IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER LAW IN INDIA: CHALLENGING TIMES

[1]Sahin Ruckia

[1]Student of Final Year L.L.M.
[1]School Of Public Law and Policy
[1]Assam Rajiv Gandhi University of Cooperative Management
[1]Sivsagar,India

Abstract: With the evolution of information technology , the sharing of information/data has advanced with a high pace. We have become dependent on technology to make our day-to-day lives smoother .The outbreak of the pandemic has also resulted in hefty dependence on technology by the people. The truth is, by being more and more active in cyberspace we are making ourselves prone to all kinds of digital assaults by cyber criminals which invariably make us a victim of cyber crime. No doubt technology is a necessary evil but one should be aware of the serious threats posed by the online data leakages, the vandalization caused by cyber criminals to individuals ,organizations and to some extent the government itself which can have some adverse effects and a morbid scenario in the long run. This article revolves around the progression of cyber crimes in India ,the steps taken by government in establishing cyber law enactments to tackle it, some safety measures that could become nifty in adverse situations to avoid getting victimized.

Index Terms **– Technology, Cyberspace, Digital assaults, Cyber criminals, Adverse.**

I. INTRODUCTION

With the introduction of computers in the early 1800s men has taken a series of progressive steps towards creating a future filled with technological advancements such as artificial intelligence, machine learning etc. The internet is one such marvelous achievement of mankind. It is a vast network that interconnects electronic devices all over the world making the exchange of information and communication swift and subtle. The developments in the field of science and technology is continuously advancing at a rapid pace improving the expedition and quality of goods and services. But with the advent of such technological advances comes the cyber criminals who try exploit the common masses with different attacks on their system called cyber attacks. So, as to keep the cyber attacks in check and to govern the cyber area ,cyber law came into existence. In this modern era, cyber law plays an integral role in the overall legal system of a country that constantly deals with the monitoring and prevention of crimes in the internet i.e. cyber crimes , data and privacy protection and the protection of digital and electronic signatures. In India ,the Information Technology Act,2000 is the primary law that deals with cybercrimes and also electronic commerce. The Information Technology Act, 2000 gives a non-exhaustive definition of cyber crime which states that a cyber crime can be described as " an act or omission that is punishable under the Information Technology Act,2000."

II. OBJECTIVES OF THE RESEARCH

As Stephane Nappo once said "The five most efficient cyber defenders are : Anticipation ,Education, Detection, Reaction and Resilience."[1] So the main objective of this article is to carry out a comprehensive research on the five efficient cyber defenders against cyber crimes and purview of India's judiciary system and some of the benchmark cyber-crime related court cases.

III. REVIEW OF LITERATURE

Mrs. Neeta Deshpande (2018) in her research brings about the fact that spreading computer viruses and worms is a severe cybercrime, but it is very difficult to detect such kind of cyber crimes as they are generally committed by websites of foreign origin. She points out the fact that the Information Technology Act, 2000 (IT Act)that governs the cyber law in India lacks the resources to catch and punish cyber criminals that commit crimes from another continent since Sec1 and Sec75 of the IT Act deals with the conduct constituting the offence that involves computer system or computer network located only in India. She also pointed out that since the cyber criminals generally operate from their houses but the police have not been given the power to search the private places under the IT Act.[2]

Nidhi Arya (2019) establishes the fact that with the increase in technological advances cybercrimes increases. Qualified people tend to commit more cyber crimes. Cyber law needs to be evolve to keep cyber crimes in check as hackers are continuously finding out new ways to exploit people's privacy. She writes that the law must find a balance between protecting the citizens from crime and infringing on their rights.[3]

Juneed Iqbal and Bilal Maqbool Beigh(2017) in their research tries to depict the fact that due to the enormous use of internet in India people have become very much prone to cyber crimes. As the nature of cyber crime is global and so the cyber criminals are not bound to a specific place which in turn makes it very hard for the law to take action against it. [4]

V. Krishna Viraja and Pradnya Purandare (2021) in their research concluded that complete eradication of Cybercrime is not possible but we can definitely reduce the impact and the number of cyber crimes by taking requisite precautionary measures to safeguard our data. Knowledge about cybercrimes and cyber laws can aid an individual to be safe and reduce the impact of the crime.[5]

