Y&A LEGAL
ADVOCATES
MUMBAI - DELHI
DUBAI - LONDON

LAW ON CYBER CRIME

INDEX

Research by: Adv. Neville Majra, Co- Founder & Senior Partner
Mentor : Adv. Yusuf Iqbal Yusuf, Founder & Managing Partner

CHAPTER 1: INTRODUCTION

The invention of Computer has made the life of human beings easier, it has been using for various purposes starting from the individual to large organizations across the globe. In simple words we can define computer as a machine that can stores and manipulate/process information or instruction that are instructed by the user. Most computer users are utilizing the computer for the erroneous purposes either for their personal benefits or for other's benefit since decades. This gave birth to "Cyber Crime". This had led to the engagement in activities which are illegal to the society. We can define Cyber Crime as the crimes committed using computers or computer network and are usually take place over the cyber space especially the Internet. Now comes the word "Cyber Law". It doesn't have a fixed definition, but in simple words we can define it as the law that governs the cyberspace. Cyber laws are the laws that govern cyber area. Cyber Crimes, digital and electronic signatures, data protections and privacies etc. are comprehended by the Cyber Law. The United Nation's General Assembly recommended the first IT Act of India which was based on the "United Nations Model Law on Electronic Commerce" (UNCITRAL) Model.

Research by: Adv. Neville Majra, Co- Founder & Senior Partner
Mentor : Adv. Yusuf Iqbal Yusuf, Founder & Managing Partner

© M/s Y & A LEGAL, ADVOCATES

CYBER CRIME AND CYBER LAW

We can define “Cyber Crime” as any malefactor or other offences where electronic communications or information systems, including any device or the Internet or both or more of them are involved.

We can define “Cyber law” as the legal issues that are related to utilization of communication technology, concretely "cyberspace", i.e. the Internet. It is an endeavor to integrate the challenges presented by human action on the Internet with legacy system of laws applicable to the physical world

Cyber Crime

In simple words we can describe “Cyber Crime” are the offences or crimes that takes place over electronic communications or information systems. These types of crimes are basically the illegal activities in which a computer and a network are involved. Due of the development of the internet, the volumes of the cybercrime activities have also increased because when committing a crime there is no longer a need for the physical presence of the criminal. Cybercrime is computer-oriented crime, which involves a computer and a network. Cybercrime can be defined as "

© M/s Y & A LEGAL, ADVOCATES

Offences that are committed against individuals or groups of individuals with the criminal motive to intentionally harm the reputation of the victim or cause physical / mental harm, or loss to the victim directly or indirectly, by the means of modern telecommunication networks such as Internet, mobile phones etc.

The unusual characteristic of cybercrime is that the victim and the offender may never come into direct contact. Cybercriminals often opt to operate from countries with nonexistent or weak cybercrime laws in order to reduce the chances of detection and prosecution.

Cyber Crime started during the period of 1960's in the form of Hacking. In the period of 1970's presence of computes introduced new crimes in the form of privacy violation, phone tapping, trespassing and distribution of illicit materials. Then, later in the period of 1980's electronic systems crime emerged in the form of software piracy, copyright violations and introduction of viruses. The extent of damage after 1980's increased due to the highly sophisticated electronic systems. These Cyber Crimes adversely impacted the Indian market, international market, Banking sector and other areas.

© M/s Y & A LEGAL, ADVOCATES

Chapter 2: Causes of Cyber Crime

Computers are exposed, therefore, the law is mandatory to protect and safeguard them against cybercrime or Cyber Crime. The reasons for the exposure of computers may as follows:

Competence to accumulate data: The computer has exclusive characteristic of storing data in a very comparatively small space this makes the user more comfortable to steal the data either physically or virtually through any electronic medium.

