Volume 11, July 2020 ISSN 2581-5504

"Cyber-Crimes and Related Aspects"

***Ritwik Marwaha**
Army Law College, Pune
(Savitri Bai Phule, Pune University)

****Pallav Bhargava**
Army Law College, Pune
(Savitri Bai Phule, Pune University)

Abstract

In today's technology driven world where internet is found in every single walk of life, we are witnessing various sorts of cyber-crimes like cyber defamation, stalking, cyber pornography, online gambling, phishing, cyber conspiracy and cyber terrorism. Among of these crimes' humanity is most severely hit by cyber terrorism. Cyber terrorism is hovering sort of a danger to innovation improvement. the event of internet and therefore the growing dependence of individuals thereon have expanded the safety dangers significantly. it's also increased the vulnerability to the aggressors like criminals, terrorists, hostile countries etc. within the present paper an effort is formed to know the ambit of cyber terrorism in India, the explanations of its occurrence, various legislations to affect the matter and therefore the remedies for tackling the grave issue. Attempt is additionally made to review the cyber terrorism from the aspect of Information Technology Act, 2000. The paper also puts light on various cases and incidents of cyber terrorism in India in recent past.

Keywords- Cyber, Terrorism, Internet, Danger, Information, Technology

Introduction

> *"An invasion by armies are often resisted but not a thought whose time has come. In fact, nothing is more powerful than a thought whose time has come."* -Victor Hugo

With the arrival of internet and technology, terrorism has emerged within the new dimensions with more destruction, vigor and deadly nature. the normal methods and ideas of terrorism are now combined with technology and if precautions aren't taken to handle this deadliest combination, it's going to take its own toll. the planet of internet may be a double-edged sword. It is often used for constructive work also as destructive work. Terrorists are gaining expertise within the field of technology to cause destruction of nature which is irreversible. This era is witnessing the worst sort of terrorism referred to as "Cyber Terrorism". Cyber terrorism makes the utilization of internet but still it's starkly different from internet crimes like fraud, theft as cyber terrorists uses the technology to cause death and injury to the institutions, economies, infrastructures. Cyber terrorist attacks are done by capture of traffic, electrical power grids, financial transactions, military command systems, telecommunication networks. the utilization of Aadhaar cards is becoming global and therefore the biggest danger faced is that it's becoming easier to mask an identity online. Also, once the Malware code are available open market, it is often bought by hackers anywhere within the world. so as to get the most aim, the cyber terrorists cripple material infrastructure of country by cyber-attacks. Cybercrime is vast spreading everywhere the planet because today terrorist do more damage with keyboard than bomb thanks to this easy excess to internet resources.

The problem most ordinarily faced in avoiding cyber terrorism is that internet recognizes no boundaries. there's absence of a consistent law to unravel the matters concerning the “jurisdictional problem”. The attacker or the terrorist may belong to any a part of the planet. it's difficult to trace such terrorists and moreover laws of all the countries vary. Today during this electronic era there exist a robust got to come up and strengthen an answer which is techno legal instead of pure legal course. And as India is on the edge of digital age, the country needs strengthen its offensive and defensive capabilities to affect the new wave of cybercrime.

Cyber-crimes are criminal offenses committed through the web or otherwise abetted by various sorts of technology. But while cybercrime may be a relatively new phenomenon, many of an equivalent offense which will be committed with a computer or smart phone, including theft or kiddie porn, were committed face to face before the pc age.

Types of Cyber-crimes

1. Phishing Scams

Phishing scams are attempts by scammers to trick anyone into giving out one’s personal information. These scammers will contact out of the blue, via email, text message, call or maybe through social media, pretending to be a legitimate business like one’s bank, telephone service or maybe internet provider.

The scammer may ask you to update them on your details in order that they can refresh their systems, they'll even ask you to fill out a survey as you've got the prospect to win a prize at the top. But here is where the scammer can get access to your email address, telephone number and more.

