscation not to interfere with other punishments to which the person affected thereby is liable under any other law for the time being in force.

The massage from above section made clear that if a person contravene the provision of IT Act and got punishment under it and at same time if he/ she find guilty under any other law for time being in force and also got punishment under that law, both punishment will apply on him i.e. the culprit abide by all punishment given to him under IT Act and other law.

7.3.2.13.1 Compounding Of Offences

Compoundable offences are those that can be compromised, i.e. the complainant can agree to take back the charges levied against the accused, whereas, non - compoundable offences are the more serious offences in which the parties cannot compromise.

Section 77A of IT Act, states that a court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act. In other words it tells about plea bargaining[139].

Section 77A reads as follows:
(*1*)A court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided, under this Act:
Provided that the court shall not compound such offence where the accused is, by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind:
Provided further that the court shall not compound any offence where such offence affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

[139] Plea bargaining is essentially derived from the principal of 'Nalo Contendere' which literary means 'I do not wish to contend'. The Apex Court has interpreted this doctrine as an "implied confession, a quasi-confession of guilt, a formal declaration that the accused will not contend, a query directed to the court to decide a plea guilt, a promise between the Government and the accused and a government agreement on the part of the accused that the charge of the accused must be considered as true for the purpose of a particular case only.

<http://www.mondaq.com/india/x/273094/trials+appeals+compensation/Plea+Bargaining+An+Overview>

(*2*)The person accused of an offence under this Act may file an application for compounding in the court in which offence is pending for trial and the provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 (2 of 1974) shall apply.

According to aforesaid provisions no offence shall be compounded under IT Act if –

- The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; or
- Offence affects the socio economic conditions of the country; or
- Offence has been committed against a child below the age of 18 years; or
- Offence has been committed against a woman.

Again all offences can be compounded under IT Act, other than the following:

(1) offences for which the punishment for life has been provided, under this Act; or
(2) offences for which imprisonment for a term exceeding three years has been provided, under this Act

Clause (3) of above section says about procedure for compounding. According to which, the person who is accused of an offence under IT Act, 2000 may file an application before the court of competent jurisdiction for compounding, during the pending for his trial. In this process the provisions of sections 265B and 265C of Cr.P.C. will apply.

It is now appropriate to discuss the provisions of 265B and 265C of Cr.P.C. here-

Section 265-B of Cr.P.C contemplates an application for plea bargaining to be filed by the accused which shall contain a brief details about the case relating to which such application is filed, including the offences to which the case relates and shall be accompanies by an affidavit sworn by the accused stating therein that he has voluntarily preferred the application, the plea bargaining the nature and extent of the punishment provided under the law for the offence, the plea bargaining in his case that he has not previously been convicted by a court in a case in which he had been charged with the same offence. The court will thereafter issue notice to the public prosecutor concerned, investigating officer of the case, the victim of the case and the accused for the date fixed for the plea bargaining. When the parties appear, the court shall examine the accused in-camera wherein the other parties in the case shall not be present, with the motive to satisfy itself that the accused has filed the application voluntarily.[140]

Further **Section 265-C** of Cr.P.C. prescribes the procedure to be followed by the court in working out a mutually satisfactory disposition. In a case instituted on a police report, the court shall issue notice to the public prosecutor concerned, investigating officer of the case, and the victim of the case and the accused to participate in the meeting to work out a satisfactory

[140] See Code of Criminal Procedure, 1973 (2 of 1974);

disposition of the case. In a complaint case, the Court shall issue notice to the accused and the victim of the case.[141]

It is noteworthy to mention here that under this section application for compounding cannot be file after get convicted or awarding the judgement by the court. The accused may file the application for compounding only during the pendency for trial of his case.

7.3.2.13.2 Offences with Three Years Imprisonment to Be Bailable

Section 77B of IT Act, states that offences punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

Section 77B reads as follows:
"Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable."

Cognisable offence means a police officer has the authority to make an arrest without a warrant and to start an investigation with or without the permission of a court.[142] Normally, serious offences are defined as cognisable and usually carry a sentence of 3 years or more.

The aforesaid section states that, under IT act:

(1) the offence punishable with imprisonment of three years and above shall be cognizable; and
(2) the offence punishable with imprisonment of three years shall be bailable; and

any provision of Code of Criminal Procedure, 1973 (2 of 1974), in this regard will not apply on above provision.

7.3.2.14 Power To Investigate Offences

Section 78 of IT Act states that a police officer not below the rank of Inspector shall investigate any offence under this Act.

Section 78 reads as follows:
"Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Inspector shall investigate any offence under this Act."

The Code of Criminal Procedure provides the general procedure for investigation of the crime. The conventional crime is investigated by using the regular methods. The law enforcement agencies were bound by some basic rules and procedural aspect. In case of traditional crimes,

[141] Ibid.
[142] Section 2(c) of the Criminal Procedure Code, 1973;

various physical evidences are generally available on the place of crime, collection of such physical evidence required a lot of common sense and little technical knowledge.
"Investigation" includes all the proceedings under the code for collection of evidence conducted by police officers or by any person other than magistrate who is authorized by the magistrate.[143]
In cyber-crime investigation certain special skill and scientific tools are require without which investigation is not possible. The Indian legal system introduced certain special provisions while investigating the cyber-crime. The Information Technology Act, 2000 has bound to amend certain provision of Criminal Procedure Code and the Evidence Act. Along with this, certain new regulation has enacted by the Indian legal system to meet with the need of cyber-crime investigation.
Previously cyber-crime investigation is done by the superior offices of the police. The Information Technology Act 2000 set up a special procedure for investigation and further proceeding in cyber-crime contended in the IT Act, 2000, which makes cyber-crime investigation slow. Under section 78 of the Act, an Inspector shall investigate the cyber-crime. Before the Amendment of 2008 in IT Act, the power of investigation was confer on the Deputy Superintendent of Police; the object behind this amendment is to bring the cyber-crime for investigation in mainstream as like a conventional crime. This Amendment gives power to the inspector to register and investigate the cyber-crime as like another crime.[144]

7.3.3 Miscellaneous Provisions

Chapter XIII of Information Technology Act provided some miscellaneous provisions. Those provisions relevant for this unit are as follows:

- Punishment for abetment of offences.
- Punishment for attempt to commit offences.
- Offences by companies.

Let us discus them under separate heading.

7.3.3.1 Punishment For Abetment Of Offences

Abetment is defines as an act of helping or encouraging someone to do something wrong or illegal.

Section 84 B of IT Act, stated that,
"Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

[143] Section 2(h) of the Criminal Procedure Code, 1973;
[144] < https://shodhganga.inflibnet.ac.in/bitstream/10603/203654/9/09_chapter%204.pdf>

Explanation.–An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment."

Section 84B was instituted by IT (Amendment) Act, 2009.
The offence of abetment is a separate and distinct offence provided in IPC[145]. A person abets the doing of a thing when he instigates any person to do that thing or engages with one or more other persons in any conspiracy for the doing of that thing or intentionally aids, by act or illegal omission, the doing of that thing, These things are the essentials of abetment as a complete crime.
According to aforesaid section, if an act or offence is said to be committed in consequence of abetment:

(1) **when it is committed in consequence of the instigation :** Instigating someone literally means to incite, provoke, urge or bring about by persuasion to do anything. *Mes rea* is an important ingredient of instigation. Instigation may be direct or indirection.
(2) **or when it is committed in pursuance of the conspiracy:** Abetment by Conspiracy involves two elements, first there is a conspiracy between two or more person and second an act or illegal omission may take place in furtherance of that conspiracy.
(3) **or when it is committed with the aid which constitutes the abetment :** it involves, (i) Doing an act that directly assists the commission of the crime, or (ii) Illegal omission of a duty you are bound to do, or (iii) Doing any act facilitates the commission of a crime.

it is to be noted that, mere intention to render assistance or merely being presence at the crime scene does not amount to aiding.

Penalty : The abettor of any offence will be punished with the punishment provided for the offence under this (IT) Act.

7.3.3.2 Punishment For Attempt To Commit Offences

In simple words attempt to commit offence means, where the offender ultimately fails to pull off the offence.

Section 84C was also instituted by IT (Amendment) Act, 2009. This section reads as follows: "Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both."

[145] "If the act abetted is committed and it constitutes an offence but no express provision is made for the punishment of its abetment, the abetment shall be punished with the punishment provided for the offence" (Section 109 of IPC).

Generally, attempted offenses occur when an individual has an actual intent to commit a crime , and takes direct action toward completion of the crime.
This section states that if a person attempts to commit an offence or instigates an offence to be committed thereby does an act which amounts to the offence, which is punishable under the IT Act, wherein no express provisions are made under this Act is amount to an offence under aforesaid section.

Aforesaid section has been farmed in order to punish the moral wrong committed when an attempt is made to commit an offence. An attempt is made punishable, because every attempt, although it falls short of success, must create alarm, which by itself is an injury, and the moral guilt of the offender is the same as if he had succeeded. Moral guilt must be united to injury in order to justify punishment. As the injury is not as great as if the act had been committed, only half the punishment is awarded.
Similarly section 511 of the Indian Penal Code (IPC), 1860, states the punishment for attempting to commit offences.

Penalty : For such an attempt, the culprit may be punished with a term which extends to one half of the longest term of imprisonment as can be provided for that offence, or with fine which is levied for committing such an offence , or with both the imprisonment and the fine.

7.3.3.3 Offences by Companies

A company is a separate legal entity established through legislation or registration process and considered a legal person. A company can be made liable for unlawful acts done by its agents when they are acting within the scope of authority.

Section 85 of IT Act makes provision about offences done by a company. This section reads as follows:
(*1*) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:
Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.
(2) Notwithstanding anything contained in sub-section (*1*), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly. Explanation.–For the purposes of this section,–

(*i*) "company" means anybody corporate and includes a firm or other association of individuals; and
(*ii*) "director", in relation to a firm, means a partner in the firm.

Provision of above section said about corporate responsibility. It clearly says that, that the company as well as any person who is responsible for conduct of its business are liable accordingly, unless it proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.
Further director, manager, secretary or other officer is also liable if the said offence is committed by his consent, knowledge or connivance or is result of negligence on the part of him.

Relevant case : *BPO data theft case*:
The recently reported case of a Bank Fraud in Pune in which some ex-employees of BPO arm of MPhasis Ltd MsourcE, defrauded US Customers of Citi Bank to the tune of RS 1.5 crores has raised concerns of many kinds including the role of "Data Protection".
The BPO is liable for lack of security that enabled the commission of the fraud as well as because of the vicarious responsibility for the ex-employee's involvement. The process of getting the PIN number was during the tenure of the persons as "Employees" and hence the organization is responsible for the crime.
Under ITA-2000 the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damage to the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.
Under Section 79 and Section 85 of ITA-2000, vicarious responsibilities are indicated both for the BPO and the Bank on the grounds of "Lack of Due Diligence". At the same time, if the crime is investigated in India under ITA-2000, then the fact that the Bank was not using digital signatures for authenticating the customer instructions is a matter which would amount to gross negligence on the part of the Bank.

7.4 SUMMARY

The most important feature of Internet is that, it completely ignores geographical boundary. A person by sitting at any corner of the world can communicate with other person without disclosing his identity. The strength of the Internet is - fastest communication at cheapest rate. However, it is unfortunate that Internet has its darker side too. Many of the characteristic features of Internet like, low cost, easy to use and fastest means of communication also gives rise to new forms of crimes like fraudulent scams, child pornography, hacking, and introducing viruses. Conventional law enforcement mechanism fails to resolve these new kinds of issues. It is felt that the new form of legislation is required to combat cyber-crimes.

The new millennium is witnessing a new form of crime, which can be done through Internet, which are differs from the conventional crimes. As Internet is decentralized, person can commit crime from anywhere in the world.

The IT Act has laid down the various offences and penalties in order to prevent misuse of the information technology. The Act further amends the Indian Penal Code, 1860, The Evidence Act, involves a computer, computer system or computer network located in India.

A summary of provisions related penalties and offences mentioned in The Information Technology Act, 2000 are given in the following table:

Section	Offence	Punishment
43	Damage to computer, computer system, etc.	Liable to pay damages by way of compensation to the person so affected.
43A	Body corporate failure to protect data	Liable to pay damages by way of compensation to the person so affected.
44	Any person failure to furnish information, return, etc	Penalty up to one lakh and fifty thousand rupees for each such failure
45	Residuary penalty	Penalty up to twenty-five thousand rupees
64	Recovery of penalty or compensation	Recovered as an arrear of land revenue and the licence or the electronic signature Certificate, shall be suspended till the penalty is paid.
65	Tampering with computer source documents	Imprisonment up to three years, or with fine up to two lakh rupees, or with both.
66	Computer related offences : dishonestly or fraudulently, does any act referred to in section 43,	imprisonment up to three years or with fine up to five lakh rupees or with both.
66A	Sending offensive messages through communication service, etc.	Imprisonment for a term which may extend to three years and with fine
66B	Dishonestly receiving stolen computer resource or communication device	imprisonment of either description up to three years or with fine up to rupees one lakh or with both.

66C	Identity theft.	Imprisonment of either description up to three years and fine up to rupees one lakh.
66D	Cheating by personation by using computer resource	imprisonment of either description up to three years and fine up to one lakh rupees.
66E	Violation of privacy	Imprisonment up to three years and/or fine up to two lakh rupees.
66F	Cyber terrorism	imprisonment which may extend to imprisonment for life.
67	Publishing or transmitting obscene material in electronic form	imprisonment of either description up to five years and also with fine up to ten lakh rupees.
67A	Publishing or transmitting of material containing sexually explicit act, etc., in electronic form.	imprisonment of either description up to seven years and also with fine up to ten lakh rupees.
67B	Publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.	On first conviction imprisonment of either description up to five years and with fine up to ten lakh rupees; second or subsequent conviction imprisonment of either description up to seven years and fine up to ten lakh rupees.
67C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information.	Imprisonment up to three years and also be liable to fine
68	Failure to comply with the directions given by Controller	Imprisonment up to two years or a fine up to one lakh rupees or with both
69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource.	imprisonment for a term which may extend to seven years and shall also be liable to fine.

69A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to seven years and also be liable to fine.
69B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to three years and shall also be liable to fine.
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to ten years and shall also be liable to fine.
70A	Provision about National Nodal Agency in respect of Critical Information Infrastructure Protection.	
70B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT	imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.
71	Offence of misrepresentation	Imprisonment up to two years, or fine up to one lakh rupees, or with both.
72	Breach of confidentiality and privacy	Imprisonment up to two years, or fine up to one lakh rupees, or with both.
72A	Disclosure of information in breach of lawful contract	Imprisonment up to three years, or fine up to five lakh rupees, or with both.
73	Publishing electronic signature Certificate false in certain particulars	Imprisonment up to two years, or fine up to one lakh rupees, or with both.
74	Publication for fraudulent purpose	Imprisonment up to two years, or fine up to one lakh rupees, or with both.

75	Act to apply for offence or contravention committed outside India	
76	Confiscation of electronic device involved in an offence	
77	Compensation, penalties or confiscation not to interfere with other punishment	
77A	Compounding of offences	
78B	Offences with three years' imprisonment to be bailable	
78	Power to investigate offences	
84B	Abetment of offences	Punished with the punishment provided for the offence under this Act
84C	Attempt to commit offences	Imprisonment of any description provided for the offence, up to one-half of the longest term of imprisonment provided for that offence, or fine as is provided for the offence, or with both.
85	Offences by companies - every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company	Shall be liable to be proceeded against and punished accordingly

However aforesaid provisions of IT Act, 2000 are also applicable to outside India. Yet jurisdiction of the case in cyber laws is complicated. Cyber-crime does not happen in a particular territory. It is geography less and borderless. So it gets very difficult to determine the jurisdiction under which the case has to be filed. Suppose a person works from multiple places and his data gets stolen from a city while he resides in some other city, there will be a dispute as to where the complaint should be filed.

7.5 GLOSSARY

Netizens : The term netizen is a portmanteau of the words Internet and citizen as in "citizen of the net". It describes a person actively involved in online communities or the Internet in general.

