WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cybercrime and Legal Challenges before Cyber World

Koshika Karanwal

5th Year, B.B.A.L.L.B(Hons.), Law College Dehradun, Uttaranchal University

A B S T R A C T

As technology is increasing day by day, our life is mostly dependent on internet. The nature has gifted human being with mind and brain which distinguishes them from other creatures and make rules to make a man superior among other living. Technology advancements have provided quicker ways to communicate through instant messages, and social media platforms. Today we are living in an era where computer become part of our day- to- day life. On a positive note, the digital gadgets like smart phones and internet helps to communicate instantly and frequently from anywhere in the world. Now – a- days cybercrime is on the lips of the everyone involves in the use of the computer and the internet whether it would be an individual or the corporate organization. Today the major social problem is crime. As technology is increasingly rapidly, the cases of crimes are also increasing. Such few crimes are phishing, hacking, email spamming, web attacks, malware, identity theft etc. Cybercrime is challenge for our society, industry and also for enforcement agencies. As today's generation most people are using internet and computer, which makes it a motive to commit crimes and frauds. To control these types of crime some act is prepared in accordance with the increasing cases of cybercrime. Some acts are Information Technology Act, 2000, The Indian Penal Code, 1860 and The Indian Evidence Act, 1872 to deal with the cases of cybercrimes and if someone commit such offence, then they shall be punishable under such acts.

1 Introduction

Concept of Cyber Crime -

The major social and legal problem in the world we live is crime. As the technology is growing rapidly, the cases of crimes are also increasing due to extensive use of internet. With the increasing use of computers, cybercrime become has become a major issue. The offences which take place on or by using internet as a medium are known as cybercrimes. Crime means any act or omission that is punishable under the law. Crime means a legal wrong that can be followed by criminal proceedings which may result into punishment.

Thus, many writers have defined crime as an anti-social and immoral1[1].

According to Black stone- Crime is an act in violation of public law including public rights and duties.

According to Donald Taft- crime is a social injury and an expression of subjective opinion varying in time and place.

According to Austin- A wrong which is pursued by the sovereign or his subordinate is a crime (public wrong).

It means an illegal use of the computers and internet. Cybercrime means an' unlawful act wherein the computer is either a tool or a target'. Cybercrime refers to the criminal activities done by using the medium of communication technology components, the internet, cyber space. Cybercrime means an internet crime or illegal online activity committed on the internet by using internet as a medium. It includes from downloading illegal activities to stealing of information from online bank accounts. Cybercrime is defined as a genus is the conventional crime where the computer is an object or subject of the constituting crime or it may be both. It is a violation and breach of law on the internet as it is

[1] Prof. S. N. Mishra Indian Penal Code as Amended by The Criminal Law (Amendment) Act,2018

committed illegally. There is no exact definition of cybercrime in the It Act,2000. It has not been defined in any statues or law. Cybercrime is a crime that happens in cyberspace through computer and the internet. Cyberspace means virtual world created by mankind using computers where they interact and exchange information in different languages from one computer to another. "William Gibson", the science fiction writer created the word 'cyber' in his novel 'Neuromancer'.

Cybercrime means the "Offences that are committed against individuals or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as (SMS/MMS), chatrooms, email" etc[2] .

In the Indian context, Cybercrime is defined as the act or omission that adversely affect a person or property or a person computer system and it is punishable under Information Technology Act,2000 and liable for the consequences under the Indian Penal Code.

Cyber law refers to the law which deals with IT laws which referred as the law of the Internet. Cyber law designed to deal with the internet computing, cyberspace. Cyber law is the law governing computer and the internet technology. In today's world highly all are affected from digitalized world which has make dramatic changes in our lifestyle. It also creates a structure for e-commerce transactions and e- filling. To simply understand the cyber law meaning, it's a legal infrastructure which deals with cybercrimes.

Cyber law consists with the rules that how people and companies use the internet and computers. The prime need of cybercrime is to maintain the law and order during online activities. If somebody is found breaking the law, the firm / person can take action against that person and make them awarded a punishment.

2 Information Technology Law (Cyber Laws) p.466

The Cyber law Act 2000 came into consideration on 17th October 2000 3[3]which deals with e- commerce and cybercrimes. It is an important act because it deals with-

- It dictated all actions and reactions in cyberspace.
- It deals with all online transactions.
- It deals with all online activities which are watched by the cyber law officials.

Criminals take advantage of fast speed internet and perform various criminal activities. Cybercrime may differ from conventional crime. As conventional crime is an act committed in violation of law forbidding and for which punishment is imposed on conviction. Some conventional crime may also be cybercrime if they are committed through the medium of internet. Such crimes are theft, fraud, misrepresentation etc. which are punishable under Indian Penal Code. Cybercrime is committed by cyber criminals. Cyber criminals are the person who commits crime with an intention of causing harm to the person. Cyber Criminals can be motivated criminals, hackers, cyber terrorists. It is commits mostly to obtain profits. Cyber criminals are either individuals or group of individuals who uses technology to commit malicious activity on digital systems and networks with the intention of stealing information or personal data.