Another way these scammers line up of your information is to inform you that ‘unauthorized or suspicious activity has been happening on your account’, and that they will then ask you for your information in order that they can “sort it out”.

In fact, they're getting to steal from you. Phishing attacks work an equivalent as fraudulent phone calls which individuals are being educated on.

2. Online Scams

Online scams, are basically scams that happen online.

Whether that’s tricking you into giving out personal details online by a billboard shooting up telling you you've got won something and posing for your card details to buy shipping. Sadly, you’ll never receive anything but you’ll start noticing weird transactions coming from your checking account.

3. Malware

Malware is that the contraction of malicious software onto your system. It's a bit of software written with the intent of causing harm to data and devices. Malware is that the overarching name for various sorts of viruses like a 'trojan' and 'spyware'. Malware is usually done through a variety of viruses which will get into your computer to cause havoc, by damaging your computer, tablet, phone; therefore, the culprits can steal master card details and other personal information.

4. Email Bombing

An email bomb is more a sort of internet abuse. Email bombing is an overload of emails directed to at least one email address, this may cause the person receiving the emails server to become sluggish or maybe crash. they'll not necessarily be stealing anything from you but having a sluggish server are often a true pain and diligence to repair.

5. Virus Dissemination

This is particularly sneaky sort of cybercrime. It not only gets a bit of malware (a virus of some sort) onto one a part of the victim's system, but it spreads across other pieces of software. Without a full and proper quarantine process and safe environment to check in (a sandbox), subsequent time you open a bit of undiagnosed-as-infected software, the method starts everywhere again.

6. Logic Bombs

Logic bombs act within the same way as an epidemic, but are small programs or sections of a program, which are triggered by an occasion. This event is often a particular date or time, a particular percentage of disc space filled, the removal of a file then on.

A program could then delete critical segments of code, execution your software as unusable. The people that implement logic bombs are most ordinarily installed by insiders who already had access to the system.

7. Theft

Internet theft is that the broad term for any sort of theft that happens over the web , this will be done through some ways like fake ads, fake emails, viruses and snooping. The aim of internet theft is to steal your personal information and use it to then steal money out of your checking account or make purchases using your details.

8. Social Media Hack & Spamming

Social media hacking is usually done as a joke, just like the attack by the people that hacked Burger King's twitter account, and many celebrities that are hacked may find yourself following people they wouldn't usually or put random statuses. albeit for the typical joe seeing a star or brand post weird stuff are often amusing, it's an invasion of privacy.

However, a hacker also can spread unwarranted content which will be distressing to people that view this content, it also can cause your account to be reported and pack up.

Social media spamming comes when an individual makes a fake account and becomes friends or followed by the typical person. This then gives the fake account the liberty to spam inboxes with bulk messaging, this will be finished spreading malware.

Spamming also can spread malicious links created with the intent to harm, mislead or damage a user or their device. Clicking on the malicious link, which can be advertising a replacement iPhone or weight loss treatment, means you'll be downloading malware which may cause the theft of private information.

Another dark side of social media is that the ability for malicious accounts to spam your output by constantly replying with negative messaging. A sort of trolling.

Though you'll easily report such behavior to the social media platform and they should remove the user, else you can block them from seeing your content, but it’s easy for people to line up new bot accounts in minutes and start their attack again.

Some people have an excessive amount of time on their hands.

9. Electronic concealment

Money generated in large volumes illegally must be laundered before it is often spent or invested. a method to launder money is to try to it electronically through messages between banks which is understood as a “wire transfer”. It had previously seemed impossible to watch or screen wire transfers as they occur thanks to the tremendous volume on transactions browsing on a day to day basis, however banks are clamping down on the difficulty and filing away any suspicious activity.

10. Eavesdropping & Surveillance

Eavesdropping without the consent of the parties may be a crime and may be done online or over the phone. the foremost common thanks to eavesdrop is to wiretap, which is that the practice of connecting a listening device, usually to a telephone line, that permits the criminal to watch conversation secretly. As newfangled technologies are introduced, computers can now be hacked for eavesdropping and surveillance. As a random tip, take a glance at, Facebook head man, Mark Zuckerberg’s painfully simple defiance against would-be webcam voyeurs.