BPO, KPO, LPO : Knowledge Processing Outsourcing or KPO is a subset of BPO. KPO involves outsourcing of core functions which may or may not give cost benefit to the parent company but surely helps in value addition. LPO or Legal Process Outsourcing is special type of KPO dealing with legal services.

w.e.f. : Abbreviation for w.e.f. is With Effect From. This is mostly used to denote where the rules or prices change happens from a date mentioned.

***Mens rea* :** *Mens rea*, is mental element, i.e. a person's awareness of the fact that his or her conduct is criminal.

Section 153A of IPC : It says about Promoting enmity between different groups on ground of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony.—

(*1*) Whoever— (*a*) by words, either spoken or written, or by signs or by visible representations or otherwise, promotes or attempts to promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, disharmony or feelings of enmity, hatred or ill will between different religious, racial, language or regional groups or castes or communities, or

(*b*) commits any act which is prejudicial to the maintenance of harmony between different religious, racial, language or regional groups or castes or communities, and which disturbs or is likely to disturb the public tranquillity, or

(*c*) organizes any exercise, movement, drill or other similar activity intending that the participants in such activity shall use or be trained to use criminal force or violence or knowing it to be likely that the participants in such activity will use or be trained to use criminal force or violence, or participates in such activity intending to use or be trained to use criminal force or violence or knowing it to be likely that the participants in such activity will use or be trained to use criminal force or violence, against any religious, racial, language or regional group or caste or community and such activity for any reason whatsoever causes or is likely to cause fear or alarm or a feeling of insecurity amongst members of such religious, racial, language or regional group or caste or community, shall be punished with imprisonment which may extend to three years, or with fine, or with both.

Distributed Denial Service of Attack: A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource.

***Bonafide* :** Bona fide means "in good faith" in Latin. It stresses the absence of fraud or deception.

CrPC : The Code of Criminal Procedure (CrPC) is the main legislation on procedure for administration of substantive criminal law in India. It was enacted in 1973 and came into force on 1 April 1974.

Law for the time being in force : "Laws for the time being in force" would necessarily mean laws in force from time-to-time and not laws in force only at a fixed point of time.

Imprisonment of either description : The Indian Penal Code specifies two types of imprisonment: simple imprisonment and rigorous imprisonment. The court can award either of it. Under simple imprisonment, a convict can remain virtually idle in the prison, but has to

work compulsorily if the court awards rigorous imprisonment.

7.6 SAQS

I. Short Answer Question

13. Under which section computer contaminant is an offence?
14. When a body corporate fails to protect sensitive personal data or information. What compensation has been provided under the IT Act?
15. Any person who fails to furnish any document, return or report under section 44. What amount would be paid as a penalty for each such failure?
16. If a person contravenes any rules and regulation mention under the Information Technology Act, for which no penalty has been separately provided. Which section of the said Act applies to him?
17. Which section of IT Act provided recovery of unpaid penalty or compensation?
18. If any person temper with the computer source document. What punishment has been provided to him under the IT Act?
19. If a man found guilty for installing spy cameras in his house to 'snoop' on his young lady tenants and neither publishing nor transmitting the obscene material in the electronic form. Will the provision of section 66E apply on him?
20. If any obscene contents have scientific, literary, artistic value or that has bona fide use for religious purposes. Does it constitute a crime?
21. Which section of the IT Act, 2000 gives the power to the Central Government to authorize any agency of the government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource?
22. 'A' after being convicted of an offence under the IT Act, file an application for compounding in the court. Could he succeeded in compounding for his offence?
23. An attempt is made to commit an offence is a moral wrong. Does it punishable?
24. Which section of Information Technology Act 2000, provided legal recognition to electronic signature?

VI. Fill In The Blanks

12. Any person who fails to file any return or furnish any information, books or other documents within the time specified, shall be liable to a penalty up to ……. for every day during which such failure continues.
13. Chapter XI of the IT Act deals with various ..... .
14. Before the amendment of 2008 …… investigate cyber offences.
15. "Hacking" means unauthorised access to a …….. .
16. ……. provided punishment for those whom do any act referred to in section 43.
17. Credit card fraud is …… in its simplest form.
18. A person is said to "……." if he cheats by pretending to be some other person.
19. "……." means reproduction in the printed or electronic form and making it available for public.

20. Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to ……. .
21. Section 67 of the IT Act is parallel to section ….. of IPC.
22. A misrepresentation is a …… of a material fact made by one party which affects the other party's decision in further activity on its behalf.
23. A ……. investigation needs certain special skill and scientific tools.

VII. True And False Statement

17. "Computer virus" means a virus who enters into a computer through the hole. (True/False)
18. In failure to maintain books of account or records, a person shall be liable to a penalty up to ten thousand rupees for every day during which the failure continues. (True/False)
19. Cyber-crime has no geographical boundaries and operate and affects very efficiently. (True/False)
20. Section 65 protect the "intellectual property" invested in the computer. (True/False)
21. Cyber- terrorism is a big threat to the world, not only India. (True/False)
22. Child pornography is strictly banned in most of the countries of the world. (True/False)
23. On the issue of national interest, the government 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. (True/False)
24. The national nodal agency work against cyber terrorism, cyber warfare and other threats. (True/False)
25. Misrepresentation of facts before any government authority is a crime. (True/False)
26. Section 72 of the IT Act apply to the disclosure of personal information of a person by a website, by his email service provider. (True/False)
27. Publication of electronic signature certificate which is false in certain particulars is an offence under section 73 of the Act. (True/False)
28. Like traditional laws the provisions of the IT Act, 2000 does not apply to any offence or contravention thereunder committed outside India by any person. (True/False)
29. The offence has been committed against a woman is compoundable under It Act. (True/False)
30. In accordance with the Information Technology Act, 2000 certain provision of Criminal Procedure Code and the Evidence Act had been amended. (True/False)

7.7 REFERENCE

1. <https://acadpubl.eu/hub/2018-119-17/2/129.pdf>
2. < https://blog.ipleaders.in/obscene-material-electronic-form/>
3. <http://cybercrimedetective.com/wp-content/uploads/2017/04/07-Cyber-Stalking-354-D-SOP.pdf>

4. < https://www.chmag.in/articles/legalgyan/powers-of-government-under-the-information-technology-act-2000/>
5. < https://nciipc.gov.in/NCIIPC_internship.html>
6. < https://www.lawctopus.com/academike/offences-act-2000/>
7. < https://blog.ipleaders.in/abetment-ipc/>
8. <http://www.legalservicesindia.com/article/1827/Electronic-Signature:-Legal-and-Technical-aspect.html>
9. <https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009>
10. The Information Technology Act, 2000; Bare Act. <https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf>
11. The Indian Penal Code; Bare Act. <https://www.iitk.ac.in/wc/data/IPC_186045.pdf>
12. <https://shodhganga.inflibnet.ac.in/bitstream/10603/203654/9/09_chapter%204.pdf
13. <https://indiacode.nic.in/handle/123456789/1999?view_type=browse&sam_handle=123456789/1362>
14. <https://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/>

7.8 SUGGESTED READINGS

1. Indian Penal Code by Prof. S.N. Sharma
2. Indian Penal Code
3. Indian Technology Act, 2000
4. An Introduction to cyber Law by Dr. J.P. Mishra

7.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. Explain the penalty and compensation for damage to the computer, computer system etc.
2. Write short notes on the following:

(i) Reasonable security practices and procedures
(ii) Sensitive personal data or information
(iii) Residuary penalty
(iv) Cyber-crime
(v) Tampering with computer source document
(vi) Section 66B of IT Act
(vii) Cheating by personation
(viii) Violation of privacy
(ix) Cyber-terrorism
(x) The exception under section 67
(xi) Child pornography

(xii) Protected system
(xiii) National nodal agency
(xiv) ICERT
(xv) Confiscation under IT Act
(xvi) Compoundable offences under IT Law
(xvii) Attempt to commit offence

3. Write an essay on the offences describes under IT Act, 2000.
4. In what manner cyber-crime differ from a traditional crime?
5. What do you understand by 'hacking with computer'? explain.
6. Why supreme court struck down section 66A? Analyse the judgement giving your views.
7. If cases are reported attracting the provisions given in 66-A IT Act, what provisions apply on the offender?
8. What do you understand by "identity theft"? What punishment has been provided for this offence under the IT Act?
9. When provisions of section 66E are applicable?
10. Section 67 of the IT Act make crime pornography in electronic form. Comment.
11. The Internet has made pornography more ubiquitous than traditional media. Comment.
12. Specify the ‘intermediary’ under IT Act, 2000. What punishment would be provided to him as he fails to preserve and retain the information prescribed by the central government?
13. Explain in brief the power of the controller under the IT Act, 2000, regarding giving direction.
14. On what ground the Central or State Government issue directions for interception or monitoring or decryption of any information through any computer resource? Explain in brief.
15. Does the IT Act, 2000 gives power to the government to issue directions for blocking for public access of any information through any computer resource? If yes, specify the relevant provision.
16. Describe the Central Government's power to authorise to monitor and collect traffic data or information through any computer resource for cyber-security.
17. "Misrepresentation applies only to statements of fact, not to opinions or predictions." Comment in the light of provisions under IT Act, 2000.
18. What do you understand by breach of lawful contract under the IT Act?
19. Specify the importance of digital signature in the present age. How Section 74 of the Act punishes creation, publication or providing of electronic signature certificate for a fraudulent or unlawful purpose?
20. As internet converted the whole world into a village, the cyber law also applicable beyond the boundary of the country. Explain in brief.
21. The punishment made under IT law provides no excuse for other compensation or imposition of any other penalty or punishment under any other law for the time being in force. Explain in brief.
22. What do you understand by abetment of offences? Explain in brief.
23. Explain offences by companies with relevant cases.

24. Why only half the punishment is awarded under attempt is made to commit an offence?

7.10 Answer SAQS

I. Short Answer Question

1. Section 43; see 7.3.1.1; **2.** Damages by way of compensation to the person so affected; see 7.3.1.2; **3.** Not exceeding one lakh and fifty thousand rupees; see 7.3.1.3; **4.** Section 45; see 7.3.1.4; **5.** Section 64; see 7.3.1.5; **6.** Imprisonment of up to three years or a fine of up to two lakh rupees, also both in some cases; see 7.3.2.1; **7.** No; see 7.3.2.2.5; **8.** No; see 7.3.2.3; **9.** Section 69B; see 7.3.2.5.2; **10.** No; see 7.3.2.13.1; **11.** Yes; see 7.3.3.2; **12.** Section 5; see 7.2.3.9;

II. Fill In The Blanks

1. five thousand rupees; see 7.3.1.3; **2.** offences; see 7.3.2; **3.** deputy superintendent of police; see 7.3.2; **4.** computer system; see 7.3.2.2; **5.** Section 66; see 7.3.2.2; **6.** identity theft; see 7.3.2.2.3; **7.** cheat by personation; see 7.3.2.2.4; **8.** Publishes; see 7.3.2.2.5; **9.** imprisonment for life; see 7.3.2.2.6; **10.** 292; see 7.3.2.3; **11.** false statement; see 7.3.2.7; **12.** cyber-crime; see 7.3.2.14

II. TRUE AND FALSE STATEMENT

1. False; see 7.3.1.1; **2.** True; see 7.3.1.3; **3.** True; see 7.3.2; **4.** True; see 7.3.2.1; **5.** True; see 7.3.2.2.6; **6.** True; see 7.3.2.3.2; **7.** True; see 7.3.2.5; **8.** True; see 7.3.2.6.1; **9.** True; see 7.3.2.7; **10.** False; see 7.3.2.8; **11.** True; see 7.3.2.9; **12.** false; see 7.3.2.11; **13.** false; see 7.3.2.13.1; **14.** True; see 7.3.2.14;

Terminal Questions and Model Questions

1. See 7.3.1.1;
2. (i) see 7.3.1.2; (ii) See 7.3.1.2; (iii) See 7.3.1.4; (iv) See 7.3.2; (v) See 7.3.2.1; (vi) See 7.3.2.2.2; (vii) See 7.3.2.2.4; (viii) See 7.3.2.2.5; (ix) See 7.3.2.2.6; (x) See 7.3.2.3; (xi) See 7.3.2.3.2; (xii) See 7.3.2.6; (xiii) See 7.3.2.6.1; (xiv) See 7.3.2.6.2; (xv) See 7.3.2.12; (xvi) See 7.3.2.13.1; (xvii) See 7.3.3.2
3. See 7.3.2;
4. See 7.3.2;
5. See 7.3.2.2;
6. See 7.3.2.2.1;
7. See 7.3.2.2.1;
8. See 7.3.2.2.3;
9. See 7.3.2.2.5;
10. See 7.3.2.3;
11. See 7.3.2.3, 7.3.2.3.1;
12. See 7.3.2.3.3;

13. See 7.3.2.4;
14. See 7.3.2.5;
15. See 7.3.2.5.1;
16. See 7.3.2.5.2;
17. See 7.3.2.7;
18. See 7.3.2.8.1;
19. See 7.3.2.9, 7.3.2.10;
20. See 7.3.2.11;
21. See 7.3.2.13;
22. See 7.3.3.1;
23. See 7.3.3.3;
24. See 7.3.3.2;

UNIT -8

ISSUES OF INTERNET GOVERNANCE.

STRUCTURE

8.1 INTRODUCTION

The Internet is a "network of networks"; it is composed of a multitude of smaller networks that must connect together ("interconnect") in order for the global network to function seamlessly. The Governance implies regulating the functioning of the Internet. In traditional telecommunications networks, interconnection is clearly regulated at the national level by State authorities, and at the international level (i.e., between national networks) by well-defined principles and agreements.

There is increasing international debate on 'Internet governance', which encompasses a variety of public policy issues related to internet infrastructure, management and use .On the Internet, access providers must interconnect with each other across international, national or local boundaries. Internationally, however, there is no regulation, and the terms of any interconnection agreement are generally determined on the basis of negotiation and bargaining.

There are many factors in the Governance of Internet at various levels those are to be regulated at national and International level. The issues may be at infrastructure level, logical level and content level. In this chapter we will study different issues in the governance of the internet and try to cover most of the factors Jurisdiction is also a factor which is to be analyzed and discussed.

8.2 OBJECTIVES

After studying this unit you will be able to:-

- Understand the meaning of the Internet Governance.
- Know about United Nations, IGF.
- Know about Cyber Crime.
- Know about various levels of the Internet Governance.
- Learn about the various causes or factors involved in the Internet Governance.

8.3.1 THE CHALLENGES

The matter of how the Internet is governed is a critical one. Internet governance refers to the processes that impact how the Internet is managed. The way in which the Internet is governed will likely have an impact on how we use it and how it evolves. The Internet is worldwide network system therefore it is to be regulated or governed universally only and certainly there are challenges in regulating and supervising and governing the Internet issues.

8.3.2 THE INTERNET GOVERNANCE FORUM

Internet governance was a key issue at the World Summit on the Information Society (WSIS), held in two phases in Geneva, 2003 and in Tunis, 2005. The Summit recognized the need for a broad based discussion of public policy issues relating to the Internet and requested the Secretary-General of the United Nations to convene a new forum for the Internet Governance Forum (IGF). The IGF is supported by a small Secretariat which was established in 2006.

The IGF is a global multistakeholder platform that facilitates the discussion of public policy issues pertaining to the internet. The IGF and all the national and regional IGF initiatives are the foremost multistakeholder venue to familarize governments with the Internet model. It is also the only place that touches on all the dimensions of Internet governance. The IGF mandate is very broad and allows for discussing almost any policy subject related to Internet governance. The Third IGF meeting was held in Hyderabad, India, on 3-6 December 2008 and the overall theme was: "Internet for All".

8.3.3 INTERNET JURISDICTION

The Internet's decentralized nature makes it likely that any given Internet transaction will involve parties from more than one jurisdiction. The main problem that is faced in ascertaining the jurisdiction is the presence of multiple parties from various parts of the world. If a party desires to sue any other party the problem arises where they can sue. In due courses it depends upon the place where defendant resides or where the cause of action arose but in case of Internet jurisdiction it is not easy to establish. For example A in India want to buy any article via online shopping and made payment through credit card but failed to receive the same and it was found that owner is at Australia and the site itself is based on New Zealand, the transaction took place on the net so was the jurisdiction lies in India or New Zealand or Australia. Such issues create confusions and contradictions and many times gives safe passage to the defendant.