1. Unproblematic to Approach: The trouble encountered in guarding a computer system from unauthorized access is that there is every opportunity of breach due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

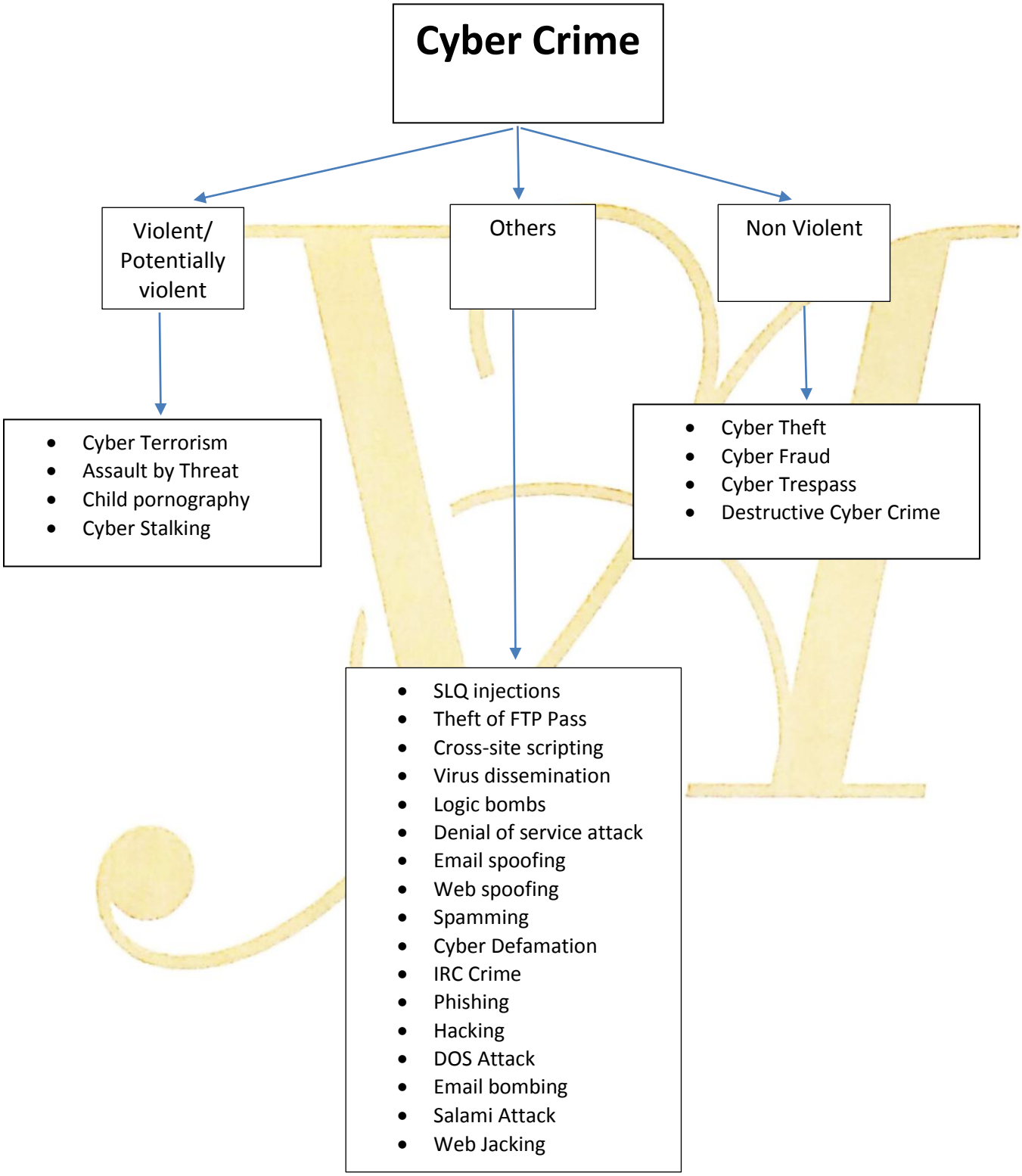
© M/s Y & A LEGAL, ADVOCATES

2. Complex: The computers effort on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

3. Negligence: Negligence is directly associated with human behaviour. While protecting the computer system it is possible there might be any negligence, which change direction provides of the cybercriminal to gain access and control over the computer system.

4. Loss of Proof: Loss of evidence facts & figures is a very common obvious problem as all the data are normally destroyed. This loss of evidences leads to paralyses of the entire computer system.

© M/s Y & A LEGAL, ADVOCATES



Research by: Adv. Neville Majra, Co- Founder & Senior Partner
Mentor : Adv. Yusuf Iqbal Yusuf, Founder & Managing Partner

© M/s Y & A LEGAL, ADVOCATES

Classification of cyber crimes

Cyber-crime is broadly divided into:

1) Violent / potentially violent cyber crimes

2) Non- violent cyber crimes

3) Other Cyber crimes

Crimes that leads to physical risks to the victim is known as Violent / Potentially violent cyber-crimes.

