Legality of Cyber Crime in India: Definition, Trends and Incidents

Vishal Sharma

Student, Amity Law School Noida

Introduction

Cyber-crime involves network and computer as an object of crime. In modern era and advancement of technology there has been an uproar increase in cyber-crimes in India. These types of crimes came into picture only in the 21st century with advanced technology. It is important to understand that no crime can be committed by the technology itself and requires a human mind or people to do so. It is the people who misuse, corrupt information and not the machines. The implications of such crimes are on individuals, society, nation and even the mankind at large. Cybercrimes are mostly carried out by internal sources or people within the workforce. Other than the insiders the criminals in cybercrime include hackers, virus-writers, terrorist and foreign intelligence services, narcotics traffickers, etc. With the introduction of automobile the legislature and law makers were forced to come up with traffic rule and motor vehicle act in the late 20th century, similarly when new technology and electronics were introduced and people came to know about the internet the need for an act or law governing the activity on the internet and computers had to be devised. In the year of 2000, an act of the parliament the Information Technology Act,2000 was introduced. The act primarily deals with cybercrime and electronic commerce and other transactions over the web in India. In addition to this an amendment was brought into force in the year 2008 and the Information Technology Amendment Act,2008 came into force over the IT Act of 2000. The act also sought to promote security practices within India that would serve the country in a global context and picture. The amendment was brought into force to address the issues that the original bill failed to cover and to make way for further improved security related concerns since the original law passed. There have been issues and problems where by the law makers cannot cope up with the advancement of technology and make adequate laws for the protection and therefore with change and advanced technology there is also a need to have an amendment in the IT Act time to time. A space with no frontiers known as cyberspace has come into the picture with the invention of World Wide Web and interconnectivity of computers. This "space" lets the people interact from different corners of the world apart from other serious business. The near total dependence of banking , government activities, e-commerce activities on the networking is providing criminals with the increased opportunities to commit crime on the internet with far to imagine distress and disastrous effects. With the increase of every other activity over the internet the cyberspace has become very prone to cybercrime and has indeed become a serious threat to the information of the people.

What does Cyber Crime Includes?

When a crime is committed such as a data theft, viruses, logic bomb , internet fraud , publishing of Obscene matter , etc. on the cyberspace these amount to cybercrime and are classified based on nature and the purpose of the offence. According to UNO expert recommendations, the term "cybercrimes" covers any crime committed by using computer system and networks, within their frameworks or against them. These crimes are white-collar crimes and are committed by students or business rivals or people from the higher strata of the society who are educated enough and able to use computer and the internet. In order to define these crimes one should see to it that-

1. A computer is used in committing such a crime.
2. When the technology is responsible for the loss or gain of two individuals in one transaction.
3. When any person knowingly or intentionally accesses and without permission alters, destroys, deletes any data or takes copies of the data or causes disruption of computer services ,etc. , he is guilty of a computer crime.

It can be said that cybercrime is an act of commission or omission, committed on or through the usage of internet as a medium and carrying out an act which is prohibited by law and for which punishment is provided. Cybercrime have been classified on the basis of nature and purpose and have been broadly categorised into three, depending upon the victims of the crime. It may be against a person, any property or involving government functions:

1. Crimes against persons- cyber harassment, cyber stalking, murder threats, defamation fraud, cyber pornography, fraud , hate messages are all types of cybercrimes against a person and have a deep and wide impact on the health and safety of the person.
2. Crimes against property- software and hardware piracy , money laundering , commercial espionage, illegal hacking , commercial extortion, hacking, cracking, virus writing , transmission of worms, Trojan horses , denial of service attack, etc. can be put under this classification. The property herein referred can be physical as well as intangible.
3. Crimes against government- a cybercrime against the government is alarming these days and hence is a matter of concern as well. The example of attack on the Octagon of the U.S Government by the Hacker group Anonymous and the attack on the twin towers in Manhattan. More examples under this category include Cyber terrorism, threats or extortion or shut down of services of the government on the web.