11. Software Piracy

Nowadays, because of the web, you'll find almost any movie, song or software for free of charge online. Software piracy is that the unauthorized use and distribution of computer software. albeit using pirated material could seem good because it’s free, it comes with a variety of risks. These risks include: Trojans, viruses, worms and other sorts of malware.

But it’s also stealing as no proceeds attend the producers of the content.

12. Data Diddling

Despite the humorous name and seemingly innocuous action compared to other cyber-crimes during this list, data diddling is that the action of skewing data entries within the user's system. The results are often huge, however. they could include adjusting financial figures up or down marginally, or it might be more complex and make a whole system unusable.

13. Hacking

In simple terms, a hacker is an intruder who accesses your computing system without your permission. Hackers do that for variety of reasons, whether that's for greed, fame or power, because it shows people, they're clever enough to urge into something they shouldn't have. However, some are going to be ready to force an entry system and steal personal banking information and corporation financial data. Hackers tend to be computer programmers and have a complicated understanding of computers.

14. Cyber Stalking

There are many cases of cyber stalking across the planet and it's especially common with teenagers and young adults. Usually the victim and therefore the stalker know one another. The victim is typically subjected to online harassment in sorts of a barrage of online messages and emails. The aim of online stalking is to form the victim miserable or exert control as a perverse way of being in touch with the victim, a bit like ordinary stalking.

15. Cyber Bullying

Cyber bullying is analogous to cyber stalking, however, the barrage of messages are often harmful, abusive, and wholly offensive. Cyber bullying also can be done by posting images and videos online which will offend the victims. It also can be excluding people online, creating fake accounts to post harmful or distressing content and again sending abusive messages. Overall, it's bullying but online usually through social media channels.

16. Fraud

Identity theft is one among the foremost common sorts of cybercrime. the most reason fraud occurs is with the view of making fraud for financial gains. Criminals usually steal identity information of others like master card information, addresses, email addresses and more. With this information they will pretend to be somebody else and make new bank accounts.

17. Child Soliciting & Abuse

Child soliciting and abuse online may be a sort of cybercrime where criminals solicit children via chat rooms for the aim of pornography. It also can are available sorts of material that shows or describes sexual assault towards children. a toddler is considered someone who is under the age of 16. this sort of cybercrime is heavily monitored by the police.

It is often a threat to companies also as individuals because the perpetrators could also be looking to adopt another persona online.

18. Ransomware

Ransomware affects many companies and has recently affected the NHS and other big corporations everywhere the planet. Ransomware enters your network and encrypts files, meaning you don't have any access to them. The attacker will send you a notification demanding an outsized sum of cash for you to then get your data back. The criminals aim is that they're going to get enough people to pay to ransom fee to urge a fast buck.

19. Computer Vandalism:

Computer vandalism may be a sort of malicious behavior that involves damages computers and data in various ways and potentially disrupting businesses. Typical computer vandalism involves the creation of malicious programs designed to perform harmful tasks like erasing disk drive data or extracting login credentials. Computer vandalism contrasts from virus, which confer themselves to existing programs.

20. Child pornography and Abuse:

the web is being highly wont to abuse children sexually worldwide. this is often also a kind of cyber-crime wherein criminals solicit minors via chat rooms for the aim of kid pornography. The Cybersecurity department of each nation is spending tons of your time monitoring chat rooms frequented by children with the hopes of reducing and preventing maltreatment and soliciting.

