Volume 1 Issue 3 ISSN NO : 2582-6034

LEGALFOXES LAW TIMES

# CYBER CRIME AND LAW

By SHIVANTIKA and VANSHIKA TAINWALA

## 1. ABSTRACT

In the recent era, the essence of crime has changed and it is not confined to the typical methods of committing a wrong which is prohibited by law. In the year 2000, the Information Technology Act was set out by the Indian Parliament recognizing the need for individual, economy and national security. The age of millennium is hyper interactive on the social media and e- networking, which in turn supplements the growth of social cyber evils in the society. The major drawback which needs to be acknowledged in the field of electronic media is that of the trivial problems of humans in day to day life, whether it is just a matter of petty ATM frauds, OTP hacks, e-wallet frauds etc..The major question to be considered is whether the sections of IT Act are sufficient to regulate all the scams and crimes pertaining to cyber crimes in India, as it's important that with the increase of internet based technology, there should be acceptable changes, amendments and additions to be made in the Act for the further protection of human civilized society.



**Keywords**: cyber crime, IT Act, technology, e-networking, internet.

## 2. INTRODUCTION TO CYBER CRIME

The contemporary world is highly engaged and hyped about the new trends and technologies that surround us, majorly being the era of internet based expansion every little thing has gained recognition world-wide. When we talk about new trends and technologies, we are often concerned with the positive and negative aspects that come along these variations in the trend. One of the most outrageous things to happen in human civilized society is the misuse of the facilities that are being provided by the internet based technologies in current scenario. The current age is conscious about posting every little detail on the social websites which in turn creates a hypothetical picture and is portrayed in form of different opinions in the society. Due to the age of 'internet recognized society', every minute things gain recognition. The term cyber crime has not been clearly defined in any Act or statute by the Indian Legislature but the simple meaning of the word is 'illegal use of any internet based or computerized technology'. Cyber crime has been underlined by the different authors and some definitions fail to underline further more complicated things that are associated with the internet based crimes in the society such as cyber frauds, cyber terrorism, cyber hacking for monetary loss and national security threats which connects much un-safe and un-predictable crimes in the society. Internet has changed the perception of human civilized society.The legislature needs to draw a fine line between the concept of respecting the individual rights of privacy, free speech and the concept of competing interest of society at large. The prevailing laws are found to be incompetent to handle the chaos created in the cyberspace as a result of which the offenders finds it easy to curb their way into increased interaction of social evil. The cyber crime is such a field that changes with greater advancements every now and then, so it is very important for the state to recognize comprehensive legal framework to address unique and new challenges faced by the people. It is also to be considered that there needs to be a co-operation between the traditional, technological international crimes of internet base.

The context and nature of the society plays a very crucial role in determining the range and types of the evil prevailing in the society. The mindset of people, the political, social, economical framework of the society helps to build a constructive application of understanding in determining the loopholes of crimes and other related aspects to it as well. The nature and scope of the crime is well understood when it is studied in context of prevailing corrective measures available for that crime with the extent of corrective measure needed to actually curbthe problem. The basic analysis

between the two helps the legislature to find a perfect balance of what is needed in the society in reference to rapid changing of internet based crimes. The growth of the internet world is so rapid that it creates a complex situation where there is very difficult to analyze and apply corrective laws. Current technology has generated a pause to the limit of time, efforts and lacuna, it has become every convenient for people to connect at large in seconds. However, the exceptional up-gradation of computers today has caused to widen the issue of jurisdictionin legal framework of every country. The jurisdictional error complicates the actual issue of crime to even a greater level. Jurisdiction is the basic step towards addressing the problem in the court to find a remedy;such a basic error slows down the process of justice in the society and also contributes to increased cases plus backlogging of cases in the courts. Theambiguity faced when the courts were burdened with questions pertaining to jurisdiction,failed to conclude any proper place/forum to decide or entertain cases involving cyber crime.

## 3. REASONS RELATING TO CONTEMPORARY EXISTENCE OF CYBER CRIME

Crime is a communal abnormality with diversified reasoning for the offence of crime. Cyber Crime is the formulation of technology and technology makes everything accessible and simple that is the reason why every human is dependent on technology without having sufficient need and awareness of the consequences. In "The Concept of Law" by Prof. HLA Hart, it is mentioned that human beings are attracted to unlawful acts which are wrong i.e. crime and so rule of law is necessary so as to enforce it upon such person who commits the wrong. The technology is easily benefitted from a person or his digital accessories with the help of prohibited or unlawful access.

It is not that possible to frame one distinctive reason behind the whole act of commission of the cyber crime in all over the world.

