

**INTERNATIONAL JOURNAL OF LEGAL
SCIENCE AND INNOVATION**
[ISSN 2581-9453]

Volume 3 | Issue 3

2020

© 2021 *International Journal of Legal Science and Innovation*

Follow this and additional works at: <https://www.ijlsi.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com>)

This Article is brought to you for free and open access by the International Journal of Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in International Journal of Legal Science and Innovation after due review.

In case of **any suggestion or complaint**, please contact Gyan@vidhiaagaz.com.

To submit your Manuscript for Publication at **International Journal of Legal Science and Innovation**, kindly email your Manuscript at editor.ijlsi@gmail.com.

Cyber Offences under Information Technology Act: An analysis

HITESH JAIN¹ BHAVYA SHARMA² AND ANUSHKA JAISWAL³

ABSTRACT

The evolution of technologies, software, social media, easy access to the internet and multi-media networks facilitates the users in the easy and quick process to work; however, the problem arises at the point where users or a group of users malignly or knowingly maligns other user(s), leading in arousal of their legal rights. The author, via the instant research paper, highlighted the brief study and empirical research regarding the occurrence of cyber offences, meaning, concept, punishment, a procedure to file complaints, prevention, steps taken by the government, and all other necessary information related to the cyber offence and Information Technology Act of 2000.

Violating the laws and punishment for such various cyber offences is given under the Indian Penal Code 1860 and Information Technology Act 2000. The researcher also mentions a detailed study of the role of the Government in curbing cybercrimes by policies, schemes, launching online portals to smooth complaints, spreading awareness to the common man, etc.

The article, along with the importance of awareness about cybercrimes and legal penalties, is also centralised on the aftermath of the cyber offence. The researcher aims to put forth the complete legal process in filing and admissibility of such online evidence in law.

The instant research paper is based on academic research, applied research, qualitative research, also contains case study research, where the researcher briefed the study of the existing judgments of the High Courts and Supreme Court of India as may require.

Keywords: IT Act 2000, Cyber Crimes, Cyber offences, cyberbullying, cyberstalking, phishing, ransomware, etc.

¹ Author is a student at Indore Institute of Law, India.

² Author is a student at Indore Institute of Law, India.

³ Author is a student at Indore Institute of Law, India.

I. INTRODUCTION

The Internet has changed the lives of everyone. According to a report, the number of internet users in India increased by 47 million (+8.2%) between 2020 & 2021⁴. Using electronic form has its advantages, but dependence on IT and the internet for a fast solution has its side effects. If this has merits, then its dark side has misuse for the criminal activities.

Cybercrime is a very general term that includes all criminal involvements using the medium of internet, computer or cyberspace. Cybercrime is not explained anywhere; it is just an idiom of an offence related to the internet and Information technology. The Indian government has taken steps to spread awareness about cybercrimes, alerts/advisories, capacity building/training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensics facilities, etc., to prevent such crimes and speed up the investigation⁵.

Simply, all illegal acts where the computer is the target or used. There is no special law for cybercrime in India, but its punishments are defined in the Indian Penal Code 1872, Information Technology Act 2000, and some provisions overlap with each other.

In 2019, recorded a total of Rs. 1.25 Trillion loss because of cyberattacks, and according to National Cyber Security Coordinator Lt Gen (Dr) Rajesh Pant, the cyber threats will increase with the increase in the technology as a country is developing 5G, Smart cities and other initiatives.

Some of the offences defined under Information Technology Act 2000 are, [Tampering with the computer source documents, hacking with a computer system, Publishing of information which is obscene in electronic form, Directions of Controller to a subscriber to extend facilities to decrypt information, Penalty for misrepresentation, Penalty for breach of confidentiality and privacy, Penalty for publishing Digital Signature Certificate false in certain particulars Publication for a fraudulent purpose, Act to apply for offense or contravention committed outside India, Confiscation, Penalties or confiscation not to interfere with other punishments, Power to investigate offenses.]⁶

II. CYBER CRIME- CONCEPT

The Information Technology Act, 2000, was thus passed as Act No.21 of 2000. The I. T. Act

⁴ Simon Kemp, Digital 2021: India. <https://datareportal.com/reports/digital-2021-india>. Accessed on 6th May 2021.