Causes of cyber-crime

Cybercriminals always choose a simple thanks to make pile. they aim rich people or rich organizations like banks, casinos and financial firms where an enormous amount of cash flows daily and hack sensitive information. Catching such criminals is difficult. Hence, that increases the amount of cyber-crimes across the world. Computers are vulnerable, so laws are required to guard and safeguard them against cybercriminals. We could list the subsequent reasons for the vulnerability of computers:

1. Easy to access

The matter behind safeguarding a computing system from unauthorized access is that there are many possibilities of breach thanks to the complex technology. Hackers can steal access codes, images, advanced voice recorders etc. which will fool biometric systems easily and bypass firewalls are often utilized to urge past many security systems.

Capacity to store data in comparatively small space.

The pc has the unique characteristic of storing data during a very small space. This makes it tons easier for the people to steal data from the other storage and use it for own profit.

2. Complex

The computers run on operating systems and these operating systems are programmed of many codes. The human mind is imperfect, in order that they can do mistakes at any stage. The cybercriminals cash in of those gaps.

3. Loss of evidence

The data associated with the crime are often easily destroyed and hence, loss of evidence.

4. Negligence

Negligence is one among the characteristics of human conduct. So, there could also be an opportunity that protecting the pc system we may make any negligence which provides a cyber-criminal the access and control over the pc system.

5. Attack of the Zombie Servers and Other Alarming Facts

The cost of knowledge breaches continues to rise and has increased 29% to a mean of $4 million per incident. In 2015, mobile devices had but a tenth infection rate, in order that they were considered safe. Now, quite three-fifths of IT security professionals report that it's either certain or likely their organization suffered a breach due to mobile devices.

Cybercriminals have rooted malware into legitimate applications and they are targeting poorly secured Wi-fi spots, thieving passwords, and more in their quest to rob information.

Attackers wish to exploit unauthorized products with weak security controls within the corporate cloud.

Zombie servers that are left unattended or aren't updated offer additional ways to access networks. Known vulnerabilities aren't patched in time – a study has found that it takes a mean of 193 days before a patch gets applied to repair a drag, albeit the patch is out there. That’s a simple place for exploiters to urge in and do their damage.

Effects of Cyber-crimes

1. The Psychological Effects could mainly be seen in teenagers as they try to conduct acts like adults by making abusive comments on someone else profile this affects them mentally.

2.Sometimes cyber-crimes also affect individuals mentally and it results into depression, anxiety, stress and sometimes due to the fear of image in public some individuals commit suicides.

3. As the Wrongdoer could easily escape from small cyber-crimes this boost their confidence and they commit big cyber-crimes as they know that they could not be easily identified.

4. Sometimes a particular religion is blamed for a wrongful act happened in the society and by making the social media a platform such religion is humiliated or trolled by posting immoral posters so by act of any individual it is wrong that people of particular religion would be humiliated and this it results they feel that they are discriminated by the society.

Legal Provisions to tackle Cyber-crimes in India

As the society changes, the concept of the crime developed along with the time and invented the cybercrime as cybercrime being a criminal act in which the computer or the network is either the tool or target, or both. In India, the criminal law means nothing but the Indian Penal Code, 1960; this is the complete code which deals with all the offences, though the concept of crime is new and technical, but the Indian Penal Code is still effective enough to cover all kinds of crime. Therefore, this conventional criminal law is sufficient to deal with all kinds of crimes, whether it is a cybercrime or any other crime.

Indian legal system enacted Information Technology Act, 2000 with intent to regulate the e-business. That is purely a contractual law dealing with the commerce, but along with e-business, it provides certain provisions dealing with unauthorized use of the internet or unauthorized use of the computer. This misuse is called as a cybercrime in the Information Technology Act, 2000, which is India's cyber Law.

The offences provided in this Act are already provided in Indian Penal Code in the various provision from the enactment of the Indian Penal Code. After coming into force of the Information Technology Act, 2000 appropriate provisions have been fused in the utilitarian criminal law of India. The substantive criminal Law of India means Indian Penal Code, because the various offences of this law are too much similar to the offences which are known cybercrime, only due to technology to commit that offences are quite different therefore the amendments are require to bring that offences under the preview of this Code. The amendment inserts certain new term in the Indian Penal Code only with intent to make effective implementation of provisions dealing with these offences which are going to commit by using the information technology. The Information Technology Act, 2000 contains wide range of offences such as tempering with computer sources, sending offensive messages, violation of privacy; publishing obscene material etc. these all illegal activities are already recognized as an offence in Indian Penal Code. These similarities can discuss in the following ways;

Similar offences also fall under the Indian Penal Code.