The proper logic for the susceptibility of computer to cyber criminality can be elaborated as follows[1]:

- CAPACITY TO STORE DATA IN COMPARETIVELY SMALL AREA

[1]CYBER CRIMEby ParthasarathiPati*available at*: http://www.naavi.org/pati/pati_cybercrimes_dec03.htm. (last visited on April 10,2019)

Computer resources have the scope to accommodateall the information in a confined space. The information stored in the ROM (Read Only Memory) will sustain as neutralized even if the power of the system is made to turn off. The data will remain as it is unless someone does it purposely or tries to exploit it leading to the commission of the cyber crime.

- WIDER ACCESS TO INFORMATION

Information is easily exploited by the wrong doers. The internet banking or transactions which people do online on day to day basis in their mobile phones or computers or laptops is easily accessible due to which information is stolen by software of hacking and other similar tools. Biometric technology can also be easily light-weighted by the recording of voice and which can impact all the security and safety measures.

- COMPLEXITY OF COMPUTER SYSTEM

Any complication arising due to any of the transaction is advantaged by the cyber criminals who exploit the weakness in the system of internet and the technology.

- NEGLIGENCE OF NETWORK USERS

Human beings are prone to make mistakes. Any negligent act on the part of users gives enough chance to the hackers to achieve illegal or prohibited access to the computer system. The criminals are then able to steal or erase the data. Instances of this are with respect to the banks, government office, Multi-national corporations business firms, etc. who have hi-tech software which are easily accessible or not guarded against the hackers due to the negligent act of their workers or employees.

- LOSS OF EVIDENCE

The customary strategies for capacity, generation and different procedures of information have now been supplanted by the advanced procedure of PC and web innovation. The lacuna that web has to offer to the digital culprits to take part in crime without having any proof in material and

regardless of whether some proof is abandoned, is unreasonably conceivable and hence it becomes difficult to persuade the police that a crime has actually taken place on the computer

## 4. CATEGORISATION OF DELINQUENT AND SEVERE CRIMINALS

The criminals involved in the commission of the cyber crime constitute of various categories. This categorical division can be justified on the base of the object they had in their mind while committing such act. Cyber crime offenders can be classified in the following heads namely-

- AGE GROUP OF SIX YEARS TO 18 YEARS

This variant is included in the category of cyber criminalis because of careless behaviour pattern in children. This age group gets involved in these types of practice due to the peer groups, relatives and the curiosity to know about technology. The competitive nature of the children in academics can also be of the reason as they want to stand good in front of their peer and family group. Peer pressure or negative influence of computer and technology can also be the reason for the same.

- HABITUAL OFFENDERS AS HACKERS



These hackers come together and influence each other with a certain objective to be fulfilled

- PROFESSIONAL HACKERS

The major objective to do such crime is monetary gain. Certain organizations pay to these hackers for the data of their rivals so that they can compete with them in the overall market.These hackers also work for the police investigation which helps the police to get call logs, internet history,and location etc of the suspected person.

- DISCONTENDED EMPLOYEES

This includes the employees of any organisation who are not satisfied with their superior or the organisation and as a matter of revenge, they leak, steal or erase the data so as to cause harm to the reputation of the company's image.

## 5. LEGAL REGIME OF CYBER CRIME

IT Act[2] was enacted on 9th of June 2000, which is the first Act covering the arena of cyber space. Law relating to cyber laws revolves mainly around:

a. Cyber crimes
b. Electronic and digital signatures
c. Intellectual property
d. Data protection

IT Act was amended in 2008 to address the issues that the original Act failed to cover and to accommodate the further development of IT and related security concerns. The cyber laws inter alia covers some topics in the Indian penal Code[3], Intellectual Property Rights, The Indian Evidence[4] Act, Companies Act[5] and others as well still does not hold enough to cover the enormous ambit of cyber crimes.

Section 66A of the IT Act was added by the IT Act Amendment of 2008.This section deals with publishing of threatening, offensive or false information. Later this section was criticized for being in violation of Article 19 of the Indian Constitution regarding freedom of speech and expression. The exceptions to this Article is on grounds of: Defamation, incitement to crime, contempt of court public order decency morality friendly relations with neighbors, national security

Section 66A restricts freedom of speech and expression through electronic means i.e. over internet and other e-sources and in no case it is included even in the restrictions provided in Article 19 of the Indian Constitution. For instance, it punishes one for sending messages which cause annoyance or hurt the sentiments or knowing it to be wrong. There are many instances wherein these types of actions are perfectly valid over other forms of media like print. A print document

[2] The Information Technology Act, 2000 (Act 21 of 2000)
[3] The Indian Penal Code, 1860 (Act 45 of 1860)
[4] The Indian Evidence Act, 1872 (Act 1of 1872)
[5] The Companies Act, 2013 (Act 18 of 2013)

can be legally valid for the same but illegal in the electronic form. This shows the lacuna of IT Act in India where a person is not even free to express his views over the internet or electronic media.