Now we talk about types of cybercrimes-

•Web Attacks-

It affects the computer via the internet. This type of viruses can be downloaded from internet and end up causing large scale and irreversible damages to your system.

•Malware-

It is an umbrella term for a code / program that is intentionally attack or affect the computer systems without the user's consent. It a software designed to destroy and damage computers and computer systems.

•Hacking-

It means an act committed by accessing your computer system without permission. It attempts to exploit a computer or a private network inside a computer. Hackers are the person who have basic knowledge and have an advanced understanding of computers.

[2] Information Technology Law (Cyber Laws) p.466
[3] [3]http://www.jigsawacademy.com.cdn.ampproject.org

•Phishing-

It is a method of gathering information using deceptive emails and websites. It is an attack which is used to steal personal credentials or credit card details as attackers pretend to be trusted individuals and trick into opening malicious links.

• **DDoS Attacks**- It attacks websites and online services.

Their aim is to overwhelm them with more traffic than the server or network can accommodate.

It targets a variety of resources from banks to new websites. They are carried out with the networks of internet connected machines.

•Identity Theft-

It occurs when someone uses another personal detail without their permission to commit fraud or other crimes. Once they access the information, they may use it to commit identity theft or sell it on a dark web.

•Cyber Defamation-

It means that publishing of false statement about an individual in cyberspace that can injure and harm the reputation of an individual. It means as the wrong which is done in either oral or written form to intentionally harm the reputation of a person in the society.

These are some of the crimes which I have discussed above. Now- a-days with the growing of digitalization, the internet crimes are also increasing at a faster pace. Now the crime can be committed from a distant location.

3 Historical Background of Cyber Crime

Cybercrime is one of the largest and targeted forms of crime. After all, the internet is available to everyone and that involves risks. Crime is committed via a computer or other devices which is connected through internet is dangerous because the identity of the perpetrator is difficult to find out. The computer invention was that people could not imagine. Before the computer is invented by "Thomas Watson", who was the former chairperson of IBM in 1943.

At the beginning of the 1970s, criminals regularly committed crimes via telephone lines an taking advantage of that, the attack was called 'phreaking'4[4]. They discovered that telephone system in America on the basic of certain tones. They were used these tones to make long distance calls. John Draper who was a well-known Phreaker, who tortured America to make use of public telephone systems to make free calls. Actually, there were no actual cybercrimes until 1980s.One person hacked another person's computer to find out, or copy or manipulate the data. The person who found guilty of cybercrime was Lan Murphy. Also, he was known as Captain Zap, which was happened in the year 1981. He hacked the America telephone company to manipulate its internal clock, so that users can still make use of free calls at peak times.

In 1986, Clifford Stall, who was administrator at the Lawrence Berkeley National Laboratory, who introduced the 'First Digital Forensic Technique' which was used to determine whether an unauthorized user had access to the system or not.

In 1986, Clifford Stall, who was administrator at the Lawrence Berkeley National Laboratory, who introduced the 'First Digital Forensic Technique' which was used to determine whether an unauthorized user had access to the system or not.

In 1988, the first worm was made that is Morris Worm, after its creator Robert Morris. While this worm was not originally intended to be malicious it is still caused a great deal of damage. In 1989, there was first ransomware attack which targeted the healthcare industry.

The U.S. Government Accountability Office in 1980 estimated that the damage could have been as high as 10,000,000.00. Ransomware is an attack that target some type of malicious software which locks user's data, until a small ransom is paid.

In this attack, an evolutionary biologist named Joseph Popp distributed 20,000 floppy disks across 90 countries. The attacks have evolved greatly over the years with the healthcare field still being a very large target.

In 90s the web browsers and e-mail, which meant to new tools for cybercriminals to exploit. Now Cybercriminals could transmit code over the internet in these new highly web browsers. Cybercriminals took what they have learned and taught and modified it as they operate with the internet, with devasting results.

[4] http://en.m.wikipedia.org

Cybercrime began to take off in early 2000's when social media came to life. The 2000s has brought us social media and saw the rise of identity theft. A website named 'Shadow Crew's' was launched for black hat hackers. This site has lasted for 2 years before being shut down by the secret service.

In 2011, Sony data exposes the records of over 100 million customers using their play station online services. In 2013, largest profile data was leaked, Edward Snowden revealed sensitive information which was stolen from several foreign governments.

In 2016, Tele Crypt ransomware appeared and it was downloaded while playing online games. It was created by researchers at Malwarebytes. In 2017, most of ransomware strains were managed to affect more than 200,000 windows computers in 150 countries. It is up to us to take the right safety measures to ensure it.

