

CYBER CRIMES

*Author: Yashwanth A S, M.com, LLB from YI7J Cyber Security and Management Consultant
LLP*

Abstract

Crime in any form adversely affects all the members of the society. In developing economies, cyber-crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitization of economic activities. Thanks to the huge penetration of technology in almost all walks of society right from corporate governance and state administration, up to the lowest level of petty shop keepers computerizing their billing system, we find computers and other electronic devices pervading the human life. The penetration is so deep that man cannot spend a day without computers or a mobile.

Snatching some one's mobile will tantamount to dumping one in solitary confinement!

Cyber Crime is not defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define cyber-crime, we can say, it is just a combination of crime and computer. To put it in simple terms 'any offence or crime in which a computer is used is a cyber-crime.'

Introduction

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.

Cybercrime can be carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

Cybercrime involves one or both of the following:

- Criminal activity *targeting* computers using viruses and other types of malwares.
- Criminal activity *using* computers to commit other crimes.

An important aspect of cybercrime is its nonlocal character: actions can occur in jurisdictions separated by vast distances. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. For example, if a person accesses child pornography located on a computer in a country that does not ban child pornography, is that individual committing a crime in a nation where such materials are illegal?

Where exactly does cybercrime take place? Cyberspace is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified.

Generally, cybercrime is on the rise. According to Accenture's State of Cybersecurity Resilience 2021 report, security attacks increased 31% from 2020 to 2021. The number of attacks per company increased from 206 to 270 year on year. Attacks on companies affect

individuals too since many of them store sensitive data and personal information from customers.

The first question that any student of cyber law must ask is whether there is a need for a separate field of law to cover cyberspace. Isn't conventional law adequate to cover cyberspace? Let us consider cases where so-called conventional crimes are carried out using computers or the Internet as a tool. Consider cases of spread of pornographic material, criminal threats delivered via email, websites that defame someone or spread racial hatred etc. In all these cases, the computer is merely incidental to the crime.

Distributing pamphlets promoting racial enmity is in essence similar to putting up a website promoting such ill feelings. Of course, it can be argued that when technology is used to commit such crimes, the effect and spread of the crime increases enormously.

History of cyber law in India

The information Technology Act is an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce, adopted the Model Law on Electronic Commerce on International Trade Law. This resolution recommended, inter alia, that all states give favourable consideration to the said Model Law while revising enacting new law, so that uniformity may be observed in the laws, of the various cyber-nations, applicable to alternatives to paper-based methods of communication and storage of information. The Department of Electronics (DoE) in July 1998 drafted the bill.

However, it could only be introduced in the House on December 16, 1999 (after a gap of almost one and a half years) when the new IT Ministry was formed. It underwent substantial alteration, with the Commerce Ministry making suggestions related to e-commerce and matters pertaining to World Trade Organization (WTO) obligations. The Ministry of Law and Company Affairs then vetted this joint draft.

With the passage of time, as technology developed further and new methods of committing crime using Internet & computers surfaced, the need was felt to amend the IT Act, 2000 to insert new kinds of cyber offences and plug in other loopholes that posed hurdles in the effective enforcement of the IT Act, 2000.

This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several counts.

Information Technology Act, 2000

Information Technology Act, 2000 is India's mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format. This legislation has touched varied aspects pertaining to electronic authentication, digital (electronic) signatures, cybercrimes and liability of network service providers.

The Preamble to the Act states that it aims at providing 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 and aims at facilitating electronic filing of documents with the Government agencies.

This Act was amended by Information Technology Amendment Bill, 2008 which was passed in Lok Sabha on 22nd December, 2008 and in Rajya Sabha on 23rd December, 2008. It received the assent of the President on 5th February 2009 and was notified with effect from 27/10/2009

Definition of cybercrime

At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

- a. Cybercrime in a narrow sense (computer crime): Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.
- b. Cybercrime in a broader sense (computer-related crime): Any illegal behaviour committed by means of, or in relation to, a computer system or network, including

such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Cyber frauds in India

According to Norton Cybercrime Report 2012, 66% of Indian online adults have been a victim of cyber fraud in their lifetime. In the past 12 months, 56% of online adults in India have experienced cyber fraud. As per the report, at least 1,15,000 people fall prey to cyber fraud every day, while 80 per minute and more than one per second leading to a rise in the average direct financial cost per victim to around Rs. 10,500.