Alazab, M., & Broadhurst, R. (2016) in their research mentioned the various motives for cyber crime activity as some of them are profit related crimes, some that perpetrated directly against electronic devices to torment the user by disabling them while other sorts of cyber crimes activity may include electronic devices or networks to spread malware and adware and getting hold of personal information and exploiting them. [6]

IV. METHODS AND METHODOLOGY

The research was done primarily by gathering data from secondary sources which included books, websites, journals, articles, survey reports etc. In this study, empirical data has also been collected from the website of Cyber Crime Portal [7] to give a robust approach to the understanding of cyber crimes and cyber law in India.

V. DISCUSSION

5.1 Cyber Crime and Cyber Law

This article tries to summarize cyber law and categorize the details by which an individual can be safeguard oneself from getting victimized under the following heads:

5.1.1 Anticipation

Anticipating a cyber crime and a cyber attack before it even happens would ensure a crime free world. As said by Wesley Mcgrew (2017) , “When it comes to cybercrimes, it’s not a matter of ‘if’ but rather ‘when’. So get ready for the onslaught before it’s too late.”[8] It is a wise to be prepared before hand and to expect the unexpected in cyberspace.

5.1.2 Education

Knowledge is the best remedy to cure most of the ailments in the world of cyberspace. In general, cybercrime may be described as “Any unlawful activity where a computer or a communication device or a computer network is used to commit or facilitate the commission of crime”.

A list of some of the cybercrimes along with their indicative explanation are given below to facilitate better understanding of cyber crimes and for reporting of complaints to the authorities.

(a) CHILD PORNOGRAPHY/ CHILD SEXUALLY ABUSIVE MATERIAL (CSAM)
A material containing obscene sexual image of a child getting abused or sexually harassed in any form is called Child sexually abusive material (CSAM). Section 67 (B) of Information Technology Act states that “it is punishable for publishing or transmitting of materials depicting children in sexually explicit act, etc. in electronic form.” [9]

(b) CYBER BULLYING
It refers to a type of harassment or bullying imposed by the use of electronic media or communication devices such as personal computers, mobile phones, laptops, etc.

(c) CYBER STALKING
The act of persistent and unwanted contact from someone by the use of electronic communication or to follow a person, or to foster personal interaction repeatedly or continuous monitoring of the internet, email or any other form of electronic communication despite a clear signal of disinterest by such persons is referred to as stalking.

(d) CYBER GROOMING
Cyber Grooming refers to when a person builds an online emotional relationship or befriends a young person and tricks or pressurizes the individual into doing a sexual act or abuses the individual sexually.

(e) ONLINE JOB FRAUD

Online Job Fraud is another common cyber crime that is making its mark in the society as it attempts to defraud people who are in search of employment by making them a false claim of offering them better employment with lucrative pay for their services.

(f) ONLINE SEXTORTION

Online Sextortion is the scenario when someone blackmails an individual and threatens to distribute his/her private, sensitive and obscene materials using an electronic form in lieu of money or some sexual privilege to the scammer/fraudster.

(g) VISHING

Vishing is becoming common in our day to day lives, it is an attempt where fraudsters tries to seek personal information of an individual like Internet Banking Customer ID and Password, ATM PIN, OTP , Card expiry date, CVV etc. through a phone call.

(h) SEXTING

Sexting is an act of sending sexually explicit digital pictures, videos, multimedia messages, text messages or emails, usually by electronic devices.

(i) SMSHING

Smishing is another type of fraud that is prevalent these days and uses mobile phone text messages to lure victims into calling back on a fraudulent phone number or when a website link is sent to the victim's device and the victim clicks on the link ,it redirects to some fraudulent websites that tend to download malicious content via mobile phone or web.