⁵ Press Information Bureau Government of India, Ministry of Home Affairs: Steps taken to deal with Cybercrime and Cybersecurity. <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579226> Accessed on 6th May 2021.

⁶ THE INFORMATION TECHNOLOGY ACT, 2000, Chapter XI, Section 65 to Section 78. <https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf> Accessed on 6th May 2021 .

got President assent on 9th June 2000, and it was made effective from 17th October 2000. India is the 12th Nation in the world to adopt a Cyber Law regime during 2000.

In a report published, cybercrime is explained in a very perspicacious way, Traditionally the theft is when someone enters another's house and steal objects kept in the house, but hacking is something sitting in his own house, through his computer hacks the computer of others and steals the data saved in the computer without physically touching the computer or entering in that house⁷.

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.

III. REASON FOR THE INCREASING CASE OF CYBERCRIME?

Cybercrimes are the easiest way to make big money; always rich people, businessmen, banks, and financial firms where money is in bulk are targeted. Operating systems are used to operate machines, and these operating systems are made up of millions of lines of code. Since the human mind is flawed, errors will occur at any time. Cybercriminals exploit these flaws.

One of the features of human behaviour is negligence. As a result, there is a chance that in defending the computer system, we will make a mistake that gives cyber-criminals access to and control of the system. Due to the pandemic, almost everyone is now working from home. A slew of recent phishing attacks seemed to be targeting remote employees directly, taking advantage of the COVID-19 moment to rob, hack, and install malware⁸.

⁷ Nikhil A. Gupta, Cybercrime and Information Technology Act 2000, An Overview, [http://mja.gov.in/Site/Upload/GR/Title%20NO.13\(As%20Per%20Workshop%20List%20title%20no13%20pdf\).pdf](http://mja.gov.in/Site/Upload/GR/Title%20NO.13(As%20Per%20Workshop%20List%20title%20no13%20pdf).pdf) Accessed at 6th May 2021.

⁸ 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/?sh=3bc44d2e501e> Accessed at 7th May 2021

IV. TYPES OF CYBERCRIME AND ITS PUNISHMENT

1. Cyber Bullying- Sending, publishing, or sharing negative, damaging, misleading, or mean material about someone else is considered cyberbullying. It may involve embarrassment or humiliation caused by revealing personal or private information about another person.

Bullying is illegal in every state, and schools are required to respond to it. As the use of technology has increased the prevalence of cyberbullying, several states have amended their legislation to include or mention cyberbullying as a crime. Schools can act in accordance with the law or in accordance with local or school policies that allow them to discipline students or take other measures⁹.

2. Cyberstalking- Cyberstalking is when an attacker uses electronic correspondence, such as e-mail or instant messaging (IM), or comments posted to a Web site or discussion group, to annoy a victim. The anonymity provided by the Internet allows a cyberstalker to harass their victim without being discovered. Many organizations are working dedicated to the cyberstalking problem. Cyberstalking messages vary from regular spam in that a cyberstalker sends offensive messages to a single victim, while a spammer sends annoying messages to a large number of people. According to former U.S. Attorney General Janet Reno, cyberstalking is often "a prelude to more serious behaviour, including physical violence"¹⁰.

3. Online Job fraud- Job frauds are sophisticated fraud, offering fictitious job opportunities to job seekers. This type of fraud is normally done through online services such as bogus websites or through unsolicited emails claiming to be from known companies or brands. It has become difficult to determine whether a job offer is legitimate or fake.

Always avoid such opportunities offered on a search engine advertisement. Do always research before you start working on something. Always check the privacy policies of the company. Always check the website of a government organization for details about government job openings. Never pay for a job¹¹.

4. Phishing- Scammers send emails or messages with a trick to steal your password, account number, or any other social security number. According to data released by the FBI's

⁹ Stop Bullying, what is Cyber bullying. <https://www.stopbullying.gov/cyberbullying/what-is-it> Accessed at 7th May 2021

¹⁰ TechTarget Contributor: Cyberstalking <https://searchsecurity.techtarget.com/definition/cyberstalking> Accessed at 7th May 2021

¹¹ Ministry of Home Affairs, Is Your Job Offer Real or Fake? <https://cybercrime.gov.in/pdf/Job%20Fraud%20Brochure%20Final.pdf> Accessed at 7th May 2021

Internet Crime Complaint Center (IC3) in its 2019 Internet Crime Report, internet-enabled crimes and scams are on the rise. Since the centre's inception in May 2000, the previous calendar year saw both the highest number of complaints and the highest dollar losses recorded¹².

