Unit 4: Facets of Cyber Crime: Offences, Penalties and Compensation

4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Doctrine of Actus Reus and Mens Rea in Cybercrimes

1.4 Facets of Cyber crime

1.5 Cyber Pornography

1.6 Test determining obscene content

1.7 Present scenario in India

1.8 Cyber Stalking

1.9 Legislative framework and position in India

1.10 Provisions under Indian Penal Code

1.11 Cyber Terrorism

1.12 Famous Incidents of Cyber Terrorism in the world

1.13 Legal provisions under the I.T. Act

1.14 Important provisions under the IT Act, 2000

1.15 Let's sum up

1.16 Further reading

1.17 Check your progress: Possible answers

1.18 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Doctrine of Actus Reus and Mens Rea in Cybercrimes

- Facets of Cyber Crime
- Legislative Framework and Position in India

1.2 INTRODUCTION

The rampant growth and development of Internet and Computer technology have paved the way to new forms of transnational crimes, especially Internet-based. The Indian Legislature does not provide the explicit definition of Cybercrime in any statute. In general, the term cybercrime means any kind of illicit activity which is carried out with the help of the internet or computers. It includes all unauthorized access of information and security breakage like privacy, password etc. with the aid of the Internet. On the whole, Cybercrime is an unlawful act wherein the computer is either used as a tool or a target or both.[43]

1.3 DOCTRINE OF ACTUS REUS AND MENS REA IN CYBERCRIMES

There are two essential elements which constitute a crime i.e., Actus Reus and Mens Rea.

- ***Actus Reus in Cyber Crimes***

  The word 'Actus' connotes a 'mental or spiritual act'. Actus Reus can be defined as "Such result of human conduct as the law seeks to prevent". Actus Reus in case of cybercrimes has become a challenging task as the entire act is committed in intangible surroundings. The element of actus reus is relatively easy to identify, but it is very difficult to prove. One must-see at what state of mind the wrongdoer has committed the crime and must be able to prove that the doer was well aware of the unauthorized access.

- ***Mens Rea in Cyber Crimes***

  Mens Rea is the second essential element in a crime and is known as 'guilty mind'. It refers to the mal-intent of the individual who commits the act. Mens rea in case of Cybercrimes

[43] Jain, Neelesh & Shrivastava, Vibhash & Professor, & Professor, Assistant (2014) "CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY" 4

encompasses two elements. Firstly, there must be an 'intent' to secure access to any kind of programme or data held in any computer, computer system or network. Secondly, the person committing such offence must have the knowledge that the access he intends to secure is unauthorized.[44]

1.4 FACES OF CYBERCRIME

- ***Hacking:*** Hacking means unauthorized access/control over a computer system or a computer network. An act of hacking completely destroys the data as well as computer programmes.
- ***E-mail Spoofing:*** A spoofed e-mail is one which misrepresents its origin i.e., it is an e-mail that appears to originate from one source while it actually has been sent from another source. In 2016, Flipkart's CEO Binny Bansal's email account was spoofed.
- ***Trojan Attacks:*** A Trojan is an unauthorized programme which passively gains control over another's system by representing itself as an authorized programme. The most common form of installing a Trojan is via e-mail.
- ***Salami attacks:*** This type of crime is normally prevalent in financial institutions in instances of financial crimes. It is also known as Salami Slicing wherein the attackers use an online database to seize the personal information of the customers such as bank details, credit card details etc. Later, the attackers keep deducting small amounts of money from every account over a stipulated period of time.[45]
- ***Data Diddling:*** Data diddling involves changing of data prior to or during input into a computer i.e., alteration of raw data before a computer processes it and then changing it back after the processing is completed. Section 66 and 43(d) of the I. T. Act, 2000 covers the offence of data diddling. The NDMC Electricity Billing Fraud Case[46] that took place in 1996 is a typical example. A private contractor was made to deal with receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized

[44] Etter, B (2001), The forensic challenges of E-Crime, Current Commentary No. 3 Australasian Centre for Policing Research, Adelaide
[45] Etter B (2002), The challenges of Policing Cyberspace, presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand
[46] 2003 IIAD Delhi 452

accounting, record maintenance and remittance in his bank was misappropriated by manipulating data files to show less receipt and bank remittance.