(j) SIM SWAP SCAM

SIM Swap Scam also called SIM jacking or SIM hijacking occurs when the fraudsters manage to acquire a new SIM card that has been issued against a registered mobile number fraudulently with the help of the mobile service provider. It is a type of identity theft as with the aid of this new SIM card, they get hold of One Time Password (OTP) and message alerts, required to carry out financial transactions in the victim's bank account. Obtaining a new SIM card against a registered mobile number fraudulently is referred to as SIM Swap.

(k)DEBIT/CREDIT CARD FRAUD

This fraud occurs when an unauthorized usage of victim's Credit card or debit card by the fraudsters takes place for the purpose of withdrawal of funds from the accounts of the victim or for purchasing things.

(l)IMPERSONATION AND IDENTITY THEFT

The act of fraudulently making use of the passwords or electronic signatures or any other unique identification feature of any other person is known as Impersonation or identity theft.

(m) PHISHING

Phishing is a type of fraud that involves in stealing of personal information such as Customer ID and password, Credit/Debit Card number, Card expiry date, CVV number etc. through an Electronic Mail that seems to be from a legitimate source.

(n)SPAMMING

Spamming occurs when multiple unsolicited e-mails are sent to an individual usually for marketing purposes, this can be commercial messages ,SMS, MMS or any other similar kinds of electronic messaging media ,trying to persuade the recipient to buy a product or service.

(o)RANSOMWARE

Ransomware is another type of computer malware that encrypts the files in the storage media or on devices like Desktops, Laptops, Cellphones etc., holding data/information as a hostage. The victim is then asked to pay a ransom to get his device decrypted.

(p)VIRUS, WORMS & TROJANS

Computer Virus is a program written to enter a victim's computer with the intention of damaging or altering the files and data in it and then replicating itself.

Worms are malicious programs that make copies of themselves constantly on the local drive, network shares, etc.

A Trojan horse is not a virus but a destructive program that imitates a genuine application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans open a backdoor entry to the victim's computer which gives malicious users/programs access to the victim's system, allowing confidential and sensitive information to be exploited by the cyber attackers.

(q) DATA BREACH

A data breach is an incident where important data from an individual or an organization is accessed and/or stolen without authorization of the owner.

(r)DENIAL OF SERVICES /DISTRIBUTED DOS

Denial of Services (DoS) attack is a cyber attack which is intended to shut down a machine or a network by interrupting the electronic device's normal functioning. Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by flooding it with traffic from multiple sources or transferring of huge amount of data that triggers a crash.

(s) WEBSITE DEFACEMENT
Website Defacement is an attack on a particular website intending to change the visual appearance of the website .The attacker may post indecent, hostile and obscene contents in the website.

(t)CYBER-SQUATTING
Cyber-Squatting is an act of neglecting the overall existence of a trademark to get benefit by selling the domain to the buyers. It can be defined as an act of registering, trafficking in, selling or using a domain name with an intent to profit from the goodwill of a trademark belonging to someone else.

(u)PHARMING
Pharming is cyber-attack that aims to redirect a website's traffic to another, fake website.

(v)CRYPTOJACKING
Cryptojacking is an unauthorized use of victim's computing resources to mine cryptocurrencies.

(w)ONLINE DRUG TRAFFICKING
In Online Drug Trafficking the drug traffickers sells, transports or illegally imports unlawful controlled substances, such as narcotic drugs, heroin, cocaine, marijuana etc. using electronic means.

(x)ESPIONAGE
The act of obtaining relevant data and information of an individual without his prior permission and knowledge .

5.1.3 Detection

In most of the Cyber crime cases related to business enterprises it has been found that the enterprises tend to fall victim to these cyber attacks without even realizing that they have a breach in security, it is only when their customer records, important documents are leaked in public domain or intellectual property turns up in their competitors hands or when their operations tends to come to a halt accompanying demand for ransom they realize that they were victimized. The law enforcements come into the picture now but the damage had already been done. The end result of it all is that, in the absence of an identified cyber criminal, the business representatives will be condemned in the court of public opinion for negligence in safekeeping of the data. So, early detection of data can be feasible only when one gets properly educated about cyber security and by implementation of a cyber security strategy taking measures to protect the principal data.