8.3.4 FACTORS NEEDED TO BE GOVERNED

There are various factors which occurs during the internet use and need to be governed by the either ways, they may be governed either by enacting law or by the service providers need to regulate them. Cyber crime in the recent past include a major incidence wherein Indian President APJ Abdul Kalam received an email containing a threat to his life; the accused sender of the mail had used a fictitious name. Some of the types of the cyber crime are as follows:-

8.3.4.1 The Information Technology Act deals with the following cyber crimes along with others:

(i) Tampering with computer source documents.

(ii) Hacking.

(iii) Publishing of Information, which is Obscene in Electronic Form.

(iv) Child Pornography.

(v) Accessing Protected system.

(vi) Breach of Confidentiality and Privacy.

8.3.4.2 The Concept of Cyber Terrorism

Cyber crime and Cyber terrorism are both crimes but differ in the motive behind it. Governments of various nations are affected by the acts of the Cyber terrorism. Various tools and methods used by Cyber terrorists are Hacking, Cryptography, Computer viruses, E-mail etc, Some of the motives behind the attacks are as follows:

(a) Threatening the Government or its agencies.
(b) Endangering the sovereignty and integrity of the nation.
(c) Putting public in fear.

8.3.4.3 Various other threats those to be governed

There are various threats those needed to be governed worldwide; some of them are discussed in brief as follows:

Malware: it is software designed to damage a computer system and the owner having no knowledge. it is created to annoy or destroy or corrupt the files of the system with a purpose of causing grave harm to the institutions. Malware should not be confused with defective software, that is, software which has a legitimate purpose but contains harmful bugs. A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user.

Hacking: Computer hacking is some degree of infringement on the privacy of others. A hacker is someone involved in computer security/ insecurity, specializing in the discovery of exploits in systems either for exploitation or prevention, tactics or detailed knowledge in gathering hidden information.

Cyber Stalking: Cyber stalking, which is simply an extension of the physical form of stalking are used to pursue, harass or contact another in unsolicited fashion. It has been defined as the use of information and communication technology, particularly the Internet, by an individual or group of individuals, to harass another individual, group of individuals, or organization. The behavior includes false accusations, monitoring, the transmission of threats, identity theft etc,

Internet Fraud: Misrepresentation within the meaning of Indian Contract Act, 1872, amounts to Internet fraud. “Phishing”, which is a form of internet fraud, involves a person pretending to be legitimate association, creating fictitious e-mails to extract personal data from users for his own advantage misrepresenting on identity of legitimate party.

8.3.5 INTERNET GOVERNANCE:

“The Internet” refers to the global, seamless interconnection of networks using Internet Protocol (IP). Internet Protocol is a network layer protocol that contains the addressing information and some control information that allows packets to be routed.

“Internet governance” can be understood as comprising the following elements:

• the technical standardization activities that promote interoperability of Internet Protocol (IP) applications as well as network security, reliability and quality for the Internet;

• the technical coordination of the key protocols and addresses and names that underpin the technical functioning of the Internet.

Internet Governance, broadly defined, is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet. It covers activities such as development and coordination of technical standards, operation of critical infrastructure and public policy issues.

Conceptually Internet Governance includes following layers

1. Physical Infrastructure layer
2. Code or Logical layer
3. Content layer
4. Security

8.3.6 ISSUES IN INTERNET GOVERNANCE

Internet governance is an important policy and governance issue that gets attention at the international level. It raises the crucial issue of how the Internet is governed sustainably as a global resource, on how Critical Internet resources such as domain names, IP address needs to be allocated, and on how global DNS infrastructure including Root Server needs to be managed. Since the first phase of World Summit on Internet Society in 2003, nations have called for a transparent, democratic and multilateral governance of the Internet.

There have been debates globally on whether in its attempts to create new International Telecommunication Rules (ITRs), the ITU trying to control the Internet, and encourage censorship. India has joined countries like US, UK and Canada to oppose government regulation of the Internet at the ITU WCIT meetings at Dubai, concluded on 14th Dec 2012, where new ITRs are being negotiated - the existing ITRs agreed upon in 1988 covered only international telephony.

8.3.7 Activities related to India Internet Governance Forum (IIGF) carried out by the National Internet Exchange of India (NIXI)

The major objectives include:

a) To provide a space for multi-stakeholder dialogue between Governments, the private sector, the technical community, academia and civil society organizations on the issues related to Internet and Internet based services/applications;

b) To inform the India's stakeholders on the issues and trends observed in the debates and discussions of the global IGF;

c) To consolidate India's views and initiatives on the issues of concern for Internet Proliferation and its Governance that could be highlighted in the Internet Governance Forum meetings;

d) To arrive at national strategies and action plan for proliferation and governance of Internet and Internet based services in the country;

e) To deliberate on policy areas vis-à-vis Internet for Governance and inclusive development

8.3.8 GUIDING PRINCIPLES

The following are recommended guiding principles for Internet governance as prescribed by the Internet Society (US):

1 Open, inclusive, and transparent participation. The participation of interested and informed stakeholders in Internet governance processes, in their respective roles and responsibilities, is necessary to ensure that outcomes are both effective and accepted. It also ensures that interested stakeholders can directly participate in the work and have access to its results.

2 Consensus-based decision making. Policy-making processes should be informed by both practical experience and the individual and collective expertise of a range of stakeholders. Decisions should be reached through accountable processes that are based on consensus.

3 Collective stewardship and empowerment. To ensure the continued security, stability, and resilience of the Internet, governance structures and principles should be developed in an environment of strong cooperation among all stakeholders, each contributing their own skills.

4 Pragmatic and evidence-based approaches. Internet governance discussions, debates, and decisions must be informed by, and depend upon, objective and empirical information.
5 Voluntarism. In the realm of Internet technical policy development, voluntarism means that success is determined by users and the public, rather than a central authority.
6 Permissionless innovation. The remarkable growth of the Internet and the ensuing explosion of innovation and Internet use is a direct result of the open model of Internet connectivity and standards development. Anyone should be able to create a new application on the Internet without having to obtain approval from a central authority. Internet governance arrangement should not constrain or regulate the ability of individuals or organizations to create and use new standards, applications, or services.
Today's Internet ecosystem is based on the fundamental tenets of the Internet itself, and draws its strength from the involvement of a broad range of players employing open, transparent, and collaborative processes. Cooperation and collaboration remain essential to the Internet's continued innovation and growth.

8.4 SUMMARY

The Internet is a "network of networks"; it is composed of a multitude of smaller networks that must connect together ("interconnect") in order for the global network to function seamlessly. There is increasing international debate on 'Internet governance', which encompasses a variety of public policy issues related to internet infrastructure, management and use. There are many factors in the Governance of Internet at various levels those are to be regulated at national and International level. Internet governance was a key issue at the World Summit on the Information Society (WSIS), held in two phases in Geneva, 2003 and in Tunis, 2005. The Internet's decentralized nature makes it likely that any given Internet transaction will involve parties from more than one jurisdiction. The main problem that is faced in ascertaining the jurisdiction is the presence of multiple parties from various parts of the world. There are various factors which occurs during the internet use and need to be governed by the either ways, they may be governed either by enacting law or by the service providers need to regulate them. There are recommended guiding principles for Internet governance as prescribed by the Internet Society (US).

8.5 GLOSSARY

WSIS-World Summit on the Information Society.

IGF-Internet Governance Forum.

IP-Internet Protocol.

ITRs- International Telecommunication Rules.

ITU- International Telecommunication Union.

IIGF- India Internet Governance Forum

8.6 SAQS

1. Short Answer Questions-

a. What is full form of IGF?

b. What are some cybercrimes those The Information Technology Act deals along with others?

2 Fill in the blanks-

A. IIGF denotes……...
B. Full form of IP is……..

8.7 REFERENCES

a) Article by Ayesha Hassan in wgig.org/docs/book/Ayesha_Hassan%20.
b) cis-india.org/internet-governance/issues-in-internet governance.
c) Internet Society[US]internet society.org/issues/internet-governance
d) intgovforum.org/multilingual/
e) dsci.in/content/internet-governance/overview-timeline-activities.
f) meaty.gov.in/content/internet-proliferation-governance.

8.8 SUGGESTED READINGS

1. Nandan Kamnath, Law Relating to Computers and Internet & E-commerce,published by Universal Law Publication Co.
2. N.C.Jain, Cyber Crime, Published by Allahabad Law Agency.

8.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. What are the guidelines prescribed by the Internet Society(US)?.

2. Write Conceptually Internet Governance layers.

SAQS

1. (a)Refer 8.5.
(b) 8.3.4.1.
2. (A) India Internet Governance Forum, (B) Internet Protocol.

Terminal Questions and Answers

(1).Refer 8.3.8, (2)8.3.5

UNIT- 9

FREEDOM OF EXPRESSION IN INTERNET.

STRUCTURE

9.1 INTRODUCTION

The term freedom of expression is indispensable in a democracy. Article 19 of the Constitution of India guarantees to the citizens of India six fundamental rights which are exercised by them throughout and in all parts of India. In our Constitution it is provided as a freedom of speech and expression under Article 19(1)(a); it is recognized as a natural right inherent in the status of a citizen. These rights are subject to the restrictions given in Article 19 (2) whereby State can impose reasonable restrictions.

Freedom of expression is enshrined in Article 19 of both the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). Article 10 of the Human Rights Act provides Freedom of expression. As the society is progressing towards in new era the Internet has afforded opportunities for people to express themselves through both private and public communication; UNESCO recognizes that the Internet holds enormous potential for development. It provides an unprecedented volume of resources for information and knowledge that opens up new opportunities and challenges for

expression and participation; the freedom of expression as envisaged by different forums has been implied to the freedom of expression through internet also.

At present internet is the main source of communication and at various forums and at day to day developments expression through internet is the medium through which individuals as well as organizations communicate or place their expressions; earlier it was possible through limited sources of publication and to a certain group of society which has been now enhanced by internet therefore a debate is necessitated at this juncture regarding freedom of expression on internet. In this chapter we are going to deal with various aspects of the freedom of expression including freedom of speech and expression especially in Indian context.

9.2 OBJECTIVES

After studying this unit you will be able to:-

- Understand the meaning of freedom of expression from various dimensions.
- Know about freedom of expression in the Universal Declaration of Human Rights.
- Know the views of UNESCO behind internet and its freedom.
- Know about the Equality and Human Rights Commission.
- Know about Article 19 of the Constitution of India.
- Understand the term freedom of expression in the Indian context.

9.3 Universal Declaration of Human Rights

The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A) as a common standard of achievements for all peoples and all nations. It sets out, for the first time, fundamental human rights to be universally protected.

According to Article 19, “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”

We can ascertain herein that at present these rights had been put forthwith in context of the Freedom of expression on internet also as it is the major medium of communication worldwide as the world has become a global village by the use of the internet. the International Covenant on Civil and Political Rights (ICCPR) holds that, " everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice".

9.4 The United Nations Educational, Scientific and Cultural Organization (UNESCO)

UNESCO recognizes that the Internet holds enormous potential for development. It provides an unprecedented volume of resources for information and knowledge that opens up

new opportunities and challenges for expression and participation. The principle of freedom of expression and human rights must apply not only to traditional media but also to the Internet and all types of emerging media platforms, which will contribute to development, democracy and dialogue.

UNESCO assumes its responsibility of promoting freedom of expression on Internet and related right such as privacy and has integrated it to its regular program. The Organization explores the changing legal and regulatory framework of Internet and provides member states with policy recommendations aiming to foster a conducive environment to freedom of expression and privacy on the Internet.

9.5 The Equality and Human Rights Commission

The Equality and Human Rights Commission is Great Britain's national equality body and has been awarded an 'A' status as a National Human Rights Institution (NHRI) by the United Nations.

Article 10 protects right to hold your own opinions and to express them freely without government interference. This includes the right to express your views aloud (for example through public protest and demonstrations) or through:

- published articles, books or leaflets
- television or radio broadcasting
- works of art
- the internet and social media

9.5.1 Restrictions to this Right:

Public authorities may restrict this right if they can show that their action is lawful, necessary and proportionate in order to:

- protect national security, territorial integrity (the borders of the state) or public safety
- prevent disorder or crime
- protect health or morals
- protect the rights and reputations of other people
- prevent the disclosure of information received in confidence
- maintain the authority and impartiality of judges

9.6 Article 19 the of India Constitution of

Protection of certain rights regarding freedom of speech, etc.-

(1) All citizens shall have the right-

(a) to freedom of speech and expression;

(b) to assemble peaceably and without arms;

(c) to form associations or unions;

(d) to move freely throughout the territory of India;

(e) to reside and settle in any part of the territory of India;

(g) to practise any profession, or to carry on any occupation, trade or business.

(Clause (f) on "to acquire, hold and dispose of property; and" omitted by Constitution (Forty fourth Amendment) Act, 1978)

Article 19 of the Constitution guarantees to the citizens of India six fundamental rights; subject to restrictions of Article 19 (2). According to Article 19(1)(a) of the Constitution of India, "all citizens shall have the right to freedom of speech and expression". State can impose restrictions also but a law restricting the exercise of any of the rights guaranteed by clause (1) of Article 19 to be constitutionally valid, must satisfy the two following conditions,-

(i) The restriction must be for the particular purpose mentioned in the clause permitting the imposition of the restriction on that particular right, and

(ii) The restriction must be reasonable.

It is important to mention here that in the Preamble to the Constitution of India the people of India declared their solemn resolve to secure to all its citizens liberty of thought and expression.

19.6.1 Meaning of Freedom of Speech and Expression

The term freedom of expression may be understood inclusively with freedom of speech as well as with freedom of opinion; expression may a step forward to these connotations. The expression may either be in the form mouth, writing, printing, pictures or any other mode and includes internet also. For any democratic government it is basis of democracy and in *Romesh Thapar v. State of Maharashtra* (AIR 1950 SC 124) it has been observed as follows:

"Freedom of speech and of the press lay at the foundation of all democratic organizations, for without free political discussion no public education, so essential for the proper functioning of the process of popular government, is possible."

Freedom of speech and expression includes the freedom of propagation of ideas and is ensured by the freedom of circulation; the ideas at present are largely propagated by the internet and any kind of unreasonable censorship would be violative to the fundamental right enshrined in Article 19(1)(a).

9.6.2 Recoganization of Freedom of expression by the Court

In *S. Rangarajan v. P. Jagjivan Ram* the duty was imposed on the State to protect the freedom of expression and observes as follows-

"It it the duty of the state to protect the freedom of expression since it is a liberty guaranteed against the State. The State cannot plead its inability to handle the hostile audience problem. It is obligatory duty to prevent it and protect the freedom of expression. "

In *S.P. Gupta v. Union of India*, right to know, receive and impart information has been recognized within the right to freedom of speech and expression."A citizen has a fundamental right to use the best mean of imparting and receiving information and as such to have an access to telecasting for the purpose. "

In *Secy., Ministry of I & B, Govt. of India v. Cricket Assn. of Bengal* the Court has held that the air waves or frequencies are public property, their use must be controlled and

regulated by a public authority in the interest of public and to prevent the invasion of their rights.

9.6.3 Certain limitations by the enactments

The IT Act and the Indian Penal Code prohibit the production and transmission of "obscene material, but there is no specific law against viewing pornography in India, except child pornography, which is prohibited under the IT Act. In the case of *Kamlesh Vaswani v. Union of India*, the petitioner asked the Supreme Court to direct the government to block all online pornography in India. In the past, the government has informed the Supreme Court that it is not technically feasible to block pornographic sites and that doing so would violate the constitution.