- ***Intellectual Property Crimes:*** Crimes pertaining to IPR includes software piracy, copyright infringement, trademark violations, theft of computer source code etc. One such crime is Domain Name violations and passing off. In Cardservice International Inc. Vs Mc Gee[47], it was held that the domain serves the same function as the trademark and is not a mere address or like finding the number on the Internet and, therefore, it is entitled to equal protection as a trademark. It was further held that a domain name is more than a mere Internet address for it also helps identify the Internet site for those who reach it, much like a person's name identifies a particular person.
- ***Phishing and Vishing:*** Phishing means the acquisition of information such as usernames, passwords, credit card details etc. by electronic communication. The information is acquired by using fake emails or fake messages which contain link of virus / malware infected fake websites. This kind of websites request the users to enter all their personal details. On the other hand, Vishing is typically used to steal credit card numbers or other kind of information from the users for use in instances of identity theft.[48]

1.5 CYBER PORNOGRAPHY

The word 'Pornography' has no specific definition in the eyes of law as every country has its own customs and traditions. Cyber Pornography can be defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials The act pornography is made legal in some countries but in others, it is illegal and banned. The Indian legal system has been structured in such a way that it contains provisions to criminalize any kind of scatological content.[49] Legalization of Child Pornography doesn't come under the purview of

[47] *Cardservice International Inc v Mc Gee*, 42 USPQ 2d 1850

[48] Eric J Sinrod and William P Reilly, Cyber Crimes (2000), A Practical Approach to the Application of Federal Computer Crime Laws, Santa Clara University, Vol 16, Number 2

[49] See e g The Post Office Act, 1893 (prohibits obscene matters being transmitted through post); The Sea Customs Act, 1878 (prohibits the import of obscene literature); The Dramatic Performances Act, 1876 (prohibits obscene plays); The Cinematograph Act, 1952 (makes provisions for censorship of films); The Press Act, 1951 (prohibits grossly indecent, scurrilous or obscene publications); The Indecent Representation of Women (Prohibition) Act, 1986 (prohibits obscene photographs of women)

pornography as a whole. Child Pornography at the very instance is a felonious act and is one of the heinous crimes that has eventually led to other severe crimes such as sex tourism, sexual abuse of child etc. The obscene contents involving children creates a major threat to the development and security of children which initiates a path for sexual abuse of children. The concepts of obscenity and pornography oscillate from time to time and from country to country. Although the terms obscenity and pornography are different, they are related to each other.

1.6 TEST DETERMING OBSCENE CONTENT

The test of obscenity was first laid down in ***Regina Vs Hicklin***[50] ***(also known as Hicklin's test*** i.e., a content is obscene if "the tendency of the matter charged with obscenity is to deprave and corrupt those whose minds are open to such immoral influences and whose hands a publication may fall". This approach was later adopted even in India in the case of ***Ranjit Singh Udeshi Vs State of Maharashtra***[51] with regards to a sale of an allegedly obscene magazine.

After the Hicklin's Test, the U.S Supreme Court went against the said rule and established a new set of principles called as the ***Community Standards Test*** **in** ***Roth Vs. United States***[52] and held that "obscene material was not protected by the First Amendment and could be regulated by the States rather than by a singular, Federal standard and also a new judicial standard for defining obscenity that invoked the average person's application of contemporary community standards to judge whether or not the dominant theme of the material taken as a whole appeals to prurient interest". Furthermore, the Supreme Court held that in order to decide how obscenity derived, we need to consider the following five-part structure:-

- The perspective of evaluation is that of an ordinary, reasonable person.
- Community Standards of acceptability are used to measure obscenity.
- Obscenity law only applies to the works whose themes are in question.
- A work, in order to be evaluated for obscenity, has to be taken in its entirety.