According to the survey, the cybercriminals have now shifted their focus to the increasingly popular social platforms. One in three adults online Indians (32%) have been either social or mobile cybercrime victims. While most internet users delete suspicious emails and are careful with their personal details online. However, 25% don't use complex passwords or change their passwords frequently and 38% do not check for the padlock symbol in the browser before entering sensitive personal information.

Types of cyber-crimes found in India are:

1. **Cyber Pornography:** This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc). (Delhi Public School case)
2. **Sale of Illegal Articles:** This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. E.g., many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.
3. **Online Gambling:** There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of hawala transactions and money laundering over the Internet have been reported. Whether these sites have any relationship with drug trafficking is yet to be explored. Recent Indian case about cyber lotto was very interesting.

A man called Kola Mohan invented the story of winning the Euro Lottery. He himself created a website and an email address on the Internet with the address 'eurolottery@usa.net.' Whenever accessed, the site would name him as the beneficiary of the 12.5 million pounds. After confirmation a Telugu newspaper published this as a news. He collected huge sums from the public as well as from some banks for mobilization of the deposits in foreign currency.

However, the fraud came to light when a cheque discounted by him with the Andhra Bank for Rs 1.73 million bounced. Mohan had pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland Bank, Sheffields, London stating that a term deposit of 12.5 million was held in his name.

4. **Intellectual Property Crimes:** These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc. In other words, this is also referred to as cybersquatting. Satyam Vs. Siffy is the most widely known case. Bharti Cellular Ltd. filed a case in the Delhi High Court that some cyber squatters had registered domain names such as barticellular.com and bhartimobile.com with Network solutions under different fictitious names. The court directed Network Solutions not to transfer the domain names in question to any third party and the matter is sub-judice. Similar issues had risen before various High Courts earlier. Yahoo had sued one Akash Arora for use of the domain name 'Yahooindia.Com' deceptively similar to its 'Yahoo.com'. As this case was governed by the Trade Marks Act, 1958, the additional defence taken against Yahoo's legal action for the interim order was that the Trade Marks Act was applicable only to goods.
5. **Email Spoofing:** A spoofed email is one that appears to originate from one source but actually has been sent from another source. E.g., Gauri has an e-mail address gauri@indiaforensic.com. Her enemy, Prasad spoofs her e-mail and sends obscene messages to all her acquaintances. Since the emails appear to have originated from Gauri, her friends could take offence and relationships could be spoiled for life.

Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

6. **Forgery:** Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Outside many colleges across India, one finds touts soliciting the sale of fake mark sheets or even certificates. These are made using computers, and high-quality scanners and printers. In fact, this has become a booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates. Some of the students are caught but this is very rare phenomenon.
7. **Cyber Defamation:** This occurs when defamation takes place with the help of computers and / or the Internet. E.g., someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

India's first case of cyber defamation was reported when a company's employee started sending derogatory, defamatory and obscene e-mails about its Managing Director. The emails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the company.

The company was able to identify the employee with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

8. **Cyber stalking:** The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the

victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

9. **Unauthorized access to computer systems or networks:** This activity is commonly referred to as hacking. The Indian law has, however, given a different connotation to the term hacking, so we will not use the term “unauthorized access” interchangeably with the term “hacking”. However, as per Indian law, unauthorized access does occur, if hacking has taken place. An active hackers’ group, led by one “Dr.Nuker”, who claims to be the founder of Pakistan Hackerz Club, reportedly hacked the websites of the Indian Parliament, Ahmedabad Telephone Exchange, Engineering Export Promotion Council, and United Nations (India)
10. **Theft of Computer System:** This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

Who commits cybercrimes?

