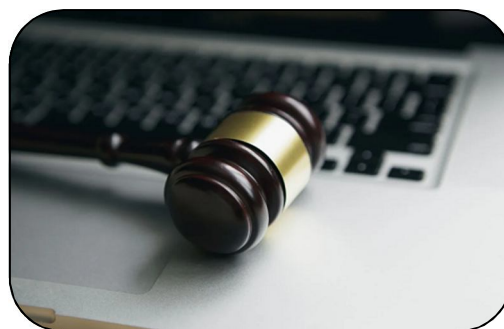




CYBER OFFENCES & PENALTIES UNDER THE INFORMATION TECHNOLOGY ACT, 2000

Dr. Priyam Sharma**Assistant Professor University Institute of Legal Studies,
Chaura Maidan, Shimla (H.P)****ABSTRACT**

The development of technology, software, social media, availability of the Internet and multi-media network helps the users in getting a fast and easier way to work; but the problem comes at the stage where either the users or some group of users do something intentionally against the other user or users, which results in the activation of their legal rights. Through this research paper, the author has brought the light on the study and empirical research of the concept of cyber offences; their meaning, concept, punishments, how to complain about them, preventive measures, steps taken by the Government and all the other necessary information regarding cyber offences and Information Technology Act of 2000. Violation of the laws and punishment for the different cyber offences has been defined through the Indian Penal Code 1860 and Information Technology Act 2000. The researcher has provided the complete detail of the role of the Government in controlling cybercrimes through policies, schemes, opening online portals for complaining, making people aware of them, etc. Along with the importance of the knowledge about cyber crimes and their punishment, the article is also based on the aftermath of cyber offence. In the instant research paper, the sources of knowledge include academic research, applied research, qualitative research, and case study research. The researcher studied the judgments of the High Courts and Supreme Court of India.



KEYWORDS: IT Act 2000 : Cyber, CrimesCyber, offences, cyberbullying, cyberstalking, phishing, ransomware, etc.

INTRODUCTION

Today in this fast moving and progressive world computer is an essential aspect of our everyday life. In order to improve and enhance its functionalities and features the introduction of internet has brought great changes in our lives. People from all walks of life ranging from corporates to businessmen or even households are now making use of the computers to create, transfer and store information in the electronic form rather than in the conventional paper or document form. Electronic storage of information has several benefits in that it is cheaper, easier to store, easy to retrieve, and fast connectivity. Nobody today can doubt the fact that computers and the Internet have made their lives so much easier and faster.

However, we cannot also doubt the fact that while it has many benefits, it has been abused by several people in order to serve their own selfish interests or otherwise cause harm to others. It is due to

the high and fast connectivity to the world from anywhere that several crimes have been committed which have necessitated legislation. However, there have been few nations which have taken an initiative in enacting certain laws for the Internet. In order to keep up with the changing generation, The Indian Parliament enacted the Information Technology Act 2000. The IT Act 2000 has been developed according to the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The rise in the rate of computer usage with the internet and the advancement in the changing technology in computers has been the reason for the enactment of the Information Technology Act 2000. The conversion of the paperwork into electronic records, storage of the electronic data, has changed the scenario of the country immensely. The Act further makes amendments in the Indian Penal Code, 1860, The Evidence Act, 1872, The Banker's Books Evidence Act, 1891 and The Reserve Bank of India Act, 1934.

CONCEPT:

Thus came the Information Technology Act, 2000 into effect as Act No.21 of 2000. The I. T. Act received assent of President on 9th June 2000 and came into force from 17th October 2000. India is the 12th nation in the world to adopt a Cyber law regime in 2000.

According to a report, the definition of cybercrime can be understood quite intelligently. Traditionally, theft is done when one enters other's house and steals things which are kept in the house. However, hacking is different. Hacking is done by sitting in one's own house using computer he/she hacks computer of other people and steals data saved in their computer without physically touching the computer or going in that house.¹

In Information Technology Act 2000, the terms 'access in a computer network' in section 2(a), 'computer' in section 2(i), 'computer network' in section (2j), 'data' in section 2(0) and 'information' in section 2(v). Moreover, the basic definition of a computer given in the act that it does not just include the computer or laptop that are in our homes but also every electronic, magnetic, optical or other high-speed data processing devise of a system which performs logical, arithmetic and memory function by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.