The Indian Penal Code (IPC) criminalizes several kinds of speech, and applies to online content. Individuals could be punished with a jail term ranging from two to seven years for speech that is found to be seditious, obscene, defamatory, promoting enmity between different groups on ground of religion, race, place of birth, residence, language, committing acts "prejudicial to maintenance of harmony," or consisting of statements, rumors, or reports that may cause fear, alarm, disturb public tranquility, or promote enmity or ill will. Internet users are also subject to criminal punishment under the Official Secrets Act for wrongful communication of information that may have an adverse effect on the sovereignty and integrity of India.

The IT Act criminalizes certain online activity in particular. The act bans the publication or transmission of obscene or sexually explicit content in electronic form, and the creation, transmission or browsing of child pornography.

In *Shreya Singhal v. Union of India,* Section 66A of the Information Technology Act, 2000 has been struck down in its entirety being violative of Article 19(1)(a) and not saved Under Article 19(2).

According to Section 66 A. Punishment for sending offensive messages through communication service, etc.-Any person who sends, by means of a computer resource or a communication device,--

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.--For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

The Hon'ble Apex Court found the provision against the violation of Freedom of speech and expression and struck down in furtherance.

9.6.4 Conclusion

It may be concluded from the above discussion that Freedom of expression in internet has been widely recognized and certain restrictions has also been imposed; therefore they are not absolute. From the judgments pronounced by the Indian Apex Court it could be ascertained that right to freedom of expression is covered under Article 19(1)(a) of the Constitution of India subject to certain restrictions.

9.7 SUMMARY

The term freedom of expression is indispensable in a democracy. Article 19 of the Constitution of India guarantees to the citizens of India six fundamental rights which are exercised by them throughout and in all parts of India. The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. According to Article 19, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." UNESCO recognizes that the Internet holds enormous potential for development. It provides an unprecedented volume of resources for information and knowledge that opens up new opportunities and challenges for expression and participation The Equality and Human Rights Commission is Great Britain's national equality body and has been awarded an 'A' status as a National Human Rights Institution (NHRI) by the United Nations Article 10 protects right to hold your own opinions and to express them freely without government interference. Public authorities may restrict this right if they can show that their action is lawful, necessary and proportionate In *S. Rangarajan v. P. Jagjivan* Ram the duty was imposed on the State to protect the freedom of expression The IT Act and the Indian Penal Code prohibit the production and transmission of "obscene material, but there is no specific law against viewing pornography in India, except child pornography, which is prohibited under the IT Act. In *Shreya Singhal v. Union of India*, Section 66A of the Information Technology Act, 2000 has been struck down in its entirety being violative of Article 19(1)(a) and not saved Under Article 19(2).

9.8 GLOSSARY

UDHR- Universal Declaration of Human Rights (UDHR)

ICCPR-International Covenant on Civil and Political Rights

UNESCO-The United Nations Educational, Scientific and Cultural Organization (UNESCO)

9.9 SAQS

1. Short Answer Questions-

a. What is provided in Article 19 of the Universal Declaration of Human Rights?

b. In which case Section 66-A of the Information Technology Act has been struck down?

2 Fill in the blanks-

C. Article 19(1) provides…….. fundamental rights.
D. Restriction to Article 19(1)(a) is given under…….. of the Constitution of India.

9.10 REFERENCES

a) un.org/en/universal-declaration-human-rights/
b)equalityhumanrights.com/en/about-us
c) equalityhumanrights.com/en/human-rights-act/article-10-freedom-expression

9.11 SUGGESTED READINGS

1. Constitution of India.
2.V.N.Shukla's Constitution of Indai, Mahendra P.Singh, Published by Eastern Book Company.

9.12 TERMINAL QUESTIONS AND MODEL QUESTIONS

1 Briefly state the cases in which Freedom of expression has been recognised ?.

2. What are the fundamental rights provided in Article 19 of the Constitution of India?

SAQS

1. (a)Refer 9.3.
(b) Shriya Singhal v. Union of India.
2. (A) 6, (B) Article 19(2).

Terminal Questions and Answers

(1).Refer 9.6.2, (2) 9.6

UNIT- 10

INTERNATIONAL POSITION ON FREE SPEECH IN INTERNET.

STRUCTURE

10.1 INTRODUCTION

Freedom of expression has long been regarded as one of the fundamental principles of modern democracies, in which civil liberties are honoured and regarded as a prerequisite for

individual development and fulfillment. In the earlier chapter position of freedom of speech on internet especially in Indian perspective has been discussed in brief. Right to free speech has been recognized by the international community and in some of the nations it has been given a status of fundamental right.

Internet speech has potentially far greater impact than speech through ordinary media. It has the potential to be the genuine voice of the grassroots, uncontrolled by any media organizations. It has the potential to communicate in video, audio, pictures and text, as well as reach far more people than the biggest satellite TV station or best-read international newspaper. So, internet speech can facilitate or incite action much more effectively than traditional media.

The First Amendment in the American Constitution famously guarantees US citizens the right to free speech. Freedom of expression is enshrined in Article 19 of both the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). Article 10 of the Human Rights Act provides Freedom of expression. UNESCO recognizes that the Internet holds enormous potential for development. It provides an unprecedented volume of resources for information and knowledge that opens up new opportunities and challenges for expression and participation; the freedom of expression as envisaged by different forums has been implied to the freedom of expression through internet also. Like India many other countries also provide the Freedom of Speech and Expression to its citizens but with some limitations. The restrictions put on the Freedom of Speech vary from country to country. In this chapter we are going to deal with various aspects of free speech on internet in International perspective.

10.2 OBJECTIVES

After studying this unit you will be able to:-

- Understand the meaning of freedom of speech.
- Know about positions of free speech in internet in various countries.
- Know about the countries where it is not provided to its citizens.

10.3 Meaning of Free Speech

Free speech signifies an opinion or expression which a person desires to express by any means, either by writing, speaking, and painting or may be via internet in this modern era of information technology.

Freedom of speech is one of the basic rights given to the citizens of most of the countries across the globe. It enables the people residing in those countries to speak their mind without the fear of being punished by the law. Freedom of speech is a principle that supports the freedom of an individual or a community to articulate their opinions and ideas without fear of retaliation, censorship, or legal sanction. The term "freedom of expression" is sometimes used synonymously but includes any act of seeking, receiving, and imparting information or ideas, regardless of the medium used.

Freedom of information is an extension of freedom of speech where the medium of expression is the Internet. Freedom of information may also refer to the right to privacy in

the context of the Internet and information technology. As with the right to freedom of expression, the right to privacy is a recognized human right and freedom of information acts as an extension to this right.

10.3.1 Origin of Freedom of Speech

The concept of freedom of speech originated long back. England's Bill of Rights 1689 adopted freedom of speech as a constitutional right and it is still in effect. The French revolution in 1789 adopted the Declaration of Rights of Man and of the Citizen. This further affirmed the Freedom of Speech as an undeniable right. The Declaration of Freedom of Speech and Expression in Article 11 states:

"The free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen may, accordingly, speak, write, and print with freedom, but shall be responsible for such abuses of this freedom as shall be defined by law".

Article 19 of the Universal Declaration of Human Rights, adopted in 1948, states that:

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers

10.4 Position of Free speech in different countries

Freedom of speech gives citizens the right to speak their opinions and express their ideas without being censored. There are certain limits to freedom of speech, including but not limited to libel, slander, incitement, copyright violation, trade secrets, and perjury. The internet is providing new possibilities of wider reach and opened up new possibilities of expressing opinion. Position in some of the countries of the world regarding freedom of speech is as follows-

10.4.1 Australia

In Australia there is no express constitutional or legislative protection of the freedom of expression at the federal level, despite this, the courts have an important role in interpreting legislation consistently with human rights where possible. Although not expressly protected at a federal level, freedom of expression does enjoy some implied and residual protection. The Australian High Court has held that an implied freedom of political communication 'is an indispensable incident of the system of representative government which the Constitution creates'.

10.4.2 Brazil

Brazil has experienced the establishment of a 'post redemocratisation' constitutional framework that undoubtedly grants freedom of speech and of the press. The country has prepared the ground for the establishment of a social communication system in alignment with the most advanced international regimes in the field.

Brazil's Federal Constitution guarantees to the Brazilians a broad access to information from different and multiple sources within a democratic environment where freedom of speech and the press is ensured. However, the country still faces some gaps in the media regulatory framework.

10.4.3 Canada

Internet access in Canada is reliable and affordable for a majority of the population. Canada's goal of universal internet access, described as the "universal service objective," was bolstered by a landmark policy decision in 2016 declaring high-speed internet a "basic telecommunications service" that should be available to all Canadians. Canadians enjoy strong protections for freedom of expression, as well as a well-developed set of rules regulating intermediary liability in cases of copyright infringement.

10.4.4 France

Freedom of expression is enshrined in the Declaration of the Rights of Man and of the Citizen. As for freedom of the press, it is enshrined in the law of 1881. But this freedom has limits: racism, anti-Semitism, racial hatred, and justification of terrorism are not opinions.

10.4.5 Germany

Although Internet censorship in Germany has traditionally been rated as low, it is practiced directly and indirectly through various laws and court decisions. German law provides for freedom of speech and press with several exceptions, including what The Guardian has called "some of the world's toughest laws around hate speech". An example of content censored by law is the removal of web sites from Google search results that deny the holocaust, which is a felony under German law.

10.4.6 India

Article 19 of the Constitution guarantees to the citizens of India six fundamental rights; subject to restrictions of Article 19 (2). According to Article 19(1)(a) of the Constitution of India, "all citizens shall have the right to freedom of speech and expression". State can impose restrictions also but a law restricting the exercise of any of the rights guaranteed by clause (1) of Article 19 to be constitutionally valid, must satisfy the two following conditions,-

(iii) The restriction must be for the particular purpose mentioned in the clause permitting the imposition of the restriction on that particular right, and

(iv) The restriction must be reasonable.

10.4.7 Britain

British citizens have a negative right to freedom of expression under the common law. In 1998, the United Kingdom incorporated the European Convention, and the guarantee of freedom of expression it contains in Article 10, into its domestic law under the Human Rights Act. However, there is a broad sweep of exceptions.The law provides for freedom of speech and press, and prohibits arbitrary interference with privacy, family, home, or

correspondence, and the government routinely respects these rights and prohibitions. An independent press, an effective judiciary, and a functioning democratic political system combine to ensure freedom of speech and press. Individuals and groups routinely use the Internet, including e-mail, to express a wide range of views.

10.4.8 United States of America

The First Amendment of the United States Constitution protects the right to freedom of religion and freedom of expression from government interference. It prohibits any laws that establish a national religion, impede the free exercise of religion, abridge the freedom of speech, infringe upon the freedom of the press, interfere with the right to peaceably assemble, or prohibit citizens from petitioning for a governmental redress of grievances. It was adopted into the Bill of Rights in 1791. The Supreme Court interprets the extent of the protection afforded to these rights.

10.5 Internet Access –

A Fundamental Human Right While certain countries and international organizations, including the United Nations, are considering whether to recognize Internet access as inherent to the right to free expression and as such to be a fundamental and universal human right, others are considering adopting content and access blocking measures.

10.6 Countries That Do Not Have Freedom of Speech

There are countries that do not give the right to Freedom of Speech to their citizens to maintain absolute control. Here are some of them as follows:

North Korea: The country does not provide Freedom of Speech and Expression to its citizens as well as the media.

Syria: The government of Syria is known for its tyranny. People here are deprived of their basic human right that is the right to Freedom of Speech and Expression.

Cuba: Yet another country that doesn't provide Freedom of Speech to its citizens. The citizens of Cuba are not allowed to pass any negative comment on the activities of the government or any political party.

Belarus: This is another country that does not offer Freedom of Speech and Expression. People cannot voice their opinions or criticize the work of the government.

Iran: The citizens of Iran are not aware what it is like to express their opinion and share their ideas freely in the public. Nobody can express any kind of discontentment against the public laws or Islamic standards.

Burma: The government of Burma is of the opinion that the Freedom of Speech and Expression is unnecessary. The citizens are asked not to express their ideas or opinions particularly if they are against any leader or political party.

Libya: Most people in this country do not even know as to what Freedom of Speech and Expression really is. The government of Libya is known for oppressing its citizens. In the age

of internet, people around the world are free to express their views on any matter but not in this country.

10.7 Universal Declaration of Human Rights

The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. It sets out, for the first time, fundamental human rights to be universally protected.

According to Article 19, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

10.8 Conclusion

It may be concluded from the above discussion that Freedom of expression and speech in internet has been widely recognized and certain restrictions has also been imposed; therefore they are not absolute. Democratic countries provide freedom of speech to their citizens while in some of the countries there is no right as such.

10.9 SUMMARY

Freedom of expression has long been regarded as one of the fundamental principles of modern democracies, in which civil liberties are honoured and regarded as a prerequisite for individual development and fulfillment. The First Amendment in the American Constitution famously guarantees US citizens the right to free speech. Freedom of expression is enshrined in Article 19 of both the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). Article 10 of the Human Rights Act provides Freedom of expression.Free speech signifies an opinion or expression which a person desires to express by any means, either by writing, speaking, and painting or may be via internet in this modern era of information technology. Freedom of information is an extension of freedom of speech where the medium of expression is the Internet. Freedom of information may also refer to the right to privacy in the context of the Internet and information technology. The concept of freedom of speech originated long back. England's Bill of Rights 1689 adopted freedom of speech as a constitutional right and it is still in effect. Freedom of speech gives citizens the right to speak their opinions and express their ideas without being censored. There are certain limits to freedom of speech, including but not limited to libel, slander, incitement, copyright violation, trade secrets, and perjury. The internet is providing new possibilities of wider reach and opened up new possibilities of expressing opinion. Democratic countries provide freedom of speech to their citizens while in some of the countries there is no right as such.

10.10 GLOSSARY

Undeniable right – Rights those cannot be denied.

Libel – a written defamation.

Slander – a false and malicious spoken statement

Perjury- the offence of willfully telling an untruth.

ICCPR-International Covenant on Civil and Political Rights . UNESCO-The United Nations Educational, Scientific and Cultural Organization (UNESCO)

10.11 SAQS

1. Short Answer Questions-

a. Which Amendment in the American Constitution famously guarantees US citizens the right to free speech?

b. The French revolution in which year adopted the Declaration of Rights of Man and of the Citizen?

2 Fill in the blanks-

E. Article 19(1) provides…….. fundamental rights.
F. Restriction to Article 19(1)(a) is given under…….. of the Constitution of India.

10.12 REFERENCES

a) un.org/en/universal-declaration-human-rights/
b)equalityhumanrights.com/en/about-us
c) equalityhumanrights.com/en/human-rights-act/article-10-freedom-expression
d) https://www.osce.org/fom/105522?download=true
e) https://www.theguardian.com/technology/1999/feb/05/freespeech.internet
f) https://www.indiacelebrating.com/essay/essay-on-freedom-of-speech/
g) https://www.humanrights.gov.au/our-work/3-freedom-expression-and-internet
h) http://www.unesco.org/new/en/brasilia/communication-and-information/freedom-of-expression/
i) https://freedomhouse.org/report/freedom-net/2018/canada
j)https://www.gouvernement.fr/en/everything-you-need-to-know-about-freedom-of-expression-in-france-0
k) https://www.law.cornell.edu/wex/first_amendment

10.13 SUGGESTED READINGS

1. Constitution of India.
2.V.N.Shukla's Constitution of India, Mahendra P.Singh, Published by Eastern Book Company.

10.14 TERMINAL QUESTIONS AND MODEL QUESTIONS

1 Name some of the countries those recognize freedom of speech in internet.

2. Name some of the countries not having freedom of speech.

SAQS

1. (a) First.
(b) 1789.
2. (A) 6, (B) Article 19(2).

Terminal Questions and Answers

(1).Refer 10.4, (2)10.6

UNIT-11

THE SALE OF GOODS REGULATIONS, 1930

11.1 INTRODUCTION

Earlier transactions related to sale and purchase of goods was contained under Chapter VII in Sections 76 to 123 of Indian Contract Act, 1872, based on English common law. The Indian Sale of Goods Act, 1930, is a mercantile law came into existence during the British period on 1 July 1930. This was based mainly on Sale of Goods Act, 1893. This Act facilitates to settle down the contracts where the seller transfers or agrees to transfer the title i. e. ownership in the goods to the buyer for consideration. Sale of Goods Act, 1930 is applicable all over India, except Jammu and Kashmir. Here under Indian Sale of Goods Act, 1930, goods sold by owner to buyer and must be sold for a certain price at a given period of time. This act was amended on 23 September 1963, and was renamed to the Sale of Goods Act, 1930.