Violent / Potentially violent cyber-crimes can be further classified into:

1) **Cyber Terrorism** - The use of the internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. It is also sometimes considered an act of Internet terrorism where terrorist activities for large scale destruction take place. It can also be defined as the intentional use of computers, networks, and public internet to cause destruction and harm for personal objectives.

© M/s Y & A LEGAL, ADVOCATES

In simple words, when a terrorist group recruits' terrorists' / sleeper cells uses chain of communication like e-mails or any other medium of communication with the help of internet to plan a destruction to cause loss of life is called cyber terrorism.

2) **Assault by threat** - In this type, the victim is forced to comply with the demands of the accused. The victim is threatened by the accused by the means of e- communication. The victim could be an individual, organization, government body which can be threatened in the name of large scale destruction if they fail to comply with illegitimate demands of the accused.

3) **Child pornography** - Child pornography is taking pictures or videos, or more rarely sound recordings of children below 18 years of age who are wearing less clothing than usual, wearing no clothing or having any physical intimacy. Child pornography is sometimes called "child sexual abuse images" because it is images of a child who is being sexually abused.

4) **Cyber stalking** - The use of the Internet or any other electronic means to stalk or harass an individual, group or organization. This may include false

© M/s Y & A LEGAL, ADVOCATES

accusations, defamation, slander and libel. This may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass.

Non Violent cybercrimes can be further classified into:

1) **Cyber theft** - Cyber theft is a part of cybercrime which means theft carried out by means of computers or the Internet.

CYBER THEFT is further divided into:

a) **Piracy-** Piracy is one of the most common types of cybercrime. Any time a file is shared or downloaded illegally online, that's piracy. This involves various deceptive practices that companies or individuals engage in order to earn profit from online users. There are a variety of practices which may include cybersquatting, domain parking, and/or deceptive ad-word use.

© M/s Y & A LEGAL, ADVOCATES

b) **Plagiarism -** The act of taking the writings of another person and claiming them as one's own. It is an act of forgery, piracy, and fraud and is stated to be a serious crime of academia. It is also a violation of copyright laws.

c) **Unlawful appropriation** - Unlawful Appropriation is wherein an individual gains access from outside the organization to transfer funds and modify documents in such a manner that it gives him legitimate right to property which he doesn't own.

d) **DNS Cache poisoning** - A poisoning attack by which cyber criminals will try to insert corrupt data into the DNS cache. Cyber crooks will be able to redirect the victim's Internet traffic to malicious websites or servers under their control by which they can interrupt in communication without victim's knowledge.

e) **Identity Theft** - It is a crime whereby criminals impersonate individuals, usually for financial gain. This occurs when someone steals your digital identity by using scams like planting malicious software on your computer. In simple words, to steal someone's personal information and to act on his behalf which may cause wrongful loss to the victim

© M/s Y & A LEGAL, ADVOCATES

Financial identity theft is the most common identity theft. Some other types are: Medical identity theft, Criminal identity theft, Child identity theft, Identity Cloning & Concealment and Synthetic identity theft.

f) **Embezzlement** - It is a type of property theft. It occurs when someone who is entrusted to manage someone else's money or property steals all or part of that money or property for their own personal gain.

g) **Company espionage** - It is a form of cyber-attack that steals classified, sensitive data or intellectual property to gain advantage over a competitive company or government entity. It is the unlawful theft/acquisition of intellectual property, such as key trade secret and patent information as well as industrial manufacturing techniques and processes, ideas and formulas.

h) **Cyber vandalism** - It is a form of damage or destruction that takes place in digital form. Instead of keying someone's physical commodity, cyber vandals may deface a website and create malware that would damage electronic files or elements that interrupt its normal utilization or removal of a disk drive to disable

© M/s Y & A LEGAL, ADVOCATES

a computer system. Vandalism is the purposeful and malicious destruction of property by someone who does not own the property. It is sometimes referred to as malicious mischief or malicious trespassing.

2) **Cyber fraud** - Cyber fraud is the act of using a computer to take or alter electronic data, or to gain unlawful use of a computer or system. In this type of crime the victim normally is trapped and pays certain amount and later understands that he was cheated or fooled.

3) **Cyber trespass -** In common language the word 'trespass', means to go on another's property without consent. Cyber trespass is defined as accessing a computer or any other electronic device without any proper authorization and gaining financial / personal information, information from a department or agency from any protected electronic device.