Reason behind increase of cyber crime :

Cyber-crimes are the most easy method of earning lots of money; always the targets are rich people, businesspeople, banks, and financial institutions which handle money in huge volumes. OS is used to run machines, and these OS consist of millions of lines of coding. Human mind is imperfect and hence errors are bound to happen. The criminals take advantage of this weakness of human mind.

One of the characteristics of human behavior is negligence. Hence there is a possibility that in protecting the computer systems from the attacks of cyber-criminals, we will commit an error that provides the criminals an opportunity to gain control over the computer systems. With the advent of the pandemic, everybody is working from their homes. Recently, many instances of phishing have been happening, taking advantage of the COVID situation.²

¹ Nikhil A. Gupta, Cybercrime and Information Technology Act 2000, An Overview, [http://mja.gov.in/Site/Upload/GR/Title%20NO.13\(As%20Per%20Workshop%20List%20title%20no13%20pdf\)](http://mja.gov.in/Site/Upload/GR/Title%20NO.13(As%20Per%20Workshop%20List%20title%20no13%20pdf))

² David Fouse- Cybercrime is on the Rise: How communications can help state and city governments. <https://www.forbes.com/sites/forbesagencycouncil/2020/06/29/cybercrime-is-on-the-risehow-communications-can-help-state-and-city-governments>

Classification of offences and their punishments:

1. Cyber Bullying- When one sends or publishes some form of negative or harmful, misleading or malicious content about someone else, it constitutes cyberbullying. This can involve embarrassing or humiliating another person based on the revelation of any information about them which should be kept private.

Bullying is prohibited by law in all the states and schools have a responsibility to deal with it. With the increase in cyberbullying cases due to the increasing usage of technology, most of the states have made changes in their laws to make provision for cyberbullying as an offence. Schools can either act according to the law or their own local or school policies to punish students.³

2. Cyber Stalking- Cyber stalking involves an offender who harasses his or her victim through e-mails or instant messages. Internet provides the opportunity for cyber stalker to torment the victim in anonymity. There are many organizations who are working hard for the solution of the cyber stalking problem. Cyber stalking differs from spam e-mails in the sense that cyber stalkers send offending mails to just one individual whereas spam senders send offensive mails to many people.⁴

3. Fraud on the job- The job fraud is an advanced kind of fraud that offers fake job prospects to those seeking jobs. This kind of fraud is usually carried out using online means such as fake websites or unsolicited emails that appear to come from well-known firms and brands. It has now become increasingly hard to tell whether a job offer is genuine or fake.

Never take advantage of any opportunity advertised on a search engine advertisement. You should always research before you start working on anything. Always verify the privacy policy of the firm. Always verify the government institution's website in relation to government job openings. Never pay for a job.⁵

4. Phishing- The scammers send you emails and messages with the intention of stealing your passwords, account numbers, and any other social security numbers.⁶

According to statistics released by the FBI's Internet Crime Complaint Center (IC3) in its 2019 Internet Crime Report, internet-enabled crimes and scams have been increasing. The calendar year prior to the center's establishment in May 2000 saw the highest complaint numbers and dollar losses ever recorded.

In 2019 IC3 had 467,361 complaints amounting to more than \$3.5 billion losses incurred by individual as well as corporate victims.⁷

5. Ransomware- Ransomware is malicious software which encodes the files of the victim. There are various methods in which a ransomware can infect a device. The method where the spam attachments are sent in emails which appear to be some trusted files for the victim is one of the most popular methods of delivery of ransomware. Once downloaded and opened they hijack the devices of the victim.