It extends to the whole of India except the State of Jammu and Kashmir. It does not affect rights, interests, obligations and titles acquired before the commencement of the Act. The Act deals with sale but not with mortgage or pledge of the goods.

11.2 OBJECTIVES

Business through internet caters to globally located customers. This rises cross border legal issues. Transactions that may be legal and valid in one jurisdiction may not be enforceable in others. Creation of wealth through cyber space would also entail the use of "offshore" financial institutions to store this wealth. This would constitute an elaborate and often untraceable form of tax avoidance. This is not only a threat to national sovereignty but also overrides traditional principles of taxation- a transgression of traditional notion of political and monetary autonomy. As wealth is generated through the means of cyber space, accounting mechanisms and monetary control would become difficult. Taxes on cyberspace would be one method of getting some amount of monetary control.

11.3 DEFINITION OF SALE:

Section 4 of the Sales of Goods Act, 1930 defines a sale of goods as a "contract of sale whereby the seller transfers or agrees to transfer the property in goods to the buyer for price". The term 'contract of sale' includes both a sale and an agreement to sell.

A contract of sale is made by an offer to buy or sell goods for a price and the acceptance of such offer by the other party. The contract may be oral or in writing. A contract of sale may be absolute or conditional.

Formalities of a contract of sale: Section 5 of the Act specifically provides for the following three steps or formalities in a contract of sale:

1) Offer and Acceptance: A contract of sale is made by an offer to buy or sell the goods for a price and acceptance of such offer.

2) Delivery and Payment: It is not necessary that the payment for the goods to the seller and delivery of goods to the buyer must be simultaneous. They can be made at different times or in instalments as per the contract.

3) Express or Implied: The contract can be in writing, oral or implied. It can also be partly oral and partly written.

11.4 FORMATION OF CONTRACT OF SALE

CONTRACT OF SALE OF GOODS

A contract of goods is a contract whereby the seller transfers or agrees to transfer the property to goods to the buyer for a price. According to Section 4(1) there may be a contract of sale between one part-owner and another and at the same time under section 4 (2) contract of sale may be absolute or conditional. The term 'contract of sale' is a generic term and includes both a sale and an agreement to sell.

Sale and agreement to sell: when under a contract of sale, the property in the goods is transferred from the seller to the buyer, the contract is called a 'sale', but where the transfer of the property in the goods is to take place at a future time or subject to some conditions thereafter to be fulfilled, the contract is called an 'agreement to sell,' under Section 4(3). An agreement to sell becomes a sale under section 4 (4) when time elapses or the conditions, subject to which the property in the goods is to be transferred are fulfilled.

11.5 ESSENTIAL ELEMENTS OF A CONTRACT OF SALE

According to Sale of Goods Act, 1930 there are five essential features of a contract of sale are as discussed below:

1) **Two partied:** There must be two parties i.e. buyer and seller to constitute a contract
2) **Subject matter to be goods:** Subject matter of contract of sale must be the goods of any kind except immovable goods.

3) **Transfer of ownership of goods:** Passing of property is necessary and not the physical delivery of goods.
4) **Consideration is price:** Consideration of a contract of sale must be money. If some goods are supplied as remuneration for work done or in exchange for some goods. It does not amount to contract of sale.
5) Essential elements of a valid contract
1) Two parties: A sale has to be bilateral because the goods have to pass from one person to another. There must be a buyer – a person who buys or agrees to buy the goods and a seller – a person who sells or agrees to sell goods. The seller and the buyer must be different persons. A part owner can sell to another part owner. A partner may, therefore, sell to his firm or a firm may sell to a partner. But if joint owners distribute property among themselves as per mutual agreement, it is not 'sale'. A person cannot be the seller of his own goods as well as the buyers of them.

However, when a bankrupt person's goods are sold under an execution of decree, the person may buy back his own goods from his trustee.

2) **Subject matter to be goods:** The term 'goods' is defined in Section 2(7). It states that 'goods' "means every kind of movable property other than actionable claims and money; and includes stock and shares, growing crops, grass and things attached to or forming part of the land which are agreed to be severed before sale or under the contract of sale".

Money cannot be sold because money means legal tender and not the old coins which can be sold and purchased as goods. Actionable claims are things that a person cannot make use of, but which can be claimed by him by means of legal action such as a debt.

Sale of immovable property is not covered under this Act. As per Section 3 of the Transfer of Property Act, 1882, 'immovable property' does not include standing timber, growing crops or grass. They are considered movable property and thus goods. Standing timber is taken as movable property while trees are immovable property.

Case Study

Things like goodwill, copyright, trademark, patents, water, gas, electricity are all goods. In the case of Commissioner of Sales Tax vs. Madhya Pradesh Electricity Board AIR 1970 SC 732, the Supreme Court observed – "…electricity…can be transmitted, transferred, delivered, stored, possessed, etc., in the same way as any other movable property…If there can be sale and purchase of electric energy like any other movable object, we see no difficulty in holding that electric energy was intended to be covered by the definition of "goods".

In the case of H. Anraj vs. Government of Tamil Nadu AIR 1986 SC 63, it was held that lottery tickets are goods and not actionable claims. Thus, sale of lottery tickets is sale of goods. Sugarcane supplied to a sugar factory is goods within the meaning of Section 2(7) of the Act as held in the case of UP Cooperative Cane Unions Federation vs. West UP Sugar Mills Assn. AIR 2004 SC 3697.

3) **Transfer of ownership of Goods:** There must be transfer of ownership or an agreement to transfer the ownership of goods from the seller to the buyer – not the transfer of mere

possession or limited interest as in the case of pledge, lease or hire purchase agreement). If goods remain in possession of seller after sale transaction is over, the 'possession' is with seller, but 'ownership' is with buyer. The Act uses the term 'general property' implying that sale involves total ownership and not a specific right limited by conditions.

Example:

Delivery of goods refers to a voluntary transfer of possession of goods from one person to another. Delivery may be constructive or actual depending upon the circumstances of each case. A contract may provide for the immediate delivery of the goods or immediate payment of the price or both. Alternatively, the delivery or payment may be made by installments or be postponed.

4) **Consideration is Price:** The consideration in a contract of sale has to be price i.e., money. If goods are offered as the consideration for goods, it will not amount to sale. It will be barter. If there is no consideration, it will be called gift. But where the goods are sold for definite sum and the price is paid partly in kind and partly in cash, the transaction is a sale.

Consideration is an essential for a valid contract as per the Indian Contract Act, 1872. It is the duty of a buyer who has received and appropriated the goods to pay a reasonable price. According to Section 2 (10) 'Price' means the money consideration for sale of goods, if the price is not fixed, the contract is void ab-initio.

Section 9 lays down how the price may be fixed in a contract of sale:

a) It can be fixed by the contract itself; or

b) It can be fixed in a manner provided by the contract. or

c) It can be determined by the course of dealings between the parties; or

d) If the price is not capable of being fixed in any of the ways mentioned ways, the buyer is bound to pay reasonable price. What is a reasonable price is a question of fact dependent on the circumstances of each particular case. It is not necessary that reasonable price should be equal to the market price.

Section 10 makes it clear that if the third party appointed under the agreement to fix the price cannot or does not make such valuation, then the agreement to sell goods will become void. If the third party is prevented in his valuation due to the buyer or the seller, the party not at fault can file a suit for damages against the party in fault.

5) **Essential elements of a valid contract:** All the essentials of a valid contract must be present. viz., competent parties, free consent, legal object and so on. The transfer of possession and ownership under the Act has to be voluntary and not be tainted with fraud or duress.

Time: Any stipulation with respect to time is not deemed to be of essence to a contract of sale unless a different intention appears from the terms of the contract.

11.6 Difference between Sale and Agreement to Sale

Difference between Sale and Agreement to Sale			
SR	**Subject Matter**	**Sale**	**Agreement to Sale**
1	**Nature of Contract**	Sale is an executed contract.	An Agreement to sale is an executor contract. In an Agreement to sale something remains to be done. It becomes sale only when the conditions of contract are fulfilled.
2	**Transfer of Property**	Transfer of Property takes place immediately in sale	Does not pass to the immediately.
3	**Creation of Right**	A sale creates "Jus in rem" means right in the goods against the whole world.	An agreement to sell creates a "Jus in person am" means a personal right against the buyer.
4	**Remedies in case of Breach**	In sale, the seller can sue for the price of goods. Seller has the right of lien, stoppage in transit and resale of goods.	In an agreement to sale, the sellar can only sue only for damages against non-performance of contract by the buyer.
5	**Consequences of insolvency**	If the buyer is adjudged insolvent, the seller must deliver the goods to official receiver.	In an agreement to sale the seller can refuse to deliver the goods unless paid for the goods.

11.7 SUMMARY

Originally, the transactions related to sale and purchase of goods was regulated by Chapter VII (Sections 76 to 123) of Indian Contract Act, 1872 – which was broadly based on English common law. A need was felt to overhaul the law due to rapid growth of mercantile transactions and various progressive English judgments being passed to meet the needs of the community. Thus, the provisions of Chapter VII were repealed, suitably amended keeping in mind the English Sales of Goods, 1893 and recent judicial decisions of the time. A separate act, the Sale of Goods Act came into force on 1st July 1930.

It extends to the whole of India except the State of Jammu and Kashmir. It does not affect rights, interests, obligations and titles acquired before the commencement of the Act. The Act deals with sale but not with mortgage or pledge of the goods.

11.7 GLOSSARY

(a). **Ab-initio** – From the very beginning.

(b). **Goods-** means every kind of movable property.

11.8 SAQS

1. Short Answer Questions-
a) What do you mean by Goods?
b) What is the objective Sale of Goods Act?
2. Fill in the blanks-
a) It extends to the whole of India except the.....
b) An Agreement to sale is an ..... contract
3. True and False type questions
a) Transfer of Property takes place immediately in sale.
(i)True, (ii) False.
b) In an agreement to sale, Seller has the right of lien, stoppage in transit and resale of goods.
(i)True, (ii) False.

11.9 REFERENCES

1. www.legalservicesindia.com/articles/tax_ec.htm
2. White paper on "E-Commerce", OECD, 1997
3. Vakul Sharma "E-commerce; new business paradigm" in S.K verma and Raman Mittal(ed.) Legal Dimensions of Cyber space p.no.51,
4. www.gartenner.com last visited on 4September, 2008.
5. http.//Europe.eu.int, last visited on 04-09-2008.
6. Introducing Electronic Commerce and EDI-EDI and the business cycle at http://www-106.ibm.com.
7. Priti Suri & Associattes, Open source and the law p.no.290, 2006.
8. Chetan Nagendra ,"The Net and the Tax Net". The Indian Tax Structure and the challenges posed by E-Comerce, in Nandan Kamath (ed) Law relating to computers, Internet and E-Commerce, p.349.
9. Sood V., Cyber Law simplified p.345,
10. http://www.ecomerce tax.com/official dos/India %20 e-commerce % 20 report % 2009 pdf.
11. http://www.ecomerce tax.com/official dos/India %20 e-commerce % 20 report % 2009 pdf.

12. Henrich H. Henry "A general Theory of Tax Structure change during Economic Development", Harward Law School, Cambridge, 1966

13. Alchian, A & H Demistez : "Production information coasts and Economic Organization" American Economic Review, 62 (1972)

14. Brodersen. "C.Taxation of Cross-border Electronic Commerce Germany", 25 Intertax - International Tax Review, issue (1997).

15. J.Yatindra Singh, Cyber Laws, P.46.

16. E-Commerce Taxation Principles : AGIIC perspecticve", on http://www.giic.org/focus/ecommerce/ectax.html

17. E-Commercetax.com

11.10 SUGGESTED READINGS

1. Income Tax, Service Tax & Vat Students' Guide to Income Tax– V.K.Singhania
2. Systematic Approach to Income Tax – Girish Ahuja.
3. Fundamentals of Corporate Accounting– J.R.Monga
4. Accounting Standards – Icai Publications. (Ca-Ipcc Level)

11.11 TERMINAL QUESTIONS AND MODEL QUESTIONS

a) Discuss in details about the need of Sale of Goods Act.

b) Describe the concept of creating a contract for sale?

Answers:

1. SAQ:

a) 14.3, 14.4 b) 14.2

2. Fill in the blanks:

a) The State of J & K b) executor

3. True and False type questions

a) True
b) False

4. Terminal Questions:

a) 14 .2 b) 13.3

UNIT-12

THE SPECIFIC RELIEF REGULATIONS, 1963

12.1 INTRODUCTION

The Specific Relief Act, 1963 (As amended by amendment Act No. 18 of, 2018.) was drafted by Parliament of India with an objective to provide remedies for Civil or Contractual Rights. It provides remedy in specie (specific remedy). It contains three parts which is divided in eight chapters. It contains 42 Sections and one schedule.

12.2 OBJECTIVE

It is an Act to define and amend the Law relating to certain kinds of specific relief like:

1. Recovery of Possession of Property
2. Specific Performance of Contract
3. Rectification of Contracts
4. Rescission of Contract

5. Cancellation of Instruments
6. Declaratory Decrees
7. Preventive Reliefs

PART I

12.3 PRELIMINARY

Section 1explains that:

(i) This Act may be called the Specific Relief Act, 1963.
(ii) It extends to the whole of India except the State of Jammu and Kashmir.
(iii)It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.

Definitions: Section 2 defines:

a) "obligation" includes every **duty enforceable** by law;
b) "settlement" means an instrument (other than a will or codicil as defined by the Indian Succession Act, 1925 (39 of 1925), whereby the destination or devolution of successive interests in movable or immovable property is disposed of or is agreed to be disposed of;
c) "trust" has the same meaning as in section 3 of the Indian Trusts Act, 1882 (2 of 1882), and includes an obligation in the nature of a trust within the meaning of Chapter IX of that Act;
d) "trustee" includes every person holding property in trust;
e) The words used herein but not defined, and defined in the Indian Contract Act, 1872 (9 of 1872), have the meanings respectively assigned to them in that Act.

Section 3 talks about Savings clause that Nothing shall deprived any right or relief provided by Indian Contract Act or by Indian Registration Act, 1908

Section 4 of this Act explains that Specific Relief to be granted only for enforcing individual's civil rights and not for enforcing Penal Laws. Penal Laws shall be enforced by their respective criminal laws.

CHAPTER II

12.4 RECOVERING POSSESSION OF PROPERTY (contained under Sections 5 to 8)

Recovery of Specific immovable property

Section 5 of this Act lays down that any person entitled to the possession of specific immovable property may recover it in the manner provided by the Code of Civil Procedure, 1908 (5 of 1908).[146]

[146] Dasappa v. Seetharam ILR1995KAR1683

Section 6 talks about the s**uit by person dispossessed of immovable property**— here these are the essentials for a suit dispossessed under this section:

(1) If any person is **dispossessed without his consent**
(2) of **immovable property**
(3) otherwise than in **due course of law,**
(4) he or any person (having sufficient interest)
(5) May institute a suit to recover the possession
(6) Exceptions; No suit under this section shall be brought—
    (a) After the expiry of six months from the date of dispossession; or
    (b) Against the Government.

(7) No **appeal** shall lie from any order or decree passed in any suit instituted under this section, nor shall any **review** of any such order or decree be allowed.

Nothing in this section shall bar any person from suing to establish his title to such property and to recover possession thereof under any relevant statute.

Recovery of Specific movable property

Section 7deals about the **Recovery of specific movable property** in the following manner—

A person entitled to the possession of specific movable property may recover it in the manner provided by the Code of Civil Procedure, 1908 (5 of 1908).

Explanation 1: A trustee may sue under this section for the possession of movable property to the beneficial interest in which the person for whom he is trustee is entitled.

Explanation 2: A special or temporary right to the present possession of movable property is sufficient to support a suit under this section.