4) **Destructive cybercrime** - A type of crime in which a criminal hacks the electronic device of the victim with mainly two purposes i) to delete all the valuable information / data to cause trouble; ii) in order to interrupt the working by

© M/s Y & A LEGAL, ADVOCATES

installing foreign programs or viruses. The criminal has no intension to misuse the information / data for any personal gains.

3) Other cyber crimes

a) SLQ Injections: An SLQ Injection is a technique that allows hackers to play upon the security and vulnerabilities of the software that runs a web site. It can be used to attack any type of unprotected or improperly protected SQL database. This process involves entering portions of SQL code into a web form and most commonly attacks the usernames and passwords. This would give the hacker further access to user's account.

b) Theft of FTP passwords: This is a very common way to tamper with the web sites. FTP password hacking takes advantage of the fact that many webmasters store their website login details on their poorly protected electronic devices. The thief then searches for the victim's system for FTP login details, and then relays them to his remote computer. This gives the thief access to the website via the poorly protected electronic device and the hacker can now modify the web pages.

© M/s Y & A LEGAL, ADVOCATES

c) Cross - site scripting - In this, the hacker infects a web page with a malicious client- side script or program. When the user visits the web page, the script is automatically downloaded to the browser and is executed typically by HTML, JavaScript, etc. to deceive and gather confidential information of the user.

d) Virus dissemination - Viruses are computer programs that attach themselves to infect a system or file and have a tendency to circulate to other computers and networks. These viruses disrupt the electronic device and its operation by affecting the data stored in it by either modifying it or deleting it altogether.

e) Logic bombs - Logic bombs are also known as "slag code", it is a malicious piece of code these are intentionally inserted into the software to execute a task when triggered by a specific event. Logic bombs are not viruses but they behave in a similar manner. The payload of a logic bomb is unknown to the user of the software, and the task that is executed is unwanted. Program codes that are scheduled to execute a particular time are known as time bombs.

f) Denial-of-Service attack - Denial of service attack is an attempt by the attackers to deny service to intended users of that service. This involves flooding an

© M/s Y & A LEGAL, ADVOCATES

electronic device with more requests than it can handle which results in server overload. This causes crash or slow down significantly so no one can access it. Using this technique, the attacker can render a website by sending massive amounts of traffic to the targeted site. This could temporarily malfunction or crash completely and would result in inability of the system to communicate adequately. Another variation to denial - of- service attack is known as "Distributed Denial of Service" attack wherein a number of geographically widespread perpetrators flood the network to cause traffic.

g) Email spoofing - This technique is a forgery of an email header. This means that the message appears to have received from someone or somewhere other than the genuine or actual source. These tactics are usually used in spam campaigns or in phishing, because people are probably going to open an electronic mail or an email when they think that the email has been sent by a legitimate source.

h) Website spoofing - Here a fresh fabricated site is prepared which looks valid to the user and customers are asked to give their card number PIN and other information, which are used to reproduce the card for use at an ATM.

© M/s Y & A LEGAL, ADVOCATES

i) Spamming - Email spam which is otherwise called as junk email. It is unsought mass message sent through email. The uses of spam have become popular in the mid1990s and it is a problem faced by most email users now a days. Recipient's email addresses are obtained by spam bots, which are automated programs that crawls the internet in search of email addresses. The spammers use spam bots to create email distribution lists. With the expectation of receiving a few number of respond a spammer typically sends an email to millions of email addresses.

j) Cyber defamation - Cyber defamation means the harm that is brought on the reputation of an individual in the eyes of other individual through the cyber space. The purpose of making defamatory statement is to bring down the reputation of the individual.

k) IRC Crime (Internet Relay Chat) - IRC servers allow the people around the world to come together under a single platform which is sometime called as rooms and they chat to each other. Cyber Criminals basically uses it for meeting. Hackers uses it for discussing their techniques. Pedophiles use it to allure small children.