[50] *Regina v Hicklin* [1868] LR 3 QB 360
[51] *Ranjit Singh Udeshi v State of Maharashtra* AIR [1965] SC 881
[52] *Community Standards Test* in *Roth v United States* [1957] 354 U S 476

- An obscene work is one that aims to excite individuals' prurient interest.

However, in ***Samresh Bose Vs Amal Mitra***[53]**,** the Supreme Court held that 'vulgar writing is not necessarily obscene'. Vulgarity arouses a feeling of disgust and revulsion and also boredom but does not have the effect of depraving, debasing and corrupting the morals of any reader of the novels; whereas obscenity has the tendency to deprave and corrupt those whose minds are open to such immoral influences. In the instant case, the court had differentiated between vulgarity and obscenity and further held that while judging the question of obscenity 'the Judge should place himself in the position of a reader of every age group in whose hands the book is likely to fall and should try to appreciate what kind of possible influence the book is likely to have in the minds of the readers'.

This Community Standards Test was also used in India in, ***K.A. Abbas Vs Union of India***[54] which stated that;

- The dominant theme taken as a whole, appeals to prurient interests according to the contemporary standards of the average man;
- The motion picture is not saved by any redeeming social value; and
- It is patently offensive because it is opposed to contemporary standards.

Later, the Millers Test was brought to light which was a developed form of Community Standards Test. The Millers Test took birth from the case of ***Miller Vs California***[55] wherein The Supreme Court of United States provided the basic guidelines and three-point tests to determine obscenity in the work. They are as follows:-

- That the average person, applying contemporary 'community standards', would find that the work, taken as a whole, appeals to the prurient interest.
- That the work depicts or describes, in an offensive way, sexual conduct or excretory functions, as specifically defined by applicable state law or applicable law.
- That the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

[53] *Samresh Bose v Amal Mitra* AIR [1986] SC 967
[54] *K.A. Abbas v Union of India* AIR [1971] SC 481
[55] *Miller v California* 413 US 15 [1973]

1.7 PRESENT SCENARIO IN INDIA

The Supreme Court of India presently adopts the *Community Standards Test* as a measure of detecting obscene content. In ***Aveek Sarkar V. State of West Bengal***[56]**,** the facts of the case revealed that a German magazine published an article about a tennis player picturing him naked with his fiancé as a stand against racism and to show that love champions over everything. The Supreme Court found the respondents innocent of the charges levied against them and held that in a situation like this Hicklin's test cannot be used and the only measure to be implemented is the community standards test; and it further stated that the photograph must be viewed in the context of the message which the photograph appears to convey, and not in isolation. The Supreme Court further instructed that a more adaptive community standards test must be applied for a continuously evolving society like India.

Under the ***Information Technology Act, 2000, Section 67*** of the Act states that publishing obscene content online is punishable with imprisonment of three years and a fine of rupees five lakhs; and subsequent conviction will lead to a punishment of imprisonment of five years and fine of ten lakh rupees. However, under the ***Information technology (Amendment) Act, 2008, section 67(A)*** it has been made clear that a publication of sexual content will lead to a punishment of five years' imprisonment on the first conviction with a fine of rupees ten lakh and a punishment of 7 years with a fine of rupees ten lakh on the subsequent conviction. ***Section 67(B)*** of the amendment which is against child pornography makes it clear that not only publication and viewing but also possession of such pornographic content is punishable with five years' imprisonment and ten lakh rupees on the first conviction and seven years' imprisonment and ten lakh rupees on the subsequent conviction.

1.8 CYBER STALKING

Cyber Stalking has been defined as a crime wherein the stalkers use the internet or any other electronic device to stalk someone. It is an advanced form of stalking which is committed over

[56] *Aveek Sarkar v State of West Bengal* [2014] 4 SCC 257

the online medium.[57] It involves a conduct of harassing or threatening an individual in order to gather information about the victim. Cyber Stalking can be conducted via email, internet and computer. The Internet provides an opportunity for the stalkers to keep a check on the activities of their victims and the risk factor is comparatively less compared to physical stalking as the identity of the stalker can be hidden.