Section 8 lays down the **Liability of person in possession, not as owner**, to deliver to persons entitled to immediate possession that:

Any person having the **possession or control** of a particular article of movable property, of which he is not the owner, may be compelled specifically to deliver it to the person entitled to its i**mmediate possession**, in any of the following cases:—

(a) When the thing claimed is held by the defendant as the agent or trustee of the plaintiff;

b) When compensation in money would not afford the plaintiff adequate relief for the loss of the thing claimed;

(c) When it would be extremely difficult to ascertain the actual damage caused by its loss;

(d) When the possession of the thing claimed has been wrongfully transferred from the plaintiff.

Explanation.—Unless and until the contrary is proved, the court shall, in respect of any article of movable property claimed under clause (b) or clause (c) of this section, presume—

(a) that compensation in money **would not afford** the plaintiff adequate relief for the loss of the thing claimed, or, as the case may be;

(b) that it would be extremely **difficult to ascertain** the actual damage caused by its loss.

CHAPTER III

12.5 SPECIFIC PERFORMANCE OF CONTRACTS

Section 9 provides some defences respecting suits for relief based on contract for specific performance of contract.

Except as otherwise provided herein where any relief is claimed under this Chapter in respect of a contract, the person against whom the relief is claimed may plead by way of defence any ground which is available to him under any law relating to contracts.

A. CONTRACTS WHICH CAN BE SPECIFICALLY ENFORCED

Section 10 deals with the **Specific performance in respect of contracts** in the following manner:

The specific performance of a contract shall be enforced by the court subject to the provisions contained in sub-section (2) of section 11, section 14 and section 16.

Section 11 deals with the Cases in which specific performance of contracts **connected with trusts enforceable:**

(1) Except as otherwise provided in this Act, specific performance of a contract shall, be enforced when the act agreed to be done is in the performance wholly or partly of a trust.

(2) A contract made by a trustee in excess of his powers or in breach of trust cannot be specifically enforced.

Section 12 talks about the **Specific performance** of part of contract:

(1) Except as otherwise hereinafter provided in this section, the court **shall not** direct the specific performance of a part of a contract.

(2) Where a party to a contract is **unable to perform the whole** of his part of it, but the part which must be left unperformed be a only a **small proportion** to the whole in value and admits of compensation in money, the court may, at the suit of either party, direct the specific performance of so much of the contract as can be performed, and award compensation in money for the deficiency.

(3) Where a party to a contract is unable to perform the whole of his part of it, and the part which must be left unperformed either— (a) forms a **considerable part of the whole**, though admitting of compensation in money; or

(b) does not admit of compensation in money; he is not entitled to obtain a decree for specific performance; but the court may, at the suit of the other party, direct the party in default to perform specifically so much of his part of the contract as he can perform, if the other party—

(i) in a case falling under clause (a), pays or has paid the agreed consideration for the whole of the contract reduced by the consideration for the part which must be left unperformed and in a case falling under clause (b) [pays or has paid] the consideration for the whole of the contract without any abatement; and

(ii) in either case, relinquishes all claims to the performance of the remaining part of the contract and all right to compensation, either for the deficiency or for the loss or damage sustained by him through the default of the defendant.

(4) When a part of a contract which, taken by itself, can and ought to be specifically performed, stands on a separate and independent footing from another part of the same contract which cannot or ought not to be specifically performed the court may direct specific performance of the former part. **Explanation—**

For the purposes of this section, a party to a contract shall be deemed to be unable to perform the whole of his part of it if a portion of its subject-matter existing at the date of the contract has ceased to exist at the time of its performance.

Section 13 talks about the **Rights of purchaser or lessee** against person with no title or imperfect title:

(1) Where a person contracts to sell or let certain immovable property having no title or only an imperfect title, the **purchaser or lessee** (subject to the other provisions of this Chapter), has the following rights, namely:

(a) if the vendor or lessor has subsequently to the contract acquired any interest in the property, the purchaser or lessee **may compel him to make good the contract** out of such interest;

(b) where the concurrence of other person is necessary for validating the title, and they are bound to concur at the request of the vendor or lessor, the purchaser or lessee may compel him to procure such concurrence, and when a **conveyance by other persons is necessary** to validate the title and they are bound to convey at the request of the vendor or lessor, the purchaser or lessee **may compel** him to procure such conveyance;

(c) where the vendor professes to sell unencumbered property, but the property is mortgaged for an amount not exceeding the purchase money and the vendor has in fact only a right to redeem it, the

(d) where the vendor or lessor sues for specific performance of the contract and the suit is dismissed on the ground of his want of title or imperfect title, the defendant has a right to a return of his deposit, if any, with interest thereon, to his costs of the suit, and to a lien for such deposit, interest and costs on the interest, if any, of the vendor or lesser in the property which

is the subject-matter of the contract. (2) The provisions of sub-section (1) shall also apply, as far as may be, to contracts for the sale or hire of movable property.

B. CONTRACTS, WHICH CANNOT BE SPECIFICALLY ENFORCED

Section 14 lays down about the Contracts not specifically enforceable. The following contracts cannot be specifically enforced, namely:

(a) Where a party to the contract has obtained **substituted performance** of contract in accordance with the provisions of section 20;

(b) A contract, the performance of which involves the performance of a **continuous duty** which the court cannot supervise;

(c) A contract which is so dependent on the **personal qualifications** of the parties that the court cannot enforce specific performance of its material terms; and

(d) A contract which is in its nature **determinable**.

Section 14A lays down about the Power of court to **engage experts**:

(1) Without prejudice to the generality of the provisions contained in the Code of Civil Procedure, 1908 (5 of 1908), in any suit under this Act, where the court considers it necessary to get expert opinion to assist it on any specific issue involved in the suit, it may engage one or more experts and direct to report to it on such issue and may secure attendance of the expert for providing evidence, including production of documents on the issue.

(2) The court may require or direct any person to give relevant information to the expert or to produce, or to provide access to, any relevant documents, goods or other property for his inspection.

(3) The opinion or report given by the expert **shall form part of the record of the suit**; and the court, or with the permission of the court any of the parties to the suit, may examine the expert personally in open court on any of the matters referred to him or mentioned in his opinion or report, or as to his opinion or report, or as to the manner in which he has made the inspection.

(4) The expert shall be entitled to such **fee, cost or expense** as the court may fix, which shall be payable by the parties in such proportion, and at such time, as the court may direct.]

Section 15 lays down about the **PERSONS FOR OR AGAINST** WHOM CONTRACTS MAY BE SPECIFICALLY ENFORCED

Who may obtain specific performance:

Except as otherwise provided by this Chapter, the specific performance of a contract may be obtained by:

(a) Any party thereto;

(b) The representative in interest or the principal, of any party thereto:

Provided that where the learning, skill, solvency or any personal quality of such party is a material ingredient in the contract, or where the contract provides that his interest shall not be assigned, his representative in interest or his principal shall not be entitled to specific performance of the contract, **unless** such party has already performed his part of the contract, or the performance thereof by his representative in interest, or his principal, has been accepted by the other party;

(c) Where the contract is a settlement on marriage, or a compromise of doubtful rights between members of the same family, any person beneficially entitled there under;

(d)Where the contract has been entered into by a tenant for life in due exercise of a power, the remainder man;

(e) A reversioner in possession, where the agreement is a covenant entered into with his predecessor in title and the reversioner is entitled to the benefit of such covenant;

f) A reversioner in remainder, where the agreement is such a covenant, and the reversioner is entitled to the benefit thereof and will sustain material injury by reason of its breach;

(fa) When a limited liability partnership has entered into a contract and subsequently becomes amalgamated with another limited liability partnership, the new limited liability partnership which arises out of the amalgamation.]

(g) When a company has entered into a contract and subsequently becomes amalgamated with another company, the new company which arises out of the amalgamation;

(h) When the promoters of a company have, before its incorporation, entered into a contract for the purposes of the company, and such contract is warranted by the terms of the incorporation, the company: Provided that the company has accepted the contract and has communicated such acceptance to the other party to the contract.

Section 16 deals with the Personal bars to relief. **Specific performance of** a contract cannot be enforced in favour of a person:

(a) Who has obtained substituted performance of contract under section 20;

(b) Who has become incapable of performing, or violates any essential term of, the contract that on his part remains to be performed, or acts in fraud of the contract, or willfully acts at variance with, or in subversion of, the relation intended to be established by the contract; or

(c) Who fails to prove] that he has performed or has always been ready and willing to perform the essential terms of the contract which are to be performed by him, other than terms of the performance of which has been prevented or waived by the defendant.

Explanation — For the purposes of clause (c)—

(i) where a contract involves the payment of money, it is not essential for the plaintiff to actually tender to the defendant or to deposit in court any money except when so directed by the court;

(ii) the plaintiff [must prove] performance of, or readiness and willingness to perform, the contract according to its true construction.

Section 17 talks about the Contract to sell or let property by one who has no title, not specifically enforceable:

(1) A contract to sell or let any immovable property cannot be specifically enforced in favour of a vendor or lessor—

(a) who, knowing himself not to have any title to the property, has contracted to sell or let the property; (b) who, though he entered into the contract believing that he had a good title to the property, cannot at the time fixed by the parties or by the court for the completion of the sale or letting, give the purchaser or lessee a title free from reasonable doubt.

(2) The provisions of sub-section (1) shall also apply, as far as may be, to contracts for the sale or hire of movable property.

Section 18 deals with non-enforcement except with **variation**:

Where a plaintiff seeks specific performance of a contract in writing, to which the defendant sets up a variation, the plaintiff cannot obtain the performance sought, except with the variation so set up, in the following cases, namely:—

(a) Whereby fraud, mistake of fact or mis-representation, the written contract of which performance is sought is in its terms or effect different from what the parties agreed to, or does not contain all the terms agreed to between the parties on the basis of which the defendant entered into the contact;

(b) Where the object of the parties was to produce a certain legal result which the contract as framed is not calculated to produce;

(c) Where the parties have, subsequently to the execution of the contract, varied its terms.

Section 19 deals with the **Relief against parties and persons** claiming under them by subsequent title:

Except as otherwise provided by this Chapter, specific performance of a contract may be enforced against—

(a) Either party thereto;

(b) Any other person claiming under him by a title arising subsequently to the contract, except a transferee for value who has paid his money in good faith and without notice of the original contract;

(c) Any person claiming under a title which, though prior to the contract and known to the plaintiff, might have been displaced by the defendant;

(ca) When a limited liability partnership has entered into a contract and subsequently becomes amalgamated with another limited liability partnership, the new limited liability partnership which arises out of the amalgamation.

(d) When a company has entered into a contract and subsequently becomes amalgamated with another company, the new company which arises out of the amalgamation;

(e) When the promoters of a company have, before its incorporation, entered into a contract for the purpose of the company and such contract is warranted by the terms of the incorporation, the company:

Provided that the company has accepted the contract and communicated such acceptance to the other party to the contract.

C. SUBSTITUTED PERFORMANCE OF CONTRACTS, ETC

Section 20 lays down that the Substituted performance of contract-

(1) Without prejudice to the generality of the provisions contained in the Indian Contract Act, 1872 (9 of 1872), and, except as otherwise agreed upon by the parties, where the contract is broken due to non-performance of promise by any party, the party who suffers by such breach shall have the option of substituted performance through a third party or by his own agency, and, recover the expenses and other costs actually incurred, spent or suffered by him, from the party committing such breach.

(2) No substituted performance of contract under sub-section (1) shall be undertaken unless the party who suffers such breach has given a notice in writing, of not less than thirty days, to the party in breach calling upon him to perform the contract within such time as specified in the notice, and on his refusal or failure to do so, he may get the same performed by a third party or by his own agency: Provided that the party who suffers such breach shall not be entitled to recover the expenses and costs under sub-section (1) unless he has got the contract performed through a third party or by his own agency.

(3) Where the party suffering breach of contract has got the contract performed through a third party or by his own agency after giving notice under sub-section (1), he shall not be entitled to claim relief of specific performance against the party in breach.

(4) Nothing in this section shall prevent the party who has suffered breach of contract from claiming compensation from the party in breach.

In addition section 20A lays down that the Special provisions for contract relating to infrastructure project-

(1) No **injunction** shall be granted by a court in a suit under this Act involving a contract relating to an infrastructure project specified in the Schedule, where granting injunction would cause impediment or delay in the progress or completion of such infrastructure project.

Explanation- For the purposes of this section, section 20B and clause (ha) of section 41, the expression “infrastructure project” means the category of projects and infrastructure Sub-Sectors specified in the Schedule.

(2) The Central Government may, depending upon the requirement for development of infrastructure projects, and if it considers necessary or expedient to do so, by notification in the

Official Gazette, amend the Schedule relating to any Category of projects or Infrastructure Sub-Sectors.

(3) Every notification issued under this Act by the **Central Government** shall be laid, as soon as may be after it is issued, before each House of Parliament, while it is in session, for a total period of **thirty days** which may be comprised in **one session or in two or more successive sessions**, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or both Houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification.

Here section 20 (b) talks about **Special Courts**-

The State Government, in consultation with the Chief Justice of the High Court, shall designate, by notification published in the Official Gazette, one or more Civil Courts as Special Courts, within the local limits of the area to exercise jurisdiction and to try a suit under this Act in respect of contracts relating to infrastructure projects.

Section 20 (C) deals with Expeditious disposal of suits-

Notwithstanding anything contained in the Code of Civil Procedure, 1908 (5 of 1908), a suit filed under the provisions of this Act shall be disposed of by the court within a period of twelve months from the date of service of summons to the defendant: Provided that the said period may be extended for a further period not exceeding six months in aggregate after recording reasons in writing for such extension by the court.

Further Section 21 talks about the **Power to award compensation** in certain cases-

(1) In a suit for specific performance of a contract, the plaintiff may also claim compensation for its breach in addition to such performance.

(2) If, in any such suit, the court decides that specific performance ought not to be granted, but that there is a contract between the parties which has been broken by the defendant, and that the plaintiff is entitled to compensation for that breach, it shall award him such compensation accordingly.

(3) If, in any such suit, the court decides that specific performance ought to be granted, but that it is not sufficient to satisfy the justice of the case, and that some compensation for breach of the contract should also be made to the plaintiff, it shall award him such compensation accordingly.

(4) In determining the amount of any compensation awarded under this section, the court shall be guided by the principles specified in section 73 of the Indian Contract Act, 1872 (9 of 1872).

(5) No compensation shall be awarded under this section unless the plaintiff has claimed such compensation in his plaint: Provided that where the plaintiff has not claimed any such

compensation in the plaint, the court shall, at any stage of the proceeding, allow him to amend the plaint on such terms as may be just, for including a claim for such compensation.

Explanation- The circumstances that the contract has become incapable of specific performance does not preclude the court from exercising the jurisdiction conferred by this section.

Here Section 22 deals with the **Power to grant relief** for possession, partition, refund of earnest money, etc.—

(1) Notwithstanding anything to the contrary contained in the Code of Civil Procedure,1908 (5 of 1908), any person suing for the specific performance of a contract for the transfer of immovable property may, in an appropriate case, ask for-

(a) possession, or partition and separate possession, of the property in addition to such performance; or (b) any other relief to which he may be entitled, including the refund of any earnest money or deposit paid or 1 [made by] him, in case his claim for specific performance is refused.

(2) No relief under clause (a) or clause (b) of sub-section (1) shall be granted by the court unless it has been specifically claimed: Provident that where the plaintiff has not claimed any such relief in the plaint, the court shall, at any stage of the proceeding, allow him to amend the plaint on such terms as may be just for including a claim for such relief.

(3) The power of the court to grant relief under clause (b) of sub-section (1) shall be without prejudice to its powers to award compensation under section 21.

Section 23 deals with the **Liquidation of damages not a bar to specific performance-**

(1) A contract, otherwise proper to be specifically enforced, may be so enforced, though a sum be named in it as the amount to be paid in case of its breach and the party in default is willing to pay the same, if the court, having regard to the terms of the contract and other attending circumstances, is satisfied that the sum was named only for the purpose of securing performance of the contract and not for the purpose of giving to the party in default an option of paying money in lieu of specific performance.