© M/s Y & A LEGAL, ADVOCATES

l) Phishing - Some other cybercrimes against individuals includes- Net extortion, Hacking, Indecent exposure, Trafficking, Distribution, Posting, Credit Card, Malicious code etc. The potential harm of such a malefaction to an individual person can scarcely be bigger.

m) Hacking - A hacker is an unauthorized user who attempts to or gains access to an information system. Hacking is a crime even if there is no visible damage to the system, since it is an invasion in to the privacy of data. There are different classes of Hackers.

i) White Hat Hackers – They believe that information sharing is good, and that it is their duty to share their expertise by facilitating access to information. However there are some white hat hackers who are just "joy riding" on computer systems.

ii) Black Hat Hackers – They cause damage after intrusion. They may steal or modify data or insert viruses or worms which damage the system.

iii) Grey Hat Hackers – Typically ethical but occasionally violates hacker ethics Hackers will hack into networks, stand-alone computers and software.

© M/s Y & A LEGAL, ADVOCATES

Network hackers try to gain unauthorized access to private computer networks just for challenge, curiosity, and distribution of information. Crackers perform unauthorized intrusion with damage like stealing or changing of information.

n) DOS Attack - In this attack, the attacker floods the servers, systems or networks with traffic in order to overwhelm the victim resources and make it infeasible or difficult for the users to use them.

o) Email bombing - It is a type of Net Abuse, where huge numbers of emails are sent to an email address in order to overflow or flood the mailbox with mails or to flood the server where the email address is.

p) Salami attack - The other name of Salami attack is Salami slicing. In this attack, the attackers use an online database in order to seize the customer's information like bank details, credit card details etc. Attacker deduces very little amounts from every account over a period of time. In this attack, no complaint is file and the hackers remain free from detection as the clients remain unaware of the slicing. Some other cybercrimes against organization includes- Logical bomb, Torjan horse, Data diddling etc.

© M/s Y & A LEGAL, ADVOCATES

q) Web Jacking - The term Web jacking has been derived from hi jacking. In this offence the attacker creates a fake website and when the victim opens the link a new page appears with the message and they need to click another link. If the victim clicks the link that looks real he will have redirected to a fake page. These types of attacks are done to get entrance or to get access and controls.

© M/s Y & A LEGAL, ADVOCATES

Chapter 5: INFORMATION TECHNOLOGY ACT, 2000

Cybercrime is fast becoming a popular way of defrauding both individuals and entities. New communication systems and digital technology has made dramatic changes in the way people transact business. Businesses are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. Trade through the medium of e-commerce has also growing rapidly in the past few years. The business or individual with an online presence are prone to cybercrime.

The growing incidence of cybercrime has led the legislature to criminalize several acts which can be termed as cybercrime. In cybercrimes computer or a computer network is used either as a tool or as a target of the crime. Typical cybercrimes committed in the arena of white collar crimes are getting unauthorized access to computer, stealing sensitive information, disrupting vital operations and critical functions. The crimes committed under cyber fraud are dealt under the Indian Penal Code, 1860 and the Information Technology Act, 2000.

The Information Technology Act, 2000 was notified on 17 October in the year 2000. It is the primary law in India which deals with laws related to

© M/s Y & A LEGAL, ADVOCATES

cybercrime and electronic commerce. It is based on the UNCITRAL Model Law on International Commercial Arbitration recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.

The original Act contained 94 sections which were divided into 13 chapters and 4 schedules. These laws are applied to the whole of India. If a crime involves a computer or network located in India, persons of other nationalities can also be indicted under this law.

This Act provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures. It also defines cybercrimes and prescribes penalties for such crimes. The Act directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures. It has also established a Cyber Appellate Tribunal to resolve disputes. This Act has also amended various sections of the Indian Penal Code,1860, The Indian Evidence Act, 1872, The Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934 to make them compliant with new technologies.

© M/s Y & A LEGAL, ADVOCATES

Section 65 of The Information technology Act, 2000 - Tampering with computer source documents.

According to this if a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or a computer network, when the computer source code is required to be kept or maintained by law for the time being in force.

Penalty: Imprisonment up to three years, or / and with fine up to Rs. 2, 00,000

Section 66 of The Information technology Act, 2000 - Hacking with Computer system.

According to this if a person with the intent to cause or knowingly that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.

Penalty: Imprisonment up to three years, or / and with fine up to Rs. 5,00,000/-

© M/s Y & A LEGAL, ADVOCATES

Section 66A of The Information technology Act, 2000 - Publishing offensive, false or threatening information.

According to this any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable.

Penalty: Imprisonment up to three years and with fine.

Section 66B of The Information technology Act, 2000 - Receiving stolen computer or any communication device.

According to this when a person receives or retains a computer resource or any other communication device which is known to be stolen or the person has reason to believe is stolen.