IC3 received 467,361 complaints in 2019—an average of nearly 1,300 every day—and recorded more than \$3.5 billion in losses to individual and business victims¹³.

5. Ransomware- Ransomware is a form of malware that encrypts a victim's files. There are many ways for ransomware to gain access to a device. Phishing spam attachments sent to the victim in an email that appears to be a file they should trust is one of the most common delivery systems. They will take over the victim's machine once they've been downloaded and opened.

India ranked second only to the United States among the countries most affected by ransomware attacks, with a 39 percent increase in the last three months. According to the report, the global daily average of ransomware attacks increased by 50% in the last three months compared to the first half of 2020. Sri Lanka, Russia and Turkey were ranked third, fourth and fifth, respectively, among the top five countries most impacted by ransomware attacks during the study period¹⁴.

There are several other offences such as Man in the middle attack, SQL Injection, ESPIONAGE, Zero exploits, Cyber terrorism & cyberextortion, etc.,

V. INVESTIGATION OF CYBERCRIMES

There are several certain skills and scientific tools without which investigation is not possible. Several amendments have been made in the Criminal Procedure Code 1973 and in Evidence Act 1872 to make the investigation more effective. 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, since the IT Act is insufficient to meet the need, the Criminal Procedure Code and the Indian Penal Code of 1860 were also revised to include cyber-crime in their scope. This

¹² How to recognize and Avoid Phishing Scams, <https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams> Accessed at 7th May 2021

¹³ 2019 Internet Crime Reports Released, <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120> Accessed at 7th May 2021

¹⁴ 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> Accessed at 7th May 2021

empowers the Inspector to register and prosecute cyber-crime in the same way as he or she does any other crime¹⁵.

Pursuant 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 launched the online cyber-crime reporting portal, www.cybercrime.gov.in, which is a citizen-centric initiative, to allow the complainants to lodge complaints relating to child pornography/child sexual abuse material or any content which is sexual in nature¹⁶.

VI. PROCEDURE FOR FILING CYBERCRIME COMPLAINTS

We can register cyber complaints with the cyber crime cells. It can be filed both in online and offline ways. It has a global jurisdiction to file a cybercrime complaint; the cybercrime complaint can be registered with any of the cybercrime cells established in India. These cells have also been raising awareness about cybercrime and the steps that can be taken to prevent being a victim. Cybercrime cells keep track of cybercrime alerts and conduct investigations.

The documents required for filing an FIR of a cybercrime depends upon the type of cybercrime committed against the victim (Social Media Crime, Cyber Bullying, Mobile Application Crime, Cyber Extortion, etc.).

Making a written complaint to the cybercrime cell has proven to be the most appropriate method of reporting the crime, as some people either cannot afford internet charges or lack the necessary expertise. A cybercrime victim may file a written complaint with the nearest cyber crime cell or any other cyber crime cell in India¹⁷.

VII. CONCLUSION

The concept of cyber-crime is no new topic, yet the consequences in the digital era, in the 21st century where the mode of occurrence of crime is changing its shape, and so does the laws. Law is a dynamic abstract that moulds itself from changes within society. India being the world's second-largest population, followed by a huge chunk of internet and social media

¹⁵ Ayush Verma, how is cyber-crime investigation conducted, 2020. <https://blog.ipleaders.in/cyber-crime-investigation-conducted> Accessed at 7th May 2021

¹⁶ 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> Accessed at 7th May 2021

¹⁷ Meera Patel, Procedure for filing a cybercrime complaint in India. <https://blog.ipleaders.in/procedure-for-filing-cybercrime-complaint-in-india/> Accessed at 7th May 2021

users, is also subjected to online frauds and crimes. Henceforth, to address the issue of seeking justice is a need of an hour. Hereby the abovementioned findings, the author need awareness among the people, and laws must be stricter. There shall be a separate cybercrime team in each district throughout the country.

Further that this paper would facilitate the online media users for basic awareness to perpetuate the crimes of the future. The author opines that the role of policymakers and administration itself has been sufficient in addressing the key problems with the crimes via online mode. Both the general and specific law deals with criminalizing the offenders.