Apart from the forms of cybercrimes discussed above there are various and different types of cybercrimes based on the extent and the scope. Amongst which some are defined and discussed below;

1. Data Leakage is committed by illegally copying the master file information of the computer for ransom, blackmailing or any other fraudulent purposes.
2. Data spying by a person on some sensitive information to which he has no authorisation and accesses the data from a home computer through a legitimate password. And the data accessed in that manner is then sold.
3. Trojan Attack also known as Trojan horse is an unauthorized program. It functions from inside a legitimate program and thereby concealing what it is actually doing. Trojan causes loss of data and files.
4. Cyber Defamation is any act, gesture, word in the cyberspace designed to harm a person's reputation on the internet or even outside it.
5. Credit Card Fraud is a lot of money of people are lost every year by consumers who have credit card and calling card numbers stolen from online databases.
6. Cyber stalking involves following the movement of a person's on the internet and by posting messages on the bulletin boards of the victim.

Present Trends of Cyber Crime in India

In 2014 general elections, BhartiyaJanta Party won the elections and came to run the government with one of its agenda being to make the country digital. They focused on Digital India to promote transactions in the cyberspace and to eliminate black money, but what the government forgot was to make the laws for cybercrime more rigid and by which they would have ensured more protection to the information and money of the citizens. In the year of 2014 the cybercrimes which were reported were about 9,622 which jumped to 11,592 in the year of 2015 after the launch of Digital India. The percentage variation in a single year was about 20%.The most number of cases under cyber-crimes were reported as per the 2016 Nation Crime Record Bureau in Uttar Pradesh (2,639 cases) (21.4%) followed by Maharashtra (2,380 cases) (19.3%) and Karnataka (1,101 cases) (8.9%) during 2016.During 2016, 48.6% of cyber-crime cases reported were for illegal gain (5,987 out of 12,317 cases) followed by revenge with 8.6% (1,056 cases) and insult to the modesty of women with 5.6% (686 cases).According to the Indian Computer Response Team a total number of 308 government websites were hacked in 2011 and there have been 62,189 incidents of cyber frauds till June 2014 according to the Home Ministry statistics. The digital India project

would only be a complete success if the project joins more and more people over the network with minimum cyber risks. Due to the poor results and a lot of increase in cybercrimes and hacking of sites in the recent years the project of digital India has been a failure according to my opinion. Although the plan of connecting more and more people and making the country technologically advanced was marvellous, only half percentage of the population of the country is so educated and advanced that they can carry out banking transactions online, or even less percentage of people who actually have the provision of internet. And to those who actually made their information digital ran a great chance of data theft and leakage. There were reports regularly in news wherein the data of the people given to the Unique Identification Authority of India for making aadhar card was leaked were circling around which made the citizens rather concerned about their data rather safe and ever since the inception of Aadhar , it has been in news regarding data theft. It was in Aadhar row that the landmark judgement of the Hon'ble Supreme court gave its decision that the Right to Privacy was a fundamental right[1]and that UIDAI should let the citizens know the usage of their information and how it is used. These reasons concern the public and make the project of Digital India an improper planned project.

Cyber Laws in India

Crimes that occur in the cyberspace in our country are governed by the Information Technology Act, 2000. The act for the very first time has defined cybercrimes and provided for penalties, punishments and compensation for hacking, unauthorized access to computer network, disruption of services, introducing computer viruses, etc. The IT Act also has a provision for penalties which goes up to Rs. 1 crore for damaging computer systems and three- year jail term with a fine of Rs. 2 lakhs for hackers. The act provided legal recognition to e-commerce, which means that contracts can be enforced, records can now be kept in an electronic form. After the act the digital signatures were given legal recognition. A special court is set up to take up cases concerning cybercrimes that is the Cyber Law Appellate Tribunal. The IT Act, 2000 is indeed a step forward and its provisions have the following positive aspect:

1. The positive aspect for the corporate sector is that digital signatures for carrying out their transactions online is legally valid .
2. Emails are now considered to be a valid and legal form of communication in our country, and which can be produced in the court of law.

[1] Justice K.S.Puttaswamy(Retd) v. Union Of India And Ors., (2017) 10 SCC 1.