Penalty: Imprisonment up to three years, or / and with fine up to Rs. 1, 00,000/-.

Section 66C of The Information technology Act, 2000 - Using password of another person. **(IDENTITY THEFT)**

According to this when a person fraudulently uses the password, digital signature or other unique identification of another person.

© M/s Y & A LEGAL, ADVOCATES

Penalty: Imprisonment up to three years, or / and with fine up to Rs. 1, 00,000/-.

Section 66D of The Information technology Act, 2000 - Cheating using computer resource.

According to this if a person cheats someone using a computer resource or any other communication device.

Penalty: Imprisonment up to three years, or / and with fine up to Rs. 1, 00,000/-.

Section 66E of The Information technology Act, 2000 - Publishing private images of others.

According to this when a person captures, transmits or publishes private images of a person without his/her consent or knowledge.

Penalty: Imprisonment up to three years, or / and with fine up to Rs. 2, 00,000/-.

Section 66F of The Information technology Act, 2000 - Acts of cyber terrorism

According to this if a person denies to an authorized personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyber terrorism.

© M/s Y & A LEGAL, ADVOCATES

Penalty: Imprisonment up to life.

Section 67 of The Information technology Act, 2000 - Publishing information which is obscene in electronic form.

According to this if a person punishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

Penalty: Imprisonment up to five years, or/ and with fine up to Rs. 10, 00,000/-.

Section 67A of The Information technology Act, 2000 - Publishing images containing sexual acts.

According to this if a person publishes or transmits images containing a sexual explicit act or conduct.

Penalty: Imprisonment up to seven years, or/and with fine up to Rs.10, 00,000/-.

Section 67B of The Information technology Act, 2000 - Publishing child porn or predating children online.

© M/s Y & A LEGAL, ADVOCATES

According to this is a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18 years of age.

Penalty: Imprisonment up to five years, or/and with fine up to Rs.10, 00,000/- on first conviction.

Imprisonment up to seven years, or/and fine up to Rs.10, 00,000/- on second conviction.

Section 67C of The Information technology Act, 2000 - Failure to maintain records.

According to this Persons deemed intermediately (such as an ISP) must maintain required records for stipulated time. Failure is an offence.

Penalty: Imprisonment up to three years, or/and with fine.

Section 68 of The Information technology Act, 2000 - Failure/ refusal to comply with orders.

According to this the controller may, by order, a direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such

© M/s Y & A LEGAL, ADVOCATES

activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under. Any person who fails to comply with any such order shall be guilty of an offence.

Penalty: Imprisonment up to 2 years, or/and with fine up to Rs. 1, 00,000/-.

Section 69 of The Information technology Act, 2000 - Failure/ refusal to decrypt data.

According to this if the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.

Penalty: Imprisonment up to seven years and possible fine.

© M/s Y & A LEGAL, ADVOCATES

Section 70 of The Information technology Act, 2000 - Securing access or attempting to secure access to a protected system.

According to this 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 protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.

Penalty: Imprisonment up to ten years, or/and with fine.

Section 71 of The Information technology Act, 2000 - Misrepresentation

According to this if anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining license or Digital Signature Certificate.

Penalty: Imprisonment up to two years, or/and with fine up to Rs.1, 00,000/-

© M/s Y & A LEGAL, ADVOCATES

Chapter 6: PROCESS OF FILING A CYBER CRIME COMPLAINT

Step-1

The very first step to file a cybercrime complaint is to register a written complaint with the cybercrime cell of the city you are currently in. Furthermore, to quote according to the IT Act, a cybercrime comes under the purview of global jurisdiction. This means that a cybercrime complaint can be registered with any of the cyber cells in India, irrespective of the place where it was originally committed.

Step 2

When filing the cybercrime complaint, you need to provide your name, contact details, and address for mailing. Moreover, the complaint needed to be written to the Head of the Cyber Crime Cell of the city where you are filing the cybercrime complaint.

Step 3

Sometimes, there might be circumstances where you may not find the cyber-cell or certain cyber-crimes are within the purview of Indian Penal Code 1860, or it is not

© M/s Y & A LEGAL, ADVOCATES

within your reach and the matter is of urgent nature, then you can file a First Information Report (FIR) at the local police station.