(2) When enforcing specific performance under this section, the court shall not also decree payment of the sum so named in the contract.

Section 24 talks about the **Bar of suit for compensation for breach after dismissal of suit for specific performance-**

The dismissal of a suit for specific performance of a contract or part thereof shall bar the plaintiff's right to sue for compensation for the breach of such contract or part, as the case may be, but shall not bar his right to sue for any other relief to which he may be entitled, by reason of such breach.

12.6 ENFORCEMENT OF AWARDS AND DIRECTIONS TO EXECUTE SETTLEMENTS

Section 25 deals with the **Application of preceding sections to certain awards and testamentary directions to execute settlements.—**

The provisions of this Chapter as to contracts shall apply to awards to which [the Arbitration and Conciliation Act, 1996 (26 of 1996)], does not apply and to directions in a will or codicil to execute a particular settlement.

CHAPTER III

12.7 RECTIFICATION OF INSTRUMENTS

Section 26 explains that **When instrument may be rectified-**

(1) When, through **fraud or a mutual mistake** of the parties a contract or other instrument in writing [not being the articles of association of a company to which the Companies Act, 1956 (1 of 1956), applies] does not express their real intention, then-

(a) either **party or his representative** in interest may institute a suit to have the instrument rectified; or

(b) the plaintiff may, in any suit in which any right arising under the instrument is in issue, claim in his pleading that the instrument be rectified; or

(c) a defendant in any such suit as is referred to in clause (b), may, in addition to any other defence open to him, ask for rectification of the instrument.

(2) If, in any suit in which a contract or other instrument is sought to be rectified under sub-section (1), the court finds that the instrument, through fraud or mistake, does not **express the real intention** of the parties, the court may in its discretion, direct rectification of the instrument so as to express that intention, so far as this can be done without prejudice to rights acquired by third persons in good faith and for value.

(3) A contract in writing may first be rectified, and then if the party claiming rectification has so prayed in his pleading and the court thinks fit, may be specifically enforced.

(4) No relief for the rectification of an instrument shall be granted to any party under this section unless it has been specifically claimed: Provided that where a party has not claimed any such relief in his pleading, the court shall, at any stage of the proceeding, allow him to **amend the pleading** on such terms as may be just for including such claim.

CHAPTER IV

12.8 RESCISSION OF CONTRACTS

Section 27 explains that **When rescission may be adjudged or refused-**

(1) Any person interested in a contract may sue to have it rescinded, and such rescission may be adjudged by the court in any of the following cases, namely:

(a) Where the contract is **voidable or terminable** by the plaintiff;

(b) Where the contract is **unlawful** for causes not apparent on its face and the defendant is more to **blame** than the plaintiff.

(2) Notwithstanding anything contained in sub-section (1), the court may **refuse to rescind** the contract-

(a) Where the plaintiff has **expressly or impliedly ratified** the contract; or

(b) Where, owing to the **change of circumstances** which has taken place since the making of the contract (not being due to any act of the defendant himself), the parties cannot be substantially restored to the position in which they stood when the contract was made; or

(c) Where third parties have, during the subsistence of the contract, **acquired rights in good faith** without notice and for value; or

(d) Where only a part of the contract is sought to be rescinded and such part is **not severable** from the rest of the contract.

Explanation.—In this section "contract" in relation to the territories to which the Transfer of Property Act, 1882 (4 of 1882), does not extend, means a contract in writing.

In addition Section 28 deals with **Rescission in certain circumstances of contracts for the sale or lease of immovable property, the specific performance of which has been decreed-**

(1) Where in any suit a decree for specific performance of a contract for the sale or lease of immovable property has been made and the purchaser or lessee does not, within the period allowed by the decree or such further period as the court may allow, pay the purchase money or other sum which the court has ordered him to pay, the vendor or lessor may apply in the same suit in which the decree is made, to have the contract rescinded and on such application the court may, by order, rescind the contract either so far as regards the party in default or altogether, as the justice of the case may require.

(2) Where a contract is rescinded under sub-section (1), the court-

(a) Shall direct the purchaser or the lessee, if he has obtained possession of the property under the contract, to restore such possession to the vendor or lessor; and

(b) May direct payment to the vendor or lessor of all the rents and profits which have accrued in respect of the property from the date on which possession was so obtained by the purchaser or lessee until restoration of possession to the vendor or lessor, and, if the justice of the case so requires, the 13 refund of any sum paid by the vendee or the lessee as earnest money or deposit in connection with the contract.

(3) If the purchase or lessee pays the purchase money or other sum which he is ordered to pay under the decree within the period referred to in sub-section (1), the court may, on application made in the same suit, award the purchaser or lessee such further relief as he may be entitled to, including in appropriate cases all or any of the following reliefs, namely:—

(a) the execution of a proper conveyance or lease by the vendor or lessor;

(b) the delivery of possession, or partition and separate possession, of the property on the execution of such conveyance or lease.

(4) No separate suit in respect of any relief which may be claimed under this section shall lie at the instance of a vendor, purchaser, lessor or lessee, as the case may be.

(5) The costs of any proceedings under this section shall be in the discretion of the court.

Section 29 deals with the **Alternative prayer for rescission** in suit for specific performance-

A plaintiff instituting a suit for the specific performance of a contract in writing may pray in the alternative that, if the contract cannot be specifically enforced, it may be rescinded and delivered up to be cancelled; and the court, if it refuses to enforce the contract specifically, may direct it to be rescinded and delivered up accordingly.

Section 30 explains that the **Court may require parties rescinding to do equity-**

On adjudging the rescission of a contract, the court may require the party to whom such relief is granted to restore, so far as may be, any benefit which he may have received from the other party and to make any compensation to him which justice may require.

CHAPTER V

12.9 CANCELLATION OF INSTRUMENTS

31. When cancellation may be ordered-

(1) Any person against whom a written instrument is **void or voidable**, and who has reasonable apprehension that such instrument, if left outstanding may cause him **serious injury**, may sue to have it adjudged void or voidable; and the court may, in its discretion, so adjudge it and order it to be delivered up and cancelled.

(2) If the instrument has been registered under the Indian Registration Act, 1908 (16 of 1908), the court shall also send a copy of its decree to the officer in whose office the instrument has been so registered; and such officer shall note on the copy of the instrument contained in his books the fact of its cancellation.

SECTION 32 What instruments may be partially cancelled-

Where an instrument is evidence of different rights or different obligations, the court may, in a proper case, cancel it in part and allow it to stand for the residue.

SECTION 33 Power to require benefit to be restored or compensation to be made when instrument is cancelled or is successfully resisted as being void or voidable-

(1) On adjudging the cancellation of an instrument, the court may require the party to whom such relief is granted, to restore, so far as may be any benefit which he may have received from the other party and to make any compensation to him which justice may require.

(2) Where a defendant successfully resists any suit on the ground—

(a) that the instrument sought to be enforced against him in the suit is voidable, the court may if the defendant has received any benefit under the instrument from the other party, require him to restore, so far as may be, such benefit to that party or to make compensation for it;

(b) that the agreement sought to be enforced against him in the suit is void by reason of his not having been competent to contract under section 11 of the Indian Contract Act, 1872 (9 of 1872), the court may, if the defendant has received any benefit under the agreement from the other party, require him to restore, so far as may be, such benefit to that party, to the extent to which he or his estate has benefited thereby.

CHAPTER VI

12.10 DECLARATORY DECREES

SECTION 34 Discretion of court as to declaration of status or right-

Any person entitled to any legal character, or to any right as to any property, may institute a suit against any person denying, or interested to deny, his title to such character or right, and the court may in its discretion make therein a declaration that he is so entitled, and the plaintiff need not in such suit ask for any further relief:

Provided that no court shall make any such declaration where the plaintiff, being able to seek further relief than a mere declaration of title, omits to do so.

Explanation.—A trustee of property is a "person interested to deny" a title adverse to the title of some one who is not inexistence, and for whom, if in existence, he would be a trustee.

SECTION 35 Effect of declaration-

A declaration made under this Chapter is binding only on the parties to the suit, persons claiming through them respectively, and, where any of the parties are trustees, on the persons for whom, if in existence at the date of the declaration, such parties would be trustees.

PART III PREVENTIVE RELIEF

CHAPTER VII

12.11 INJUNCTIONS GENERALLY

SECTION 36 Preventive relief how granted-

Preventive relief is granted at the discretion of the court by injunction, temporary or perpetual.

SECTION 37 Temporary and perpetual injunctions-

(1) Temporary injunctions are such as are to continue until a specific time, or until the further order of the court, and they may be granted at any stage of a suit, and are regulated by the Code of Civil Procedure, 1908 (5 of 1908).

(2) A perpetual injunction can only be granted by the decree made at the hearing and upon the merits of the suit; the defendant is thereby perpetually enjoined from the assertion of a right, or from the commission of an act, which would be contrary to the rights of the plaintiff.

CHAPTER VIII

12.12 PERPETUAL INJUNCTIONS

SECTION 38 Perpetual injunction when granted-

(1) Subject to the other provisions contained in or referred to by this Chapter, a perpetual injunction may be granted to the plaintiff to prevent the breach of an obligation existing in his favour, whether expressly or by implication.

(2) When any such obligation arises from contract, the court shall be guided by the rules and provisions contained in Chapter II.

(3) When the defendant invades or threatens to invade the plaintiff's right to, or enjoyment of, property, the court may grant a perpetual injunction in the following cases, namely:—

(a) Where the defendant is trustee of the property for the plaintiff;

(b) Where there exists no standard for ascertaining the actual damage caused, or likely to be caused, by the invasion;

(c) Where the invasion is such that compensation in money would not afford adequate relief;

(d) Where the injunction is necessary to prevent a multiplicity of judicial proceedings.

SECTION 39 Mandatory injunctions-

When, to prevent the breach of an obligation, it is necessary to compel the performance of certain acts which the court is capable of enforcing, the court may in its discretion grant an injunction to prevent the breach complained of, and also to compel performance of the requisite acts.

SECTION 40 Damages in lieu of, or in addition to, injunction-

(1) The plaintiff in a suit for perpetual injunction under section 38, or mandatory injunction under section 39, may claim damages either in addition to, or in substitution for, such injunction and the court may, if it thinks fit, award such damages.

(2) No relief for damages shall be granted under this section unless the plaintiff has claimed such relief in his plaint:

Provided that where no such damages have been claimed in the plaint, the court shall, at any stage of the proceedings, allow the plaintiff to amend the plaint on such terms as may be just for including such claim.

(3) The dismissal of a suit to prevent the breach of an obligation existing in favour of the plaintiff shall bar his right to sue for damages for such breach.

SECTION 41 Injunction when refused-

An injunction cannot be granted-

(a) to restrain any person from prosecuting a judicial proceeding pending at the institution of the suit in which the injunction is sought, unless such restraint is necessary to prevent a multiplicity of proceedings;

(b) to restrain any person from instituting or prosecuting any proceeding in a court not sub-ordinate to that from which the injunction is sought;

(c) to restrain any person from applying to any legislative body;

(d) to restrain any person from instituting or prosecuting any proceeding in a criminal matter;

(e) to prevent the breach of a contract the performance of which would not be specifically enforced;

(f) to prevent, on the ground of nuisance, an act of which it is not reasonably clear that it will be a nuisance;

(g) to prevent a continuing breach in which the plaintiff has acquiesced;

(h) when equally efficacious relief can certainly be obtained by any other usual mode of proceeding except in case of breach of trust;

[(ha) if it would impede or delay the progress or completion of any infrastructure project or interfere with the continued provision of relevant facility related thereto or services being the subject matter of such project.]

(i) when the conduct of the plaintiff or his agents has been such as to disentitle him to be the assistance of the court;

(j) when the plaintiff has no personal interest in the matter.

SECTION 42 Injunction to perform negative agreement.—

Notwithstanding anything contained in clause (e) of section 41, where a contract comprises an affirmative agreement to do a certain act, coupled with a negative agreement, express or implied, not to do a certain act, the circumstance that the court is unable to compel specific performance of the affirmative agreement shall not preclude it from granting an injunction to perform the negative agreement.

Provided that plaintiff has not failed to perform the contract so far as it is binding on him.

12.13 SUMMARY: Specific Relief Act provides specific performance which has traced its origin out of set principles of equity. When Damages are not adequate remedy we want some specific remedy to do justice. This Specific Relief Act is a collective bundle of such specific remedies. These remedies are in form of injunction but it is not confined to itself. As we have seen in the objectives of this Act, it deals with different other remedies like:

1. Recovery of Possession of Property
2. Specific Performance of Contract
3. Rectification of Contracts
4. Rescission of Contract
5. Cancellation of Instruments
6. Declaratory Decrees
7. Preventive Reliefs

An order for specific relief cannot be ordered if money in compensation is an adequate relief. In the case of sever hardship to the defendant on unconscionable contracts. Claimant has unclean hands, contract requires constant supervision etc.

12.14 GLOSSARY

1. **Injunctions:** An order to do or not to do something**.**
2. Instrument: A formal Legal document.
3. Performance: How a person does a piece of work.
12.15 SAQS

A. Short Answer Questions:

(a) Define obligation.

(b) Define injunction.

B. Fill in the Blanks:

(a) The specific performance of a contract shall be enforced by the.....

(b) Section 16 deals with the.....to relief.

C. True and False:

(a) Section 6 talks about the suit by person dispossessed of immovable property.

(i) True (ii) False

(b) Section 13 talks about the Rights of purchaser or lessee against person with no title or imperfect title.

(i) True (ii) False

12.16 SUGGESTED READINGS:

1. Specific Relief Act, 1963,
2. Specific Relief Act by R.K. Bangia

3. Specific Relief Act by Pollack & Mulla
4. Specific Relief Act by Sarkar

12.17 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. What are the various specific remedies available under Specific Relief Act, 1963?
2. What are the essentials of declaratory suits?
3. When a Contract is part performed?

Answer to Short Questions:

A. SAQS

(a) Refer 2.3 (b) 12.11

B. Fill in the blanks:

(a) Refer 12.5 (b) Refer 12.5

C. True and False

(a) Refer 2.4 (b) Refer 2.5

Answer to Terminal Questions:

(1)Refer Specific Relief Act, 1963 (2) Refer 12.10 (3) Refer 12.5

UNIT-13

THE CONSUMER PROTECTION REGULATIONS, 1986

13 .1 INTRODUCTION

In India Consumer Protection as a movement ensured the safe interest of consumers by enactment of the The Consumer Protection Act. The Consumer Protection Act, 1986 was introduced in the Lok Sabha on 5th December, 1986 to provide better protection in the interest of consumers. Consumer Protection Act has been enacted as a form of social welfare legislation resulting out of widespread consumer protection movements in India.

It provides the establishment of consumer councils and other authorities for the settlement of consumers' disputes and also for the matters connected therewith. The act was passed by Assembly in October 1986 and came into force on 24 December 1986. It extends to the whole of India except the State of Jammu and Kashmir.

The act makes provisions to include both tangible goods and intangible services (henceforth referred to as product) purchased from a trader or service provider (henceforth referred to as company).The act can apply to any consumer who uses the product for non-commercial activities, the only exception being use of it to earn his livelihood. In other words, the act excludes commercial customers fully, but includes individual domestic customers, groups of domestic customers, societies and not-for-profit organizations.

13.2 OBJECTIVES:

The Consumer Protection Act, 1986, aims to provide:

1. To promote and protect the rights of consumers.
2. To be established Consumer Protection Council at the Central and State level.
3. Speedy and simple redressal to consumer disputes.