1.9 LEGISLATIVE FRAMEWORK AND POSITION IN INDIA

Cyber Stalking gathered importance after the evolution of the internet. California was the first state to pass the anti-stalking law in 1990. The gravity of cyber stalking came into focus in India with the ***Manish Kathuria Case.*** This was first reported case cyber stalking case in India and it was the reason the provisions pertaining to cyber stalking were included in the Information Technology (Amendment) Act, 2008. The Delhi Police arrested Manish Kathuria for stalking a person called Ritu Kohli by illegally chatting with her name on 'www.mirc.com' website. As a result, the victim started receiving obscene calls from various parts of India and abroad. The matter was reported to the Delhi Police wherein a case registered under Section 509 of the Indian Penal Code for outraging the modesty of a women.[58] However, the said section does not cover cyber stalking. This case was an alarm to the Government and as a result ***Section 66A of the Information Technology (Amendment) Act, 2008 i.e., Punishment for sending offensive messages through communication service, etc.*** The offences like obscenity, defamation, bullying etc. came under the purview of the said section.

However, the aforesaid section was struck down in the year 2015 in the writ petition ***Shreya Singhal Vs Union of India[59].*** The Apex Court struck down Section 66A of Amendment Act, 2008 as it was misused by the authorities to the effect of violating ***Article 19(1) of the Constitution of India i.e., Freedom of Speech and Expression.***

---

[57] Kabay, M E (2000) Studies and Surveys of Computer Crime, Focus <http://securityportal.com/cover/coverstory2001211.html>

[58] Section 509 of IPC states that, Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both

[59] *Shreya Singhal v Union of India* WP (Crl) No 167 of 2012

At present, ***Section 72 and Section 72A*** of the Information Technology (Amendment) Act, 2008 regulate cyber stalking. Section 72 of the Act pertains to Penalty for breach of confidentiality and privacy and Section 72A of the Act deals with punishment for disclosure of information in breach of lawful contract.

1.10 PROVISIONS UNDER INDIAN PENAL CODE

There are no direct provisions that deal with the issue of cyber stalking. However, there are certain provisions under the Indian Penal Code that have some linkage with cyber stalking.

a) Section 354D defines 'Stalking'. It states that, any man who,

- 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 monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking.

b) Section 292 defines 'Obscenity'. It states that, the act of sending obscene materials to the victim on a social networking site or through emails or messages etc. or deprave the other person by sending any obscene material using the internet with the intention that the other person would read, see or hear the content of such material, shall amount to the offense under the said section being committed.

c) Section 507 relates to 'Criminal Intimidation by anonymous communication'. It states that, when the stalker tries to hide his identity so that the victim remains unaware of the source from where the threat comes, it amounts to an offence. This satisfies the very characteristic of cyberstalking i.e., anonymous identity. The stalker shall be guilty if he attempts to conceal his/her identity.

d) Section 354C defines 'Voyeurism'. It states that, any man who watches, or captures or disseminating the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator.[60]

[60] KPMG (2000) , E-Commerce and Cyber Crime: New Strategies for Managing the Risks of Exploitation, USA

1.11 CYBER TERRORISM

Cyber Terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored therein that are carried out to intimidate or coerce a country's government or citizens in furtherance of political or social objectives. It is a combination of cyberspace and terrorism. There isn't an appropriate definition for Cyber Terrorism which can be accepted worldwide. However, a universally acknowledged definition of Cyber Terrorism is 'A criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and / or disruption of services to create fear within a given population with a goal of influencing a government or population to conform to a particular political, social or ideological agenda'.[61]