5.1.4 Reaction

Falling prey to cyber crime effects a victim very harshly as it reduces the individual's online participation and also the effect is much stronger for those who express concern over it. E-commerce frauds which is prevalent these days reduces the victims online banking activities and other activities related to this area suggesting that prevalence of cyber crime can pose a serious threat to the concerned parties who rely on the internet for conducting their business.[10] So, it is a wise decision to be prepared beforehand than to repent later.

5.1.4 Resilience

The ability of an entity or an individual to be able to deliver the intended result despite adverse cyber events.[11] The notion also denotes the ability to restore the regular delivery mechanisms after such events as well as the ability to continuously change or modify these delivery mechanisms if needed in the face of changing risks.[12] In simple words the trait to bounce back after facing a cyber attack and having a plan in place to respond and recover after an attack is known as Resilience.

5.2 Information Technology Act, 2000 and Cyber Law

The legal system in India is extremely detailed and unambiguous. India has a well-defined legal system in place and most of the laws in India were enacted taking into consideration the social, political ,economical and cultural diversity of India. The advent of technology, computers and internet brought about enactment of new and complex legal issues which required the enactment of Cyber Laws .Cyber laws come under the Information Technology Act, 2000 which came into existence on 17th October 2000.
As technology is developing at a fast rate and so are the various methods of commitment of crime using the Internet & Computers evolving and so the IT Act 2000 ought to be amended from time to time to insert new kinds of cyber offences and to plug in other Loopholes that poses hurdles in the effective enforcement of the IT Act, 2000. Below are the various Sections under IT Act, 2000 and examples of a few court cases revolving around the IT Act, 2000.

5.2.1 Sections related to Penalties, Compensation and Adjudication

(1) Section 43 - Penalty and Compensation imposed for damage to computer, computer system etc.[13]
    (i) Section 43A - Compensation imposed for failure to protect information/data.
(2) Section 44 - Penalty imposed for failure to furnish information or return, etc.
(3) Section 45 - Residuary Penalty.
(4) Section 47 - Factors to be taken into account by the adjudicating officer.

5.2.2 Sections related to Offences

(1) Section 65- Offences associated with tampering of computer source documents.[13]
(2) Section 66 - Computer related various types of offences.[13]
(i) Section 66A - Punishment for sending offensive messages with the help of communication service.
(ii) Section 66B - Punishment for dishonestly receiving stolen computer resources or communication device.
(iii) Section 66C - Punishment for identity theft.
(iv) Section 66D - Punishment for cheating by personation by using computer resource.
(v) Section 66E - Punishment for violation of privacy.
(vi) Section-66F- Cyber Terrorism
(3) Section 67 - Punishment for publishing or transmitting obscene material in electronic form.[13]
(i) Section 67A - Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form.
(ii) Section 67B - Punishment for publishing transferring and transmission of material depicting children in sexually explicit act, etc. in electronic form.
(4) Section 69 - Powers to issue directives for interception or monitoring or decryption of any data through any computer resource.[13]
(i) Section 69A - Power to issue directions for blocking for public access of any data through any computer resource.
(ii) Section 69B - Power for authorization of collection and monitoring of traffic data or information through any computer resource for Cyber Security.
(5) Section 71 - Penalty for misrepresentation.
(6) Section 72 - Breaching of confidentiality and privacy.[13]
(i) Section 72A - Punishment for Disclosure of data in breach of lawful contract.
(7) Section 73 - Penalty for publishing of electronic Signature Certificate falsely in certain particulars.
(8) Section 74- Publication for fraudulent purpose.
(9) Section 75 - Act to apply for offences or contraventions carried out outside India.
(10) Section 77 - Penalties or confiscation not to interfere with other punishments.[13]
(i) Section 77A - Compounding of Offences.
(ii) Section 77B - Offences with three years imprisonment to be cognizable.
(11) Section 78 - Power to investigate offences made.[13]

5.2.3 Court cases under IT Act, 2000

(a)Relevant Case: In the case of Shreya Singhal Vs. Union of India, two women were arrested under Section 66A of the IT Act, 2000, alleged to have posted objectionable comments on social networking site Facebook regarding complete shutdowns in Mumbai after the demise of a political leader.
Verdict: Here, the honourable Court held that Section 66A is ambiguous and is violative of the right to freedom of speech and takes away the speech that is innocent. It removed an arbitrary provision from IT Act,2000 and upheld the citizens fundamental right to free speech in India.[14]