4. The thoughtful piece of legislation intends to protect the consumers at large from exploitation.
5. As a Magna Carta this statute is for checking the unfair trade practices and 'defect in goods' and 'deficiencies in services'.
6. It led to the establishment of a widespread network of consumer forums and appellate courts all over India.
7. It is significant to note it's impacted that how businesses approach, consumer complaints and empowered consumers are affected to a great extent[147]

13.3 DEFINITIONS:

Some of the important definitions under Consumer Protection Act, 1986 are as follows:

COMPALINANT[148]:

In order to initiate an action under the Consumer Protection Act, 1986, a complaint is required from the complainant. The term 'complaint' has been defined in section 2(1) (c) of the Act. According to clause (b) of section 2 (1) of the Consumer Protection Act for filing a complaint a COMPLAINANT is required and the complaint can be made by any of the following as a complainant:

i. a consumer or
ii. any voluntary consumer association registered under the Companies Act, 1956 (1 of 1956), or under any other law for the time being in force; or
iii. the Central Government or any State Government, who or which makes a complaint; or
iv. one or more consumers, where there are numerous consumers having the same interest;
v. In case of death of a consumer, his legal heir or representative.

Complaint under section 2(c) means any allegation in writing made by a complainant that:

(i) An unfair trade practice or a restrictive trade practice has been adopted by any trader or service provider

(ii) The goods bought by him or agreed to be bought by him suffer from one or more defects

(iii)The services hired or availed of or agreed to be hired or availed of by him suffer from deficiency in any respect

(iv) A trader or the service provider, as the case may be, has charged for the goods or for the services mentioned in the complaint, a price in excess of the price fixed or displayed

CONSUMER

Section. 2 (1) (d) of the Consumer Protection Act, 1986, defines "consumer" as any person who buys any goods for a consideration, who pays or will pay. Hires or avails any service for a consideration for which he has paid or will pay. However, it does not include a person obtaining goods for resale or any commercial purpose.

[147] Kumar, Vineet. "An Analysis of Consumer Protection Laws in India". iPleaders. Retrieved 10 December 2016.

[148] https://shodhganga.inflibnet.ac.in/bitstream/10603/7831/11/11_chapter%203.pdf

CONSUMER DISPUTE

Under section 2 (e) means a dispute where the person against whom a complaint has been made, denies or disputes the allegations contained in the complaint.

DEFECT

Under section 2 (f) means any fault, imperfection or shortcoming in the quality, quantity, potency, purity or standard which is required to be maintained by or under any law for the time being in force or under any contract, express or implied or as is claimed by the trader in any manner whatsoever in relation to any goods.

DEFICIENCY

Under section 2 (g) means any fault, imperfection, shortcoming or inadequacy in the quality, nature and manner of performance which is required to be maintained by or under any law for the time being in force or has been undertaken to be performed by a person in pursuance of a contract or otherwise in relation to any service

GOODS

Under section 2 (i) means goods as defined in the Sale of Goods Act, 1930.

13.4 CONSUMER DISPUTES REDRESS FORUMS

It includes anyone who consumes goods or services at the end of the claim of production.[149]

The definition of consumer may be discussed in following two parts:-

(i) Consumer of goods

(ii) Consumer of services

According to sub-clause (i) of section 2(1) (d) a consumer of goods and services means any person who-

(a) **buys any goods** for consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment,

(b) includes any **user of such goods** other than the person who buys the, when such use is made with the approval of the buyer but

(c) **does not include** a person who obtains such goods for resale or for any commercial purpose. Commercial purpose does not include use by a consumer of goods bought by and used by him exclusively for the purpose of earning his livelihood, by means of self-employment.

The above provision discloses that a person claiming himself to be a consumer should fulfill the following **requirements**:

(i) there should be a sale transaction between the seller and the buyer,

(ii) the sale must be of goods,

(iii) the buying of goods must be for consideration,

[149] Morgan Stanley Fund v. Kartick Dass & ors. (1994) II CPJ 7 (S.C.)

(iv) the consideration has been paid or promised or partly paid and partly promised, or under any system of deferred payment; and
(v) the user of the goods may also be a consumer when such use is made with the approbation of the buyer.
It may, however, be noted that a person who obtains the goods for resale or for any commercial purpose is not included within the meaning of the term consumer. This clearly reveals that the intention of the legislature is to restrict the benefits of the Consumer Protection Act to ordinary consumers buying goods or hiring services for consumption and not for resale or large scale commercial activity. Where the goods have been purchased or used by the consumer exclusively for the purpose of earning his livelihood, by means of self-employment, such use of the goods will not be treated as 'commercial purpose.[150]

- **Rights of a Consumer**

Under the Consumer Protection Act, 19886, Consumers Rights include:
the consumers Right to Safety,

1. Right to Consumer Education,
2. Right to Information,
3. The right to be protected against marketing of goods which are hazardous to life and property.
4. The right to be informed about the quality, quantity, potency, purity, standard and price of goods to protect the consumer against unfair trade practices.
5. The right to be assured, wherever possible, access to an authority of goods at competitive prices.
6. The right to be heard and to be assured that consumers interests will receive due consideration at appropriate forums.
7. The right to seek redressal against unfair trade practices or unscrupulous exploitation of consumers.

13.5 REDRESSAL AGENCY

In order to achieve the aims and objectives of this Act, the Consumer Protection Act, 1986, sets up redressal agencies under chapter III in the following manner:

1. District Forum,
2. State Commission and
3. National Commission

13.5.1 COMPOSITION OF THE DISTRICT FORUM

1) a person who is, or has been, or is qualified to be a District Judge, who shall be its President,
2) two other members, one of whom shall be a woman, who shall have the following qualifications, namely
    i. be not less than thirty-five years of age,
    ii. possess a bachelor's degree from a recognized university,

[150] The consumer protection Act, 1986 Explanation under clause (d) of Sec. 2(1).

iii. be persons of ability, integrity and standing, and have adequate problems relating to economics, law, commerce, accountancy, industry public affairs or administration.

Every member of the District Forum shall hold office for a term of five years or up to the age of 65 years, whichever is earlier.

JURISDICTION OF THE DISTRICT FORUM

(I) Subject to the other provisions of this Act, the District Forum shall have jurisdiction to entertain complaints where the value of the goods or services and the compensation, if any, claimed does not exceed rupees twenty lakhs.

Manner in which complaint shall be made

A complaint in may be filed with a District Forum by the consumer or any recognised consumer association one or more consumers, Central or the State Government. The complaint should be given with required amount of fee. Once the compliant is received it should proceed with it within 21 days. District forum will sent a copy of complaint to the counter parties. If the counter party is not taking appropriate action within 30 days forum will precede the action. If opposition reply by denying the complaint forum will fix date to hear the parties and will take decision after hearing both parties.

Finding of the District Forum: District forum will have following decisions:

a) Complaints where the value of the goods or services and compensation, if any, claimed does not exceeds rupees twenty lakhs.
b) to remove the defect pointed but by the appropriate laboratory from the goods in question;
c) (b) to replace the goods with new goods of similar description which shall be free from any defect;
d) (c) to return to the complainant the price, or, as the case may be, the charges paid by the complainant;
e) (d) to pay such amount as may be awarded by it as compensation to the consumer for any loss or injury suffered by the consumer due to the negligence of the opposite party
f) to remove the defects in goods or deficiencies in the services
g) to discontinue the unfair trade practice
h) (g) to withdraw the hazardous goods from being offered for sale;
i) (h) to cease manufacture of hazardous goods and to desist from offering services which are hazardous in nature
j) to provide for adequate costs to parties

Appeal

Any person aggrieved by an order made by the District Forum may prefer an appeal against such order to the State Commission within a period of thirty days from the date of the order, in such form and manner as may be prescribed.

13.5.2 COMPOSITION OF THE STATE COMMISSION

State Commission shall consist of

A person who is or has been a Judge of a High Court, appointed by the State Government, who shall be its President and not less than two and not more than such number of members, as may be prescribed, and one of who shall be a woman.

Jurisdiction of the State Commission

(i) Complaints where the value of the goods or services and compensation, if any, claimed exceeds rupees twenty lakhs but does not exceed rupees one crore.
(ii) (ii) Appeals against the orders of any District Forum within the State.

Appeals:

Any person aggrieved by an order made by the State Commission in exercise of its powers conferred by sub-clause (i) of clause (a) of section 17 may prefer an appeal against such order to the **National Commission** within a period of thirty days from the date of the order in such form and manner as may be prescribed.

13.5.3 NATIONAL COMMISSION

(a) A person who is or has been a Judge of the Supreme Court, to be appointed by the Central Government, who shall be its President;

(b) Not less than four, and not more than such number of members, as may be prescribed, and one of whom shall be a woman.

Jurisdiction of the National Commission:

Complaints where the value of the goods or services and compensation, if any

(i) Complaints where the value of the goods or services and compensation, if any exceed one crore.
(ii) (ii) Appeals against the orders of any State Commission

Appeal

Any person, aggrieved by an order made by the National Commission in exercise of its powers may prefer an appeal against such order to the Supreme Court within a period of thirty days from the date of the order.

Limitation period:

The District Forum, the State Commission or the National Commission shall not admit a complaint unless it is filed within two years from the date on which the cause of action has arisen.

CONSUMER DISPUTE REDRESSAL AGENCIES AND THEIR JURISDICTION

S.R.	COURT	PRESIDENT	OTHER MEMBERS	AMOUNT OF COMPENSATION

1.	District Consumer Disputes Redressal Forum	Must be Qualified to a Judge	Two Other Members. One must be a Women	Up to 20 Lakhs
2.	State Consumer Dispute Redressal Commission	Must be Person who is or has been a Judge of High Court	At least Two other members	20 Lakh to One Crore
3.	National Consumer Dispute Redressal Commission	Must be Person who is or has been a Judge of Supreme Court	At least four other members	More than One Crore

13.6 CONSUMER PROTECTION COUNCILS

Under Consumer Protection Act, 1986 below are the various authorities set up to resolve Consumer disputes.

CENTRAL CONSUMER PROTECTION COUNCIL

The Act provides for setting up a Central Consumer Protection Council by the Central Government and State Consumer Councils by each state of India. The Central Consumer Protection Council shall consist of (1) the Minister in Charge of Consumer Affairs in the Central Government who shall be its chairman and such number of other official or non-official members representing such interests as prescribed.

It is required by the Act that Central Consumer Protection Council will meet as and when necessary. However, at least one meeting of the Central Council must be held every year. The objects of the council are to protect the rights of consumers and promote their interest as listed under clauses (a) to (f).

SECTION 4: Central Consumer Protection Council:

(1) The Central Government shall, by notification, establish with effect from such date as it may specify in such notification, a Council to be known as the Central Consumer Protection Council (hereinafter referred to as the Central Council).

(2) The Central Council shall consist of the following members, namely:

(a) the Minister in charge of the [consumer affairs] in the Central Government, who shall be its Chairman, and

(b) such number of other official or non-official members representing such interests as may be prescribed.

SECTION5 - PROCEDURE FOR MEETINGS OF THE CENTRAL COUNCIL

(1) The Central Council shall meet as and when necessary, but [at least one meeting] of the Council shall be held every year.

(2) The Central Council shall meet at such time and place as the Chairman may think fit and shall observe such procedure in regard to the transaction of its business as may be prescribed.

SECTION6 - OBJECTS OF THE CENTRAL COUNCIL

The objects of the Central Council shall be to promote and protect the rights of the consumers such as,--

(a) the right to be protected against the marketing of goods1[and services] which are hazardous to life and property;

(b) the right to be informed about the quality, quantity, potency, purity, standard and price of goods1[or services, as the case may be] so as to protect the consumer against unfair trade practices;

(c) the right to be assured, wherever possible, access to a variety of goods1[and services] at competitive prices;

(d) the right to be heard and to be assured that consumer's interests will receive due consideration at appropriate fora;

(e) the right to seek redressal against unfair trade practices1for restrictive trade practices] or unscrupulous exploitation of consumers; and

(f) the right to consumer education.

STATE CONSUMER PROTECTION COUNCIL

Under Section 7 of Consumer Protection Act, 1986, District Consumer Protection Council shall consists of;

SECTION 7: STATE CONSUMER PROTECTION COUNCIL

(1) The State Government shall, by notification, establish with effect from such date as it may specify in such notification, a Council to be known as the Consumer Protection Council for State.

(2) The State Council shall consist of the following members, namely:--

(a) the Minister in-charge of consumer affairs in the State Government who shall be its Chairman;

(b) such number of other official or non-official members representing such interests as may be prescribed by the State Government.

(c) such number of other official or non-official members, not exceeding ten, as may be nominated by the Central Government.

(3) The State Council shall meet as and when necessary but not less than two meetings shall be held every year.

(4) The State Council shall meet at such time and place as the Chairman may think fit and shall observe such procedure in regard to the transaction of its business as may be prescribed by the State Government.

SECTION 8: The objects of every State Council shall be to promote and protect within the State the rights of the consumers laid down in clauses (a) to (f) of section 6.

DISTRICT CONSUMER PROTECTION COUNCIL

Under Section 8(a) of Consumer Protection Act, 1986, District Consumer Protection Council is established:

SECTION: 8 (a) **DISTRICT CONSUMER PROTECTION COUNCIL**

(1) The State Government shall establish for every district, by notification, a council to be known as the District Consumer Protection Council with effect from such date as it may specify in such notification.

(2) The District Consumer Protection Council (hereinafter referred to as the District Council) shall consist of the following members, namely:

> (a) the Collector of the district (by whatever name called), who shall be its Chairman; and
>
> (b) such number of other official and non-official members representing such interests as may be prescribed by the State Government.

(3) The District Council shall meet as and when necessary but not less than two meetings shall be held every year.

(4) The District Council shall meet as such time and place within the district as the Chairman may think fit and shall observe such procedure in regard to the transaction of its business as may be prescribed by the State Government.

SECTION 8 (b) OBJECTS OF THE DISTRICT COUNCIL

The objects of every District Council shall be to promote and protect within the district the rights of the consumers laid down in clauses (a) to (f) of section 6.]

13.7 SUMMARY:

The Consumer Protection Act, 1986 is quite a comprehensive legislation. Under this Act not only manufacturers and suppliers of goods but services such as insurance providers, medical treatment, lending and recovery of bank loans also come within the purview of this Act.

It is important to note that the Indian Consumer Protection Act is a social welfare legislation and has been designed to avoid technicalities, procedural delays, procedural requirement, court fees and costs.

Objective of this Act is to provide for better protection of the interests of consumers and for that purpose to make provisions for the establishment of Consumer Councils and other authorities for the settlement of consumer disputes and for matters connected therewith. It protects the consumers from unfair trading or unfair trade practices.

13.8 GLOSSARY

1. COMPLAINT: means any allegation in writing.

2. REDRESSAL: means settlement of any issue between parties.

13.9 SAQS

A. Short Answer Type Question:

(a) Define Consumer.

(b) What do you mean by Complaint?

(c) Define Goods.

B. Fill in the Blanks:

(a) As a.....this statute is for checking the unfair trade practices and 'defect in goods' and 'deficiencies in services'.
(b) Every member of the District Forum shall hold office for a term of..... or up to the age of ..... years, whichever is earlier.

C. True and False:
(a) Consumer means any person who buys any goods for a consideration.
(i) True (ii) False
(b) Objective of Consumer Protection Act is to provide better protection to the interests of consumers.
(i) True (ii) False

13.10 REFERENCES:

1. ncdrc.nic.in/bare_acts/Consumer%20Protection%20Act-1986.html
2. https://www.legalcrystal.com/act/51060/consumer-protection-act-1986-complete-act
3. http://www.economicsdiscussion.net/acts/consumer-protection-act-1986/highlights-on-the-consumer-protection-act-1986/11053
4. https://www.google.co.in/search?ei=FuMxXbDLGMnVvATjtYvIDA&q=consumer+protection+act+1986+b
5. https://www.slideshare.net/RITAKAKADE/consumer-protection-act-1986-79347961

13.11 SUGGESTED READINGS

(a) **Law of Sale of Goods Act** by Avtar Singh.
(b) **The Sale of Goods Act** by Pollock & Mulla

(c) **The Sale of Goods Act** by R.K. Bangia

13.12 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. What do you mean by 'consumer' with reference to Consumer Protection Act 1986? Explain its salient features of Consumer Protection Act?
2. Define the term services. Explain the deviancy in services.

Answers:

A. SAQs
(a) 13.3 (b) 13.3 (c) 13.3

B. **Fill in the Blanks**
(a) 13.4 (b) 13.5

C. True and False

(a) True (b) True