1) Sending threatening messages by email- Section 503 IPC[1]
2) Sending defamatory messages by email- Section 499 IPC[2]
3) Forgery of electronic records- Section 463 IPC[3]
4) Bogus websites, cyber frauds- Section 420 IPC[4]
5) Email spoofing- Section 463 IPC[5]
6) Web-jacking- Section 383 IPC[6]

[1] https://indiankanoon.org/doc/878688/
[2] https://indiankanoon.org/doc/1041742/
[3] https://indiankanoon.org/doc/1328629/
[4] https://indiankanoon.org/doc/1436241/
[5] https://indiankanoon.org/doc/1328629/
[6] https://indiankanoon.org/doc/262864/

7) E-Mail Abuse- Section 500 IPC[7]
8) Online sale of Drugs- NDPS Act, 1985[8]
9) Online sale of Arms- Arm's Act, 1959[9]
10) Pornography- Section 292 IPC[10]

India also, like other countries of western has a well-developed legal infrastructure and it is going with the development and time. The result of this, India too is sharing the legal liability, which is the outcome of the technological boom. Though the India is having rich heritage of the legal system, then also it facing the problem of the traditional notion of the jurisdiction which is the great difficulty for the laws related to the cyber space. To meet the need of 21st Century the Indian legal system deals with the laws relating to the cyber space and cybercrime as following:

1. Information Technology Act, 2000[11]: To regulate the electronic communication the Indian Parliament has enacted this Act, which involve the use of alternatives to the paper base means of communication and storage of information, to facilitate the electronic filing with the government agencies. Along with the enactment of the IT Act 2000, to recognize the electronic communication certain important amendments has made in the Indian laws, the amendments are required to make the execution of the regular laws in the IT age. The main object of the IT Act was to facilitate legal reorganization and regulation of commercial activities through electronic medium. This Indian Act is based mainly on the United Nations resolution No A/RES/51/162[12]; as well as on the UNICITRAL Model Law on Electronic Commerce[13]. This is only one act in Indian legal system, which known as the Cyber Law of India.

At the outset, this act no-where defines the term cybercrime and this Act does not focus its attention towards the various forms of cyber-crimes. If we see the basic object of this Act, it is business law rather than the criminal law. The maximum provisions of this Act deal with the regulations of e-commerce. The law is enacted to meet the digital technology and new communication technology and it also provides penalties for misuse or illegal use of technology in certain situation therefore it is known as cyber law of India. As per the preamble of the Act, the object is more dealing with the electronic communication and the contract, which made through the internet. The preamble of Act says there is need for bringing in suitable amendments in the existing laws in our country to facilitate e-commerce. It is also proposed to create the civil and criminal liabilities for contravention of the provision of the proposed legislation.

[7] https://indiankanoon.org/doc/1408202/

[8] https://indiacode.nic.in/bitstream/123456789/10483/1/the_narcotic_drugs_and_psychotropic_substances%2C_act%2C_1985.pdf

[9] https://indiacode.nic.in/bitstream/123456789/10495/1/arms_and_ammunition_act_1959.pdf

[10] https://indiankanoon.org/doc/1704109/

[11] https://indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[12] https://undocs.org/en/A/RES/51/162 ; dated 30th January, 1997

[13] https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

The Information Technology (Amendment) Act, 2008[14]