The second-most affected country by ransomware attacks after the United States is India, with 39 percent increase in the last three months. According to the report, there has been 50 percent rise in the daily average of ransomware attacks in the last three months when compared to the first half of 2020. Sri

³ Stop Bullying, what is Cyber bullying. <https://www.stopbullying.gov/cyberbullying/what-is-it>

⁴ TechTarget Contributor: Cyberstalking <https://searchsecurity.techtarget.com/definition/cyberstalking> Accessed

⁵ Ministry of Home Affairs, Is Your Job Offer Real or Fake? <https://cybercrime.gov.in/pdf/Job%20Fraud%20Brochure%20Final.pdf>

⁶ How to recognize and Avoid Phishing Scams, <https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

⁷ Internet Crime Reports Released, <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120>

Lanka, Russia and Turkey occupy third, fourth and fifth positions respectively in terms of top five most affected countries from ransomware attacks in the study period.⁸

There are several other forms of cybercrimes such as Man in the middle attack, SQL Injection, ESPIONAGE, Zero exploits, Cyber terrorism & cyber extortion, etc.

Study of cybercrimes:

There are many certain skills and scientific tools that cannot be done without for investigation purposes. There have been certain changes in the Criminal Procedure Code of 1973 and in the Evidence Act of 1872 in order to increase efficiency of the investigation.

According to section 78 of the IT Act, 'A police officer not below the rank of Inspector shall investigate any offence under this act'.

However, as the IT Act is not sufficient to address the need, there were certain changes made to the Criminal Procedure Code and the Indian Penal Code of 1860 where the issue of cyber-crime is concerned. This allows the Inspector to prosecute and register cyber-crime in the same way as any other crime.⁹

According to section 80 (2) of the IT Act, 'any person who is arrested under sub-section (1) by an officer other than a police officer then such officer shall, without any unreasonable delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station'. The Government of India had started an online cyber-crime reporting portal, www.cybercrime.gov.in, which is a citizen centric one, so that the complainants could register their complaints regarding any kind of sexually explicit content including those pertaining to child pornography or child sexual abuse material.¹⁰

Procedure:

Cyber complaints can be reported to the cyber crime cells. The report can be made both offline and online. This process has got global jurisdiction to lodge a cybercrime complaint; the cybercrime complaint can be lodged with any of the cybercrime cells in India. They have also raised awareness regarding the cybercrime and measures which could be adopted to avoid becoming a victim of cybercrime. Cyber crime cells monitor cyber crime alerts and do the investigation.

The documents needed for filing FIR on cybercrime depend upon the kind of cybercrime committed against the victim (Social Media Crime, Cyber Bullying, Mobile Application Crime, Cyber Extortion, etc.).

Writing a complaint letter to the cyber crime cell has been found to be an appropriate way of filing the complaint, as some people cannot afford internet charges or the expertise. A cybercrime victim can lodge his complaint in written form with the nearest cyber crime cell or any other cyber crime cell in India.¹¹

⁸ India becomes the second-most targeted country for ransomware after surge in attacks over the last three months <https://cio.economictimes.indiatimes.com/news/digital-security/india-becomes-the-second-most-targeted-country-for-ransomware-after-surge-in-attacks-over-the-last-three-months/78526531>

⁹ Ayush Verma, how is cyber-crime investigation conducted, 2020. <https://blog.ipleaders.in/cyber-crime-investigation-conducted>

¹⁰ Ministry of Home Affairs, Shri Amit Shah inaugurates Indian Cyber Crime Coordination Centre (I4C) in New Delhi; dedicates National Cyber Crime Reporting Portal to the Nation, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1599067>

¹¹ Meera Patel, Procedure for filing a cybercrime complaint in India. <https://blog.ipleaders.in/procedure-for-filing-cybercrime-complaint-in-india>

CONCLUSION:

Cyber-crime is not a novel topic; however, the impacts of the same are different due to changes in the pattern of occurrence of crime in the era of information technology, where there is a constant change in the laws. Law is an abstract phenomenon which is influenced by changes in society. As India is the world's second most populated nation followed by many internet users, it is prone to cyber crimes. Therefore, the problem of finding justice has become an urgent need. Thus, from the above discussion, it can be said that awareness among people should be raised, and there should be more strict laws. There must be a cybercrime cell in each district of the nation.

Moreover, it is expected that this paper will help the online media users get aware of crimes which may occur in the future. It is suggested by the author that the contribution of policymakers and administration has been adequate enough in resolving the issues related to crimes committed via online medium.