Many petitions were filed which challenged the constitutionality of S.66.In one of the leading case of SHREYA SINGHAL V. UNION OF INDIA[6], the Supreme Court examined the Indian, English and US law on free discourse, struck down Section 66A of the Information Technology Act as it was over-expansive and ambiguous and violated Article 19(2)of the Constitution

## 6. CONFRONTATION OF CYBER CRIME IN INDIA

- **IS THE AVAILABLE CYBER KNOWLEDGE ENOUGH TO PERCIVE FUTURE PROBLEMS?**

➢ Is ITAct 2008 equipped for perceiving wrongdoings that we see each day in Cyber Space?

Cyber Crime is an emerging arena in the field of crime. Since technology is changing everyday so is the crime and the standards of criminals.Cyber crime needs to be generic in nature so that it includes the offences which may be added in the near future due to change in technology and other factors.The explanation of offences in the IT Act 2000 was more generic compared to the Amendment in 2008. The Section 66A (E-mail related offences), Section 66F (punishment for cyber terrorism i.e. imprisonment for life), Section 67B (exacting arrangement for Child Pornography), Section 66B (maintenance of stolen PC gadgets) have included an alternate view in the field of the digital wrongdoing. Sections 67, 67A alongside Section 66 permits security against profanity.

Section 43A and Section 72A have given importance to "Information Protection". Section 43 is currently connected with Section 66 and for the offences where there is disallowed access and which is hurtful to the PC framework and to the clients. Section 67C is a prevailing area that

[6]AIR 2015 SC 1523.

builds the duties of organizations and middle people and furthermore adds extraordinary forces to Section 65.

Sections 69,69A and 69B bolstered by Section 70B give tremendous forces to Government organizations to permit data security in the Cyber Space which incorporates families and private corporate division. Section 70 gives forces to control data security in the Government frameworks. Sections 71, 73 and 74 give insurance to the Digital Signature framework.66C and 66 D deal with the identity misuse which are done in the way of password theft or other sources.

- Are our Police receptive when a grievance is made?

Police officers are trained with certain degree of specialization in the arena of cyber crime but it not up to the extent that it is providing proper justice to the victims in the society. For this, there is a need for special cyber crime police station in every state or district where speedy justice can be provided at the beginning level of crime only. The mere existence of few cyber stations discourage the police to lodge FIR for the complaint relating to cyber crime.Therefore it requires a national level policy formulation for correcting the lacunas relating to police department in the area of cyber crime.



- Are we lacking expertise in the field of cyber law and cyber forensics?

When we connect the general rules and laws of the legal world with that of the cyber space, a variety ofdifferences and contradictions are seen in the field thus it becomes very important to subjectivelyanalyze the concept and this can be achieved through the specialized work of the cyber forensicresearch and departments.In order to attain maximum level of potential in governing the cyber laws it is very crucial for ourcountry to uplift the level of education regarding the awareness of cyber crimes and its laws. The samecan be attained through setting up of High school level conferences, awareness programs, activities forthe students to learn the basic of just and un-just in the cyber world.At the level of graduation, students shall be made to learn specific important laws that shall help inintroduction of safety measures in the cyber space.Further proper

education for Management and technical curriculum shall also be encouraged at basic as well as higher level.

## 7. CONCLUSION-A SPECULATIVE VIEW OF FUTURE

The digital technology has facilitated the advancement of the human civilized society. There is no set ofparticular codified rule to access the just and un-just, good or evil but the state through practice tries tomaintain a situation where practicable scenario can exist for human survival. A lack between thecontingencies that the government needs to consider is a must for analyzing the extent of crime thatcan be done through cyber space. The discussed Sections of the Act need not stand valid enough whilegoverning with the increased or advanced level of criminal minds in the cyber world.

Cyber crime has not just been an issue in the minds of law makers, but also concerns the administrators,government and local users. Internet has become a driving force for many criminal activities. Although, aset of work and attempts has been made to codify and procedure in the laws pertaining to cyber space, a major set of focus and work still needs to be done. The basic analysis of what the government is lacking in the control of cyber crime is to analyze a specificcode of direction which shall address all the contingencies of cyber crime. The team work of lawenforcers, the team of security controllers and a valid set of rules can help our country confine towardsbuilding a crime free society.