(b)Relevant Case: In the Case of CBI Vs. Arif Azim, a website called www.sonysambandh.com enabled Non Resident Indians (NRIs) to send Sony products to their Indian friends and relatives after online payment for the same . A complaint was lodged with Central Bureau of Investigation (CBI) and further, a case under Sections 418,419 and 420 of the Indian Penal Code,1860 was registered. The investigations concluded that Arif Azim while working at a call center in Noida, got access to the credit card details of Barbara Campa which he misused later on.
Verdict: The Court's approach was lenient towards Arif Azim as he was a young boy and a first-time convict;The court released the convicted person on probation for 1 year. This was one among the landmark cases of Cyber Law because it displaced that the Indian Penal Code,1860 can be an effective legislation to rely on when the IT Act is not exhaustive. [15]

(c) Relevant Case: In the case of Poona Auto Ancillaries Pvt. Ltd, Pune Vs. Punjab National Bank, HO New Delhi & Others 2013 in which one of the largest compensation awarded in legal adjudication of a cyber crime dispute. Maharashtra's IT secretary Rajesh Agarwal had ordered PNB to pay Rs. 45 lakhs to the complainant Manmohan Singh Matharu, MD of Pune – based firm Poona Auto Ancillaries. A fraudster had transferred Rs. 80.10 lakh from Matharu's account in PNB, Pune after Matharu responded to a phishing email. Complainant was asked to share the liability since he responded to the phishing mail but the Bank was found negligent due to lack of proper security checks against fraud accounts opened to defraud the complainant.[16]

(d) Relevant Case: In the case of Avnish Bajaj vs. State, famously known as Bazee.com case (2005) CEO of e-commerce Portal was arrested and was given bail later under Section 67 of IT Act on account of an obscene video uploaded on Bazee.com for sale. He proved his due diligence but in 2005, Information Technology Act did not have any provision for 'Intermediary!
Verdict: The honourable court pointed that Mr. Bajaj was not involved in the airing of pornographic content and points that the evidence gathered demonstrates that the cyber pornographic offence was committed by someone other than bazee.com. The CEO has granted bail on the sureties of Rupees one lakh. Thus the onus is on the accused to show that he was only a service provider and not a content creator.[17]

(e) Relevant Case: In the case of State of Tamil Nadu Vs. Suhaskatti, the accused was convicted under Section 469 and 509 of the Indian Penal Code (IPC), 1860 and Section 67 of the IT Act by Additional Chief Metropolitan Magistrate. Suhaskatti was punished with a rigorous imprisonment of 2 years along with a fine of Rs.500 under Section 469 of IPC, Simple imprisonment of 1year along with a fine of Rs.500 under Section 509 of the IPC, and rigorous Imprisonment of 2 years along with a fine of Rs. 4000 under

Section 67 of the IT Act the present case is a landmark case in cyber law as it ensured efficient handling of the case by making conviction possible within 7 months from filing the FIR.[18]

(f) Relevant Case: The Bank NSP Case is a leading cybercrime case where management trainee of the Bank was engaged to be married . The couple exchanged many emails using the company computers . After some time the two broke up and the girl created fraudulent email ids such as "*indianbarassociations"* and sent emails to the boy's computer to do this . The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.[19]

(h) Relevant Case: Cyber Attack on Cosmos Bank In August 2018, the Pune branch of Cosmos bank was drained of Rs. 94crores, in an extremely bold cyber attack. By hacking into the main server, the thieves were able to transfer the money to a bank in Hong Kong . Along with this, the hackers made their way into the ATM server, to gain details of various VISA and Rupay debit cards. The switching system i.e the link between the centralized system and the payment gateway was attacked, meaning neither the bank nor the account holders caught wind of the money being transferred .According to the cybercrime case study internationally, a total of 14000 transactions were carried out, spanning across 28 countries using 480 cards. Nationally ,2800 transactions using 400 cards were carried out. This was one of its kinds and infact the first malware attack that stopped all communication between the bank and the payment gateway. [20]

(i) Relevant Case: In case of Tampering with Computer Source Documents and manipulation , Tata Indicom employees were taken into custody in relation to the tampering of the electronic 32-bit number (ESN) that is programmed into cell phones. The theft was for Reliance Intercom. In a verdict on a later date, the court said that since the source code was manipulated, it calls the use of Section 65 under the Information Technology Act [21].