3. For the companies, they will be able to carry out electronic commerce using the legal infrastructure provided under the IT Act, 2000.
4. After the act defined cybercrimes and levies penalties for the same, the corporate can now have relief as the penalty for damaging the computer system can go up to Rs. 1 crore.
5. The act enables the companies to file an application or other document with any office and authority in an electronic form, thereby saving time and wasting of manpower.
6. Under the Act the Cyber Law Appellate Tribunal has been set up which will take up exclusive cases concerning the authorities and involving cybercrimes.

In the year of 2008 the IT Act of 2000 was amended and replaced with the Information Technology Amendment Act,2008 and came into force after presidential assent in Feb 2009. The new amended act had more strict rules and emphasised on levying heavy penalties for crimes done in cyberspace. The new amended act become much more strict and had salient features like that of Section 43 under which the corporate body has a liability to control the sensitive personal data , section 66F which in specific talks about cyber terrorism and how it impacts at large and threatens the unity, section 66C which talks about dishonest use of somebody else's digital signature, punishable with imprisonment which may extend to 3 years and fine up to Rs. 1 Lakh, apart from these section 67B attempts to address the issue of child pornography .

The Amended IT Act has a lot of provisions safe guarding the information and to protect the data theft and penalises the wrong doer heavily. The IT Act looks after the cybercrimes in the country and the cases concerning the act are tried and heard by the Cyber Law Appellate Tribunal. The act is a great step and at a great time and there is no doubt that with such a huge population with advanced technology the act is an absolute necessary in the country today. But there is also a need to regular updating of the said act as the advancement of the technology is a lot faster in the modern era and to cope up with it the act needs to amended with time to time.

How to seek redressal for a Cyber Crime in India?

The Information Technology Act gives way or provides for the establishment of Cyber Appellate Tribunal(CAT), which would decide cases and appeals against the orders passed by the Controller and Adjudicating Officer. The tribunal will make speedy decisions as they will deal only with the provisions of the act. The central government by notification shall establish

one or more appellate tribunals to be known as Cyber Appellate Tribunal. The cases cannot be filed directly to CAT as it is an appellate tribunal and has appellate jurisdiction against the orders of the Controller and Adjudicating Officer. An original appeal or case may be filed with the Controller and Adjudicating Officer and the adjudicating officer has the power to award compensation to the affected person not exceeding rupees five crore. In furtherance to this an appeal shall lie against the order of the Controller or the adjudicating officer to a CAT having jurisdiction in the aforesaid matter or the concerned matter. The limitation period of filing appeal against the order of the controller or adjudicating officer.is forty – five days from the date on which the aggrieved party receives the copy of the order. CAT shall not be bound or limited by the Code of Civil Procedure, 1908. The tribunal is guided by the principles of natural justice. Normally one person may file one application but the tribunal may allow more people to join and file a single application if the cause of action is same and nature of relief prayed is same. Every application filed before the registration should be accompanied by a fee along with it of Rs. 2000/-.

Composition of Cyber Appellate Tribunal is the tribunal that shall consist of one chairperson and such members as the central government by notification in the official gazette may appoint. IT Act of 2000 had provided for one member commission but that is not the case in the amended act, which provides for multimember commission and an extensive and comprehensive selection procedure of the members.

Conclusion and Suggestions

The Information and Technology Act of 2000 was a great need at the time when the country was going through the phase of technological advancement and the law makers did a great job in coming up with the laws to govern activities on the cyberspace. But since neither the advancement of technology stopped nor was the act perfect to the utmost level with its penalties, the law makers had to come up with an amended IT Act in 2008. The act was much stricter and levied heavy penalties on wrong doer. The advancement of technology is never going to stop with such an advanced research on them similarly to tackle problems in the upcoming years and the problems relating data theft and loss that people are facing, the law makers have to keep the IT Act under a strict check and make changes time to time with change in technology. In the early 21st century the use of QR codes were almost nil whereas today QR codes apart from sharing data are used for transactions as well. Our country is amongst very few countries to have an altogether different Act for governing the activities on

the net. The act as of now has very well provided each detail and is serving its purpose rightly.