1.12 FAMOUS INCIDENTS OF CYBER TERRORISM IN THE WORLD

- ***Attack on the Indian Parliament***

The Indian Parliament was attacked by a cyber-attack on 13th December, 2001. The attackers used new technology and committed forgery to fulfil their end. They forged the gate pass and for the attack they downloaded the official logo of Ministry of Home Affairs, other documents and the layout of the Parliament building. Police found a laptop from main accused Mohammed Afzal and Shaukat Hussain Guru. The Police officials established that they have accessed the internet through Pakistan based Internet Service Providers (ISP). Additionally, the Investigating officers found incoming and outgoing cell phone call numbers of deceased terrorists and a satellite connection with deceased terrorist's cell phone.[62]

- ***Yugoslavia Conflict***

[61] Russell G Smith, Peter Grabosky and Grgor Urbas, 0521840473 – Cyber Criminals on Trial, Cambridge University Press

[62] Sayantan Chakravarty, "Parliament attack well-planned operation of Pakistan-backed terror outfits, evidence shows", India Today, December 31st 2001

When NATO[63] air strikes hit the Former Republic of Yugoslavia in Kosovo and Serbia, NATO web servers were subjected to sustained attacks by hackers employed by the Yugoslav military. All NATO's 100 servers were subjected to 'ping saturation', Distributed Denial of Service (DDoS)[64] assaults and bombarded with thousands of e-mails, many containing viruses. The attacks on NATO servers coincided with numerous website defacements of the American military, government, and commercial sites by Serbian, Russian, and Chinese sympathizers of Yugoslavia. These attacks caused serious disruption of NATO communications infrastructures.

- ***Epsilon***

Epsilon was one of the costliest cyber-attacks in history. Epsilon was the world's largest provider of marketing and handling services to industry giants such as JP Morgan Chase, Best Buy, and other major financial service providers, retailers and other major companies in 2011. It had an estimated damage cost that ranged from $225 million to $4 billion dollars. Names and email addresses were stolen from Epsilon, the world's largest email marketing firm in 2011, which handled more than 40 billion emails every year, more than 2,000 brands worldwide including Marks and Spencer. The company faced a spear phishing attack, a sophisticated fraud which aims to gather user details by sending emails from a trusted company with many users, such as PayPal. So, in the attack, the hackers targeted the email addresses that they could use for their criminal activities, making the implications a lot greater than estimated.

- ***Sony PlayStation Network, Microsoft's Xbox Live Network Case***

In this case, the confidential data of the employees and their families were leaked in 2014. The company faced a huge loss in revenue due to the publication of employee information which included their salaries, social security numbers, and executive emails. Due to this, an attack was launched by the *'Lizard Squad'*, a cyber-terrorist against the Tor Project, a

[63] The North Atlantic Treaty Organization, also called the North Atlantic Alliance, is an intergovernmental military alliance based on the North Atlantic Treaty which was signed on 4 April 1949. The organization constitutes a system of collective defence whereby its member states agree to mutual defense in response to an attack by any external party

[64] One common form of DOS and DDOS attacks use a technique known as ping saturation. Ping is a simple Internet utility used to verify that a device is available at a given Internet address. Ping saturation occurs when ping is used in an attack to overwhelm a system. The intent in these types of attacks is to disrupt services on a network or system by flooding it with requests

network of virtual tunnels that allow people and groups to improve their privacy and security on the Internet and after that North Korea attacked the network infrastructure wherein the network had gone down for almost 10 hours.

1.13 LEGAL PROVISIONS UNDER THE I.T. ACT

A new ***Section 66F*** was inserted by the Information Technology (Amendment) Act, 2008. Prior to the aforementioned provision, there was no specific provision in the IT Act, 2000 that dealt specifically with Cyber Terrorism.