(j) Relevant Case: In Bomb Hoax Mall Case an hoax email was sent by a 15- year old boy from Bangalore, the Cyber Crime Investigation Cell (CCIC) arrested him in 2009. The boy was accused of sending an email to a private news company saying " I have planted 5 bombs in Mumbai, you have two hours to find them". The concerned authorities were contacted immediately, in relation to the cyber case in India, who traced the IP address(Internet Protocol) to Bangalore.[22]

5.3 Data related to cyber crimes reported in India during the year 2019

(a) India is a vast country with 28 states and 8 Union Territories .The data in Table 5.3.1 ,Table 5.3.2 and Table 5.3.3 is a collection of cyber crimes cases that were reported to the police in the year 2019 by the States/UTs of India excluding the state of West Bengal from where the data of the year 2018 was taken .The data was gathered from the Cyber Crime Portal [2]

Table 5.3.1: Police Disposal of Cyber Crime Cases (Crime Head-wise) under Information Technology Act, 2000

Sl. No.	Crime Heads	Cases Reported during the year (2019)
1	Tampering computer source documents	173
2	Computer Related Offences	28079
3	Ransom-ware	1023
4	Offences other than Ransom-ware	3444
5	Dishonestly receiving stolen computer resource or communication device	558
6	Identity Theft	12255
7	Cheating by personation by using computer resource	5520
8	Violation of Privacy	812
9	Cyber Terrorism	12
10	Publication/transmission of obscene / sexually explicit act in electronic form	7426
13	Publishing or transmitting of material depicting children in Sexually explicit act in electronic form	102
14	Preservation and retention of information by intermediaries	14
16	Interception or Monitoring or decryption of Information	9
17	Un-authorized access/attempt to access protected computer system	2
18	Attempt to Commit Offences	14
19	Other offences under Sections 67 of IT Act	3552
	Total Offences under IT Act ,2000	**30729**

Table 5.3.1: The table provides the number of cyber crime offences under Information Technology Act ,2000 in 2019 which added up to be 30729. In the above table Section 67 of the IT Act is mentioned which states that "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."[3]

Table 5.3.2: Police Disposal of Cyber Crime Cases (Crime Head-wise) under Indian Penal Court (IPC) AND Special and Local Laws(SSL)

Sl. No.	Crime Heads	Cases Reported during the year 2019
1	Abetment of Suicide (Online)	8
2	Cyber Stalking/Bullying of Women/Children	777
3	Data theft	285
4	Online Fraud	6233
5	Credit Card/Debit Card	367
6	ATMs	2067
7	Online Banking Fraud	2093
8	OTP Frauds	549
9	Others	1157
10	Cheating	3393
11	Forgery	512
12	Defamation/Morphing	19
13	Fake Profile	87
14	Counterfeiting	5
15	Currency	5
16	Cyber Blackmailing/Threatening	372
17	Fake News on Social Media	190
18	Other Offences	1849
	Total Offences under IPC	13730

Table 5.3.2 : The table provides the number of cyber crime offences under Indian Penal Court (IPC) in 2019 which adds up to be 13730

Table 6.3: Police Disposal of Cyber Crime Cases (Crime Head-wise) under Special and Local Laws(SSL)

Sl. No..	Crime Heads	Cases Reported during the year 2019
1	Gambling Act (Online Gambling)	22
2	Lotteries Act (Online Lotteries)	9
3	Copy Right Act	34
4	Trade Marks Act	0
5	Other SLL Crimes	22
	Total Offences under SLL	87

Table 5.3.3 : The table provides the number of cyber crime offences under Special and Local Laws(SLL)in 2019 which adds up to be 87

Table 5.3.4: Total number of cyber crimes cases reported in the year 2019

Crime Heads	**Cases Reported during the year 2019**
Total Offences under IT Act ,2000	30729
Total Offences under IPC	13730
Total Offences under SLL	87
Total Cyber Crimes	44546

Table 5.3.4 : The total number of cyber crime cases reported to the police by the States/UTs of India during the year 2019 sums up to be 44546 which determines the level of seriousness of cyber crimes in India .