After the execution from the 2000, the IT Act is facing difficulties while executing. Due to certain technical loopholes in IT Act, 2000, the amendment is sought to for the smooth execution of the Act; the amendment takes place in 2008, which has changed the nature of the IT Act. To meet the hurdles for the enforcement certain important sections are inserted in the IT Act and it brought the various illegal activities on computer in the preview of cybercrime in this Act the Information Technology (Amendment) Act, 2008 which was made effective from 27th October 2009. The IT (Amendment) Act, 2008 has brought notable variations in the IT Act, 2000 on several counts. The amendment added certain important definitions in the Act, Section 2(h) is added "Communication device" which bring the cell phone under the preview of cybercrime. This amendment brings all communication devices, cell phones, iPods or other devices used to communicate, send or transmit any text, video, audio or image. Section 2 (w) has also bring the service providers under the preview of cybercrime. The amendment Act also injected numerous new things in the Act as like the controlling authority, power of adjudicative authority. However, more important is that, certain provisions regarding the offences are included in the Act. Many cyber-crimes for which no express provisions existed in the IT Act, 2000 now included by the IT (Amendment) Act, 2008. This Act adds new provisions in section 66, as like Sending of offensive or false messages (66A), receiving stolen computer resource (66B), identity theft (66C), cheating by personation (66D), violation of privacy (66E). These all things though concern with the privacy rights but that is going to violated by different mode so it requires to be in the Act.

A new offence of Cyber terrorism was furthered in Section 66 F which prescribes punishment that may extend to life imprisonment. Section 66 F, have jurisdiction over any act committed with the intent to threaten the unity, integrity, security or sovereignty of India. For other offences mentioned in Section 66, punishment prescribed is generally up to three years and fine of one/two lakhs and these offences are cognizable and bailable. This will not prove to play a warning factor for cyber criminals. Further, as per new Section 84B, abetment to commit an offence is made punishable and the new Section 84C makes an attempt to commit an offence also a punishable offence with imprisonment. In certain offences, such as hacking (Sec 66) punishment is higher from three years of imprisonment and fine of five lakhs.

In Section 67, for publishing of obscene information imprisonment term has been reduced from five years to three years and fine has been increased from one lakh to five lakhs. Section 67(A) enhances an offence of reproducing, material containing sexually explicit deportment, is punishable with imprisonment for five years with a fine up to ten lakhs. This provision is essential to limit MMS attacks and video voyeurism. Section 67(B) punishes offence for child pornography, child's sexually explicit act with imprisonment for a term up to five years and fine up to ten lakhs.

[14] https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMTk4NzY=

Punishment for disclosure of information in breach of lawful contract under Section 72 is increased from two years up to five years and from one lakh to five lakhs or both. This will deter the commission of such crime. By the virtue of Section 84(B), person who backs a cybercrime will be punished under the Act. This provision will play a preventive role in stopping commission of conspiracy linked with cyber-crimes. In addition, punishment for attempt to commit offences is given under Section 84(C), which will be punishable with one half of the term of imprisonment prescribed for that offence or such fine as provided or both. Thus, the important changes take place in IT Act 2008, which brings the various crimes, which are committed by using the computer or any communication device. Then also various cyber-crimes are going to be registered using the Indian Penal Code. It shows that the Amendment cannot cover all the cyber-crimes, because the cybercrime is basically different from the conventional crime, however the way to commit the crime is changed and computer is a tool to commit the crime.

2. Indian Penal Code, 1860[15]: Indian Penal Code is the universal criminal law of India. The base to constitute the offence is nothing but the guilty intention and prohibited act according to the Indian Penal Code. The Indian penal Code is basic criminal law of India, along with the time, the legal system enacted certain special criminal law. The cybercrime is creation of information technology age, though the modes or ways to commits cybercrime is different from the conventional crime, but it is not much different from the conventional crime. The IT Act has not covered all the cyber-crimes; again, Indian Penal code is applicable.

Due to the universal nature of the IPC, it covers almost all the crime. Therefore, the enactment of Information technology compels the law makers to amend the Indian Penal code, which is called as a conventional Penal law of India. The First schedule to the Information Technology Act of 2000 has amended the certain provisions of Indian Penal code, 1860. The amended provision has been widened to include offences involving electronic record. Sec 192 of the Indian Penal code has amended the meaning of fabricating false evidence to include any false entry or electronic records containing a false statement. The word electronic record is creation of this digital world.