- i. **Insiders** - Disgruntled employees and ex-employees, spouses, lovers
- ii. **Hackers** - Crack into networks with malicious intent
- iii. **Virus Writers** - Pose serious threats to networks and systems worldwide
- iv. **Foreign Intelligence** - Use cyber tools as part of their Services for espionage activities and can pose the biggest threat to the security of another country
- v. **Terrorists** - Use to formulate plans, to raise funds, propaganda

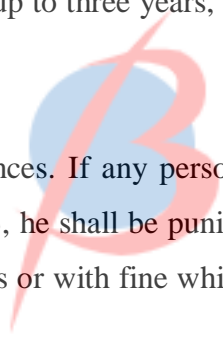
Penalties and offences under the IT Act, 2000

The Indian Law has not given any definition to the term ‘cybercrime or cyber frauds. In fact, the Indian Penal Code does not use the term ‘cybercrime’ at any point even after its amendment by the Information Technology Act 2000. Chapter XI of the Information Technology Act, 2000 deals with offences/crimes related to cyber space

In keeping with the demand of the times, the Cyber Crime Investigation Cell (CCIC) of the CBI, notified in September 1999, started functioning with effect from 3.3.2000. The Cell is

headed by a Superintendent of Police. The jurisdiction of this Cell is all India, and besides the offences punishable under Chapter XI, IT Act, 2000, it also has power to look into other high-tech crimes.

Offences under other legislations

- **Sec 65.** Tampering with computer source documents. Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
 - **Sec 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.
- 
BRILLOPEDIA
- **Sec 66A.** Punishment for sending offensive messages through communication service, etc. The Supreme Court of India in Shreya Singhal vs U.O.I on 24 March, 2015 declared "Section 66A of the Information Technology Act, 2000 is struck down in its entirety being violative of Article 19(1)(a) and not saved under Article 19(2)"
 - **Sec 66B.** Punishment for dishonestly receiving stolen computer resource or communication device. Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

- **Sec 66C.** Punishment for identity theft. Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

- **Sec 66D.** Punishment for cheating by personation by using computer resource. Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

- **Sec 66E.** Punishment for violation of privacy. Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

- **Sec66F.** Punishment for cyber terrorism. 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

- **Sec 67.** Punishment for publishing or transmitting obscene material in electronic form.: Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

What can be done when Cybercrime Happened?

Cybercrime complaint registration in the following ways:

- Online Cyber Crime complaint (National Cybercrime Reporting Portal),
- Offline Cyber Crime complaint (Cyber Crime Cell)
- FIR (Local Police station)
- Reporting online website for Cybercrimes: www.cybercrime.gov.in

Although a comprehensive regulatory framework with regard to laws governing the cyber space, particularly such acts is yet to be framed, there exists certain legal provisions under various Statutes which can come in aid of a person who is a victim of cyber violence.

Conclusion

During the period of the pandemic, many women and children have become the victim of various cybercrimes. The rate of cybercrime increased unbelievably during the lockdown in

India. A total number of 704 cybercrimes against women were registered in 2020 and 504 in 2021 (till July). The data provided above is evidence of the fact that the lockdown and pandemic frustration made the offenders commit such crimes aggressively.

The most common cybercrimes committed against women during the pandemic are Cyber Stalking, Sextortion, Cyber Hacking, Cyber Bullying, Sexual Abuse (including sexually explicit and pornographic content against the victim), Cybersex Trafficking, and Phishing. The most common cybercrimes committed against children during the pandemic are Sexual Abuse of Children, Cybersex Trafficking, Cyber Bullying, Child Grooming, etc. Women and children are the most vulnerable parts of society and hence, became easy targets of cybercrime offenders and sexual predators during the lockdown.

To fight these cybercrimes committed against women and children, the Indian legal system provides various laws. The first and the foremost step of a victim should be to register the cybercrime complaint in the nearest cybercrime cell or on the National Cybercrime Reporting portal, or in case of no access to any of these platforms the victim can register an FIR in the local police station.

The provisions of Information Technology Act, 2000, Indian Penal Code, 1860, Indecent Representation of Women (Prohibition) Act, 1986, and Protection of Children from Sexual Offences Act, 2012 prohibits the above-mentioned cybercrimes against women and children and also punishes the offender with strict punishments of imprisonment and fine.

Today, we can see e-commerce is becoming a part of study of almost all the courses in management and commerce. It is an integral part of any book or manuscript that is written on retailing, and it claims a significant share in this text also. The reason behind this lies in the fact that e-commerce technology is different and more powerful than any of the other technologies we have seen in the past century.

While these other technologies transformed economic life in the 20th century, the evolving Internet and other ITs will shape the 21st century in many ways. The foremost of these is the rise of a sizeable class of Internet-habituated consumers, and then is the creation of an ecosystem essential for e-tailing's growth. In India's case, both these factors are poised to fall into place rapidly.