VI. CONCLUSION

There are numerous new innovations and tricks emerging at a rapid rate in India developed by the cyber criminals to get hold of confidential data of an individual or a business in order to exploit them or simply to create havoc and chaos for the fun of it. We must be extremely careful to understand the confinements and various security risks while messing with things we don't know in the internet. The Cyber law system is governed by the IT Act , and when it cannot offer a remedy to a specific offence or when the IT Act fail to contain exhaustive provision relating to the offence, the IPC should govern the cyber crimes and strictly penalize the wrongdoers. As India moves closer to a digital nation, crime is on the rise, and new forms of cyber crime are emerging day by day which is a threat to privacy and as a result an advance legislation is required to be enacted to deal with such kinds of cyber threats and help the innocent being trapped in the hands of the cyber attackers. There is so much we can do to ensure a safe, secure and trustworthy computing environment if we constantly improvise the strength of our cyber security. It is crucial not only to our national sense of well being, but also to India's national security and economy .

REFERENCES

[1] https://www.mobilecorp.com.au.
[2] Mrs. Neeta Deshpande "A Brief Study on Cyber Crimes and IT Act in India" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), October 2018.
[3] Nidhi Arya "Cyber Crime Scenario in India and Judicial Response" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), Volume-3 | Issue-4, June 2019.
[4] Juneed Iqbal and Bilal Maqbool Beigh, "Cybercrime in India: Trends and Challenges" Published in International Journal of Innovations & Advancement in Computer Science, Volume 6, Issue 12, December 2017.
[5] V Krishna Viraja and Pradnya Purandare, "A Qualitative Research on the Impact and Challenges of Cybercrimes."2021 J. Phys.: Conf. Ser. 1964 042004.
[6] Alazab, M., & Broadhurst, R. (2016). Spam and criminal activity. Trends and Issues in Crime and Criminal Justice, 526. https://doi.org/
[7] https**://**www.cybercrime.gov.in/
[8] htpps://www.cio.com/article
[9] https://indiakanoon.org.
[10] Rainer Bohme and Tyler Moore," How Do Consumers React to Cybercrime ?", DOI:10.1109/eCrime.2012.6489519 Conference: eCrime Researchers Summit (eCrime), 2012
[11] Fredrik Björck, Martin Henkel, Janis Stirna, and Jelena Zdravkovic, "Cyber Resilience – fundamentals for a definition', Springer,2015
[12] Kahan, Jerome H., Andrew C. Allen, and Justin K. George. "An operational framework for resilience." Journal of Homeland Security and Emergency Management 6.1 (2009), page 10
[13] https:// ww.itlaw.in/judgments
[14] Shreya Singhal vs. UOI AIR 2015 SC1523
[15]CBI Vs Arif Azim (Sony Sambandh Case) AIR 2003
[16] Poona Auto Ancillaries Pvt. Ltd, Pune Versus Punjab National Bank, HO New Delhi & Others cyber Appeal/4/2013, Misc Applications/120/2018.
[17] Avnish Bajaj Vs State, famously known as Bazee.com case (NCT) of Delhi (2008)150 DLT 769
[18] State of Tamil Nadu Vs Suhaskatti CC No. 4680 of 2004
[19] The Bank NSP Case (State by Cyber Crime Police Vs. Abubakar Siddique)
[20] Cyber Attack on Cosmos BankIn 2018
[21]Syed Asifuddin And ors . Vs the State of Andhra Pradesh 2006(1) ALD Cri 96, 2005 CriLJ 4314
[22] Bomb Hoax Mail Case AIR 2009