Section 66F relates to 'Punishment for cyber terrorism'.[65] It stated that,

Whoever, 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-

- denying or cause the denial of access to any person authorized to access computer resource; or
- attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
- 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

- knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer

[65] Section 66F, Information Technology (Amendment) Act, 2008

database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

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

1.14 IMPORTANT PROVISIONS UNDER THE I.T. ACT, 2000

SECTIONS	OFFENCES	PENALTIES
Section 65	**Tampering with computer source documents**	**Imprisonment up to 3 years or fine up to 2 lakh rupees or both.**
Section 66	**Hacking the computer system with intent or knowledge**	**Imprisonment up to 3 years or fine up to 2 lakh rupees or both.**
Section 66B	**Misappropriation of information stolen from computer or any other electronic gadget**	**Imprisonment up to 3 years or fine up to 1 lakh rupees or both.**
Section 66C	**Stealing someone's identity**	**Imprisonment up to 3 years or fine up to 1 lakh rupees**
Section 66D	**Accessing personal data of someone with the help of computer by concealing their identity**	**Imprisonment up to 3 years or fine up to 1 lakh rupees**

Section 66E	**Breach of Privacy**	**Imprisonment up to 3 years or fine up to 2 lakh rupees or both.**
Section 66F	**Cyber Terrorism**	**Imprisonment which may extend to imprisonment of life.**
Section 67	**Publication of obscene information in e-form**	**Imprisonment up to 5 years and fine up to 1 lakh rupees.**
Section 67A	**Publishing or circulating sex or pornographic information through electronic means**	**Imprisonment up to 7 years or fine up to 10 lakh rupees.**
Section 67B	**Publication or broadcast of such objectionable material from electronic means, in which children are shown in obscene mode**	**Imprisonment up to 5 years or fine up to 10 lakh rupees.**
Section 68	**Failing to comply with the directions of the controller**	**Imprisonment up to 3 years or fine up to 2 lakh rupees or both.**
Section 71	**Misrepresentation**	**Imprisonment up to 2 years or fine up to 1 lakh rupees or both.**
Section 72	**Breach of confidentiality and privacy**	**Imprisonment up to 2 years or fine up to 1 lakh rupees or both.**
Section 72A	**Disclosure of information**	**Imprisonment up to 3 years or fine up to 5**

	in breach of lawful contract	**lakh rupees or both.**
Section 73	**Publishing false digital signature certificate and false in certain particulars**	**Imprisonment up to 2 years or fine up to 1 lakh rupees or both.**
Section 74	**Publication for fraudulent purposes**	**Imprisonment up to 2 years or fine up to 1 lakh rupees or both.**

1.15 LET'S SUM UP

In this chapter, we have studied about the varied facets of cybercrimes along with the legislative framework and position in India. We have also seen the provisions under IPC with respect to Cybercrime offences. Finally, we have ended the discussion with the famous incidents of cyber terrorism in the world and the important provisions under I.T. Act, 2000.

1.16 FURTHER READING

- S.T. Viswanathan, *The Indian Cyber Laws with Cyber Glossary*, 2001, p. 81
- Rhiannon Williams, "The Biggest Ever Cyber Attacks and Security Breaches", The Telegraph, Available on http://www.telegraph.co.uk/technology/internet-security/10848707/The-biggestever-cyber-attacks-and-security breaches.html.
- See "Is Cyber-Terrorism the New Normal?" Available at http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/

1.17 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are cybercrimes?

Cybercrimes are illegal acts in which a computer is made a tool or object whereby the means or purpose of committing it involves influencing the function of a compute; or instances involving computer technology wherein unethical or unauthorized behaviour relating to the automatic transmission of data results in creating victims and perpetrators.

2. What are the various facets of cybercrime?

The various facets of cybercrime are as follows:

- Hacking
- Email spoofing
- Trojan attacks
- Salami attacks
- Data diddling
- Intellectual property related crimes
- Phishing and vishing

3. What is cyber pornography?

Cyber Pornography can be defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials.

4. What is cyber stalking?

Cyber Stalking is an advanced form of stalking committed over online medium and can be defined as a crime wherein the stalkers use the internet or any other electronic device to stalk someone.

5. What is cyber terrorism?

Cyber Terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored therein that are carried out to intimidate or coerce a country's government or citizens in furtherance of political or social objectives.

1.18 ACTIVITY

Infer the reason that Information Technology Act is a *'Cyber Crime Friendly Act'*. (1500-2000 words.