When the electronic record is comes under the preview of the IPC, then most of the offences relating the documents which are committed by way of computer are comes under the jurisdiction of IPC, though they are known as a cybercrime. Section 192 deals with the fabricating false evidence, whenever any electronic record is falsely made which provided for the judicial proceeding then it amounts to be fabricating false evidence. This offence can be committed by using the computer as a tool, and then also it is subject to the Indian Penal code, apart from this the crime like web-jacking, threatening emails etc. are within the preview of section 383 of IPC dealing with the extortion.

[15] https://indiacode.nic.in/bitstream/123456789/4219/1/THE-INDIAN-PENAL-CODE-1860.pdf

In the IT Act, Section 66B used the word “dishonest intention” which is not defined in the IT Act then one can refer to IPC, which is a general legislation in the area of criminal law. When any cyber fraud is committed in real sense it would be cheating which is defined in section 415 of I.P.C. when any person makes the cheating by using internet it is very easy to him to hide his identity, this act perfectly comes it the offence provided under section 416 of I.P.C. that is cheating by personation. Apart from these various cyber offences are relevant under the sections as like 405,406,463,465 of IPC. even the launching of virus is provided under section 43 of IT Act is comes under the preview of sec. 425 of IPC.

The act of launching of virus and other 86 computer contaminants, would also amount to criminal offence of mischief. If the essentials of mischief are satisfied it would be an offence too. Thus, the Indian Penal Code almost covers various cyber-crimes, but considering the needs and development along with the information Technology Act certain important amendments made in Indian Penal Code in 2000. The amendments are sought to bring the paperless transactions under the preview of conventional criminal law. This amendment is suitable in the age of electronic commerce. Due to amendment the Act eliminated the basic requirement of paperless record and documents because substantive as well as procedural law.

3. Indian Evidence Act[16] and Criminal procedure Code[17]: These are two important procedural laws in Indian legal system. Both are dealing with the procedure of criminal proceeding. Due to increasing crimes of fraud through the computer and internet, these Act are also required to amend and made suitable for the information technology age. Considering the need acquired changes have been made in the Indian Evidence Act, Indian Penal Code and Criminal Procedure Code by the Indian Parliament on December 23, 2008 with the passing of Amended IT Bill 2006. In Indian Evidence Act, Section 3 relating to interpretation clause words 'Digital Signature' and 'Digital Signature Certificate', the words 'Electronic Signature' and 'Electronic Signature Certificate' are substituted. In Criminal Procedure Code, after Section 198 A, Section 198 B has been inserted according to which, "No Court shall take cognizance of an offence punishable under Sections 417, 419 and 502 of the Indian Penal Code, except upon a complaint made by the person aggrieved by the offence". Moreover, in the Indian Penal Code the meaning of some words like "offences" and "computer resource" has Section 198 A of Cr. P.C. 1973 been made more exhaustive which take colour from the IT Act, 2000. It shows that India is successful in facing new challenges of IT. Many amendments have been made in the Copy Right Act on the argument that certain knowledge should be treated as private property and capable of 'Ownership'. Considering the requirement of society now, cyber law is providing a worth in administration of justice.

4. Cyber laws in India: Apart from the Information Technology Act and Indian Penal Code, there are certain laws and regulations, which deal with the cybercrime. Even certain civil laws are relevant in certain misuse in cyber space. However, generally the fraud is there

[16] https://indiankanoon.org/doc/1953529/
[17] https://indiankanoon.org/doc/445276/

in cybercrime, therefore it concerns with the criminal law, otherwise even Law of Tort is also relevant and can provide the remedy to unauthorized use of the computer and internet. Apart from The Information Technology Act 2000 and Indian Penal Code 1860, there are various other laws relating to cybercrime in India. They are as following.