Online complaint filing Mechanism

There are initiatives taken by some of the State's cyber cell police stations by providing an online platform to the victims of cybercrimes to file a complaint even though from remote places and never bothering themselves, physically. (www.cybercrime.gov.in)

The documents which are required to be submitted with the complaints referring to various cyber-crimes are hereby provided:

For Email Based Complaints

- A written brief about the offence
- A copy of the suspected email as received by the original receiver (forwarded emails should be avoided)
- The complete header of the suspected email
- Hard and soft copies of the alleged email and its header

© M/s Y & A LEGAL, ADVOCATES

- Ensure that the soft copy is provided in a CD-R

For Social Media Based Complaints

- A copy or screenshot showing the alleged profile/content
- A screenshot of the URL of the alleged content
- Hard and soft copies of the alleged content
- Ensure that the soft copy is provided in a CD-R

For Mobile Application Based Complaints

- A screenshot of the alleged application and the location from where it was downloaded
- The victim's bank statements in case any transactions were made after the incident
- Soft copies of all the aforesaid documents

For Business Email Based Complaints

- A written brief about the offence
- Originating name and location
- Originating bank name and account number

© M/s Y & A LEGAL, ADVOCATES

- Recipient's name (as in bank records)
- Recipient's bank account number
- Recipient's bank location (not mandatory)
- Date and amount of transaction
- SWIFT number

For Data Theft Complaints

- A copy of the stolen data
- The copyright certificate of the allegedly stolen data
- Details of the suspected employee(s)

The following documents are required in relation to the suspected employee(s):

1. Letter of Appointment
2. Non-disclosure Agreement
3. Assigned list of duty
4. List of clients that the suspect handles

- The proof of breach of your copyright data
- Devices used by the accused during his/her term of service (only if available)

© M/s Y & A LEGAL, ADVOCATES

For Ransom ware/Malware Complaints

- The email ID, phone number or evidence of any other means of communication through which the demand for ransom was made
- In case the malware was sent as an email attachment, screenshots of the email with the complete header of the first receiver

For Internet Banking/Online Transactions/Lottery Scam/Fake Call Related Complaints

- Bank statements of the concerned bank for the last six months
- A copy of the SMSs received related to the suspected transactions
- Copy of the victim's ID and address proof as in bank records

For Bitcoin Based Complaints

- A written brief about the offence
- The address of the bitcoin
- The amount of bitcoin in question
- The address from/to whom the purchase/sale of the bitcoins have been done

© M/s Y & A LEGAL, ADVOCATES

For Online Cheating Complaints

- A print out of the alleged email with its complete header as received by the original receiver (forwarded emails should be avoided)
- Victim's bank statement
- Details of the suspected transactions
- Soft copies of all the aforesaid documents

© M/s Y & A LEGAL, ADVOCATES

Chapter 7: NEED FOR CYBER LAW

As the cases of cybercrime grow; there is a growing need to prevent them. Cyberspace belongs to everyone. There should be electronic surveillance which means investigators tracking down hackers often want to monitor a cracker as he breaks into a victim's computer system. The two basic laws governing real-time electronic surveillance in other criminal investigations also apply in this context, search warrants which means that search warrants may be obtained to gain access to the premises where the cracker is believed to have evidence of the crime. Such evidence would include the computer used to commit the crime, as well as the software used to gain unauthorized access and other evidence of the crime.

Researchers must explore the problems in greater detail to learn the origins, methods, and motivations of this growing criminal group. Decision-makers in business, government, and law enforcement must react to this emerging body of knowledge. They must develop policies, methods, and regulations to detect incursions, investigate and prosecute the perpetrators, and prevent future crimes. In addition, Police Departments should immediately take steps to protect their own information systems from intrusions (Any entry into an area not previously

© M/s Y & A LEGAL, ADVOCATES

occupied).Internet provides anonymity: This is one of the reasons why criminals try to get away easily when caught and also give them a chance to commit the crime again. Therefore, we users should be careful. We should not disclose any personal information on the internet or use credit cards and if we find anything suspicious in e-mails or if the system is hacked, it should be immediately reported to the Police officials who investigate cyber-crimes rather than trying to fix the problem by ourselves.

Computer crime is a multi-billion dollar problem. Law enforcement must seek ways to keep the drawbacks from overshadowing the great promise of the computer age. Cybercrime is a menace that has to be tackled effectively not only by the official but also by the users by co-operating with the law. The founding fathers of internet wanted it to be a boon to the whole world and it is upon us to keep this tool of modernization as a boon and not make it a bane to the society.