1. Common Law (governed by general principles of law)
2. The Bankers' Book Evidence Act, 1891[18]
3. The Reserve Bank of India Act, 1934[19]
4. The Information Technology (Removal of difficulties) Order, 2002[20]
5. The Information Technology (Certifying Authorities) Rules, 2000[21]
6. The Information Technology (Certifying Authorities) Regulations, 2001[22]
7. The Information Technology (Securities Procedure) Rules, 2004[23]
8. Various laws relating to IPRs.

Thus, the Indian legal system is having various laws concerning the cyber-crimes. But the nature of the cybercrime is technical, therefore it requires the technical process to execute the criminal law in proper sense. The technical process is lacking in Indian legal system, therefore though the substantive criminal law is sufficient, but due to lacking in procedural aspect its unable to execute it in India. The basic problem in the cybercrime is that, there is specific manner by which the internet can be misuse; it is on the criminals, that they always misuse it in different manner, therefore it is not possible to the legal system to meet with the need. Apart from this, the nature of cybercrime is transnational, therefore it required the international co-operation. Mere making laws is not sufficient, cyber law cannot work without the international co-operation. The Information Technology Act 2000 and all the related laws having provision regarding the transnational jurisdiction, but execution is possible when all countries in the world recognized that act as a crime, and allow the proceeding on that aspect.

Conclusion

At the end we would like to conclude it by asking a few questions that for what purpose the Social Media is and for what purpose it is being used by the youth? Can it be used for bringing a positive change in the society, the answer of these questions is hidden in the acts done by youngsters as we have again and again mentioned the use of Social Media is only done for getting popularity or to take revenge by various means. It's very important that today's youth must be aware of the future consequences and this was done not only by various Organizations but also by some Youth Channels such as MTV by introducing serials like MTV Webbed and Troll Police which could be seen as a perfect example to make youth aware that how their wrongful acts create negative impact on the society as a whole as they

[18] https://indiankanoon.org/doc/1976331/

[19] https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RBIAM_230609.pdf

[20] http://www.bareactslive.com/ACA/ACT1966.HTM

[21] https://meity.gov.in/writereaddata/files/Information%20Technology%20%28Certifying%20Authority%29.pdf

[22] https://cyberpandit.org/?page_id=1989

[23] https://meity.gov.in/writereaddata/files/The%20Information%20Technology%20%28Security%20Procedure%29%20Rules%2C%202004.pdf

showcase the cases in which the trollers are called upon on the show and made guilty for their wrongful acts as the main aim of the show is to make them realize by making them meet the person they trolled on social media.

One of the main causes or reasons of increasing suicides is also Cyber-crimes, as it is used as a mean for taking revenge by posting the victim’s images or obscene videos and this revenge gives negative impact on victim’s sentiments or feeling. It is not always that the boys use social media to harass but sometimes even girls try to harass boys by posting the screenshots on their profile to gain sympathy and for damaging reputation of boys in front of her friends and the whole society. Now as we earlier mentioned some reasons of cyber-crimes and the main reason which came is that the accused could easily escape due to lack of evidence and somewhat inefficiency of investigating agencies.

Even sometimes if the crime is committed against the women and with the fear to face the society and fear of being embarrassed, they do not file suit against the wrong-doer and by not filing the case, they boost self-confidence of cyber-criminals to continue with their wrongful acts. Therefore, in order to put light on suggestions we would like to say that there should be a special tribunal for handling cybercrime cases by keeping the personal information of the victim confidential.

The Investigation Agencies should also recruit more specialized experts that could easily deal or locate and find suitable evidences against the person so that a fair trial could be done against the wrong-doer. At the end we can use social media for stopping such crimes by using high level security for maintaining privacy of the person and the account must be fully verified to stop troller from trolling anyone. As the society could not prevent such crimes but their small steps by creating awareness or giving knowledge to their upcoming generations for the right use of social media could make a big difference and take our society to bright and sage future and to use the social media in the positive manner rather than trolling anyone.