There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are as follows:

© M/s Y & A LEGAL, ADVOCATES

1. Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.

2. Cyberspace has complete disrespect for jurisdictional boundaries. A person in India could break into a bank's electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.

3. Cyberspace handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.

4. Cyberspace is absolutely open to participation by all. A ten year-old in Bhutan can have a live chat session with an eight year-old in Bali without any regard for the distance or the anonymity between them.

© M/s Y & A LEGAL, ADVOCATES

5. Cyberspace offers enormous potential for anonymity to its members. Readily available encryption software and stenographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.

6. Cyberspace offers never seen before economic efficiency. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.

7. Electronic information has become the main object of cybercrime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds.

8. A software source code worth cores of rupees or a movie can be pirated across the globe within hours of their release.

© M/s Y & A LEGAL, ADVOCATES

9. Theft of corporeal information (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic records are copied quickly, inconspicuously and often via telecommunication facilities. Here the "original" information, so to say, remains in the "possession" of the "owner" and yet information gets stolen.

© M/s Y & A LEGAL, ADVOCATES

Chapter 8: SOME IMPORTANT CASE LAWS

1) The Bank NSP Case:

In this case a management trainee of a bank got engaged into a marriage. The couple used to exchange many emails using the company's computers. After some time they had broken up their marriage and the young lady created some fake email ids such as "*Indian bar associations*" and sent mails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a huge number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

2) Andhra Pradesh Tax Case

The owner of the plastics firm in Andhra Pradesh was arrested and cash of Rs. 22 Crore was recovered from his house by the Vigilance Department. They wanted evidence from him concerning the unaccounted cash. The suspected person submitted 6,000 vouchers to prove the legitimacy of trade, however when careful scrutiny the vouchers and contents of his computers it unconcealed that every one of them were made after the raids were conducted. It had been concealed that the suspect was running 5 businesses beneath the presence of 1 company and used fake

© M/s Y & A LEGAL, ADVOCATES

and computerized vouchers to show sales records and save tax. So the dubious techniques of the businessman from the state were exposed when officials of the department got hold of computers utilized by the suspected person.

3. Pune Citibank Emphasis Call Centre Fraud:

It is a case of sourcing engineering. USD $350000 from City bank accounts of four US customers were dishonestly transferred to bogus accounts in Pune, through internet. Some employees of a call centre gained the confidence of the US customers and obtained their PIN numbers under the guide of helping the customers out of difficult situations. Later they used these numbers to commit fraud. Highest security prevails in the call centres in India as they know that they will lose their business. The call centre employees are checked when they go in and out so they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers. All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals

© M/s Y & A LEGAL, ADVOCATES

were traced. Police has been able to prove the honesty of the call centre and has frozen the accounts where the money was transferred.

© M/s Y & A LEGAL, ADVOCATES

DISCLAIMER:

This information has been sourced from the following:

1) Cyber Crime Portal at https://cybercrime.gov.in/

2) https://en.wikipedia.org/wiki/Cybercrimehttps://www.youtube.com/watch?v=VIfXjWAYkt8

3) https://www.youtube.com/watch?v=VIfXjWAYkt8

4) https://books.google.co.in/books?id=53zCDwAAQBAJ&pg=PA510&lpg=PA510&dq=The+invention+of+Computer+has+made+the+life+of+human+beings+easier,+it+has+been+using+for+various+purposes+starting+from+the+individual+to+large+organizations+across+the+globe.&source=bl&ots=YxsxQfLRtT&sig=ACfU3U1qURxOJNqJQhiE7PzNcwNJ8nu3pA&hl=en&sa=X&ved=2ahUKEwiiwq-JgZ7qAhVDzzgGHfoyCvIQ6AEwAHoECAwQAQ#v=onepage&q=The%20invention%20of%20Computer%20has%20made%20the%20life%20of%20human%20beings%20easier%2C%20it%20has%20been%20using%20for%

© M/s Y & A LEGAL, ADVOCATES

20various%20purposes%20starting%20from%20the%20individual%20to%20large%20organizations%20across%20the%20globe.&f=false

5) https://en.wikipedia.org/wiki/Information_Technology_Act,_2000#:~:text=The%20Information%20Technology%20Act%2C%202000,with%20cybercrime%20and%20electronic%20commerce.

© M/s Y & A LEGAL, ADVOCATES