In 2020, 80% of the firms have seen an increase in cyberattacks. The damage related to cybercrime is approximately $6 trillion annually by 2021. In during the lockdown, people are accessing social media websites such as Instagram, Facebook etc. in addition to watching movies and series by subscribing to web channels such as Netflix, Amazon etc. or also indulge in online games by installing various applications. People tend to provide or give access their personal information which are available on their phones, social media accounts in order to use the services provided by that applications[5].

Therefore, it is essential to secure mobile devices, applications by installing anti -virus and make changes in the security settings to prevent data from being lost. Another side in the lockdown has been growing in demand is pornography.

4 Legislative safeguards against Cyber Crime:

The provisions against cybercrime in India are enumerated mainly within these statutes:

- The Information Technology Act, 2000
- Indian Penal Code,1860
- Evidence Act, 1872
- The Information Technology Act,2000-

With the start of 21st century, new communication medium or digital technology came into existence. This technology has the changed the human life. After that there was an increase in cyber offences. To control and tackle this new technology, the Information technology Act, 2000 came into force. This act is known as "The Information Technology Act, 2000".

Commencement- This Act came into force on 17th October 2000. President consent was given on 9th June 2000 and it was published in the Official Gazette on 9th June 2000 of Central Government.

Extent- It extent to whole of India, same as otherwise provided in this act. It applies to any offences or contravention thereunder committed outside India by any person.

It is a primary law which deals with the laws of cybercrime and e-commerce. This Act is based on the "United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January,1997"6[6]. The objective of the act is to carry lawful and trustworthy electronic and online transactions or to reduce cybercrimes. In order to attract the provisions of the act, the offences must involve computer, network and computer system. It deals with the legal validity of the electronic contracts and recognition of electronic signatures. It is done via electronic exchange of data and other transactions with electronic mode of communication.

The Information technology Act 2000, has 13 chapters and 90 sections in it. This is a modern legislation which makes ats like hacking, defamation, identity theft, cyber terrorism, a criminal offence. It amended the Indian Penal Code 1860, the Indian Evidence Act,1872 for the matter connected thereto.

Amendments brought in Information technology Act,2000

The Information technology Act ,2000 has brought amendments in four statues and these changes has been provided in schedule 1-4.

[5] http://www.lexology.com

[6] http://www.geeksforgeeks.org

- First Schedule- It deals with the amendments in the Indian Penal Code. It has widened the scope of the word 'document' to bring it with the ambit of electronic documents.
- Second Schedule- It deals with the amendment related to Evidence Act. It pertains to the inclusion of electronic document in the definition of evidence.
- Third Schedule- It deals with the amendment in Banker's Book Evidence Act. It includes printouts of data stored in floppy disk, tape or any other electronic form of storage.
- Fourth Schedule- It amends the Reserve Bank of India Act. It deals with the fund transfer through electronic means between the bank and other financial institutions.

A major amendment was made in year 2008, a section 66A was introduced which penalized sending of offensive messages. It also introduced section 69, which gave authorities the power of monitoring or decryption of any information. It includes sections which are as below-

- Sec- 43: Penalty for damage to computer, computer system.
- Sec -65: Tampering with computer source documents.
- Sec -66: Hacking with computer system
- Sec-67: Publishing of information which is obscene in electronic form
- Sec- 68: Power of the controller to give directions
- Sec- 69: Direction of controller to a subscriber to extend facilities to decrypt information
- Sec-70: Protected system
- Sec-71: Penalty for misrepresentation
- Sec- 72: Breach of confidentiality and privacy
- Sec- 73: Penalty for publishing Digital Signature Certificates false in certain particulars.
- Sec- 74: Publication for fraudulent purpose
- Sec- 75: Act to apply of the offence or contravention committed outside India.
- Sec- 76: Confiscation
- Sec- 77: Penalties and confiscation not to interfere with other punishments.
- Sec- 78: Power to investigate offences.

- **The Indian Evidence Act, 1872-**

This Act, has been amended in the manner specified in the Second Schedule of the Information Technology Act, 2000. This Act has been repeated by the Information Technology Act, 2008(10of 2009). This act has given new dimensions by introducing the various amendments in the Evidence Act,1872 and has been substituted with the words 'Electronic Record' and 'Digital Signature[7] '.

Information Technology Law (Cyber Law) p.491-

Electronic Evidence is like any kind of storage device like computers, CD's, DVD's, hard drives, digital cameras, fax machines and CCTV etc. Whether the evidence is physical evidence, electronic evidence, trace evidence, all evidence must be treated the same.

Section 3 of the Evidence Act, 1872 states "All documents produced for the inspection of the Court" was substituted by "All documents including electronic records produced for the inspection of the Court"[8].

Evidence is not only limited to only computers but may also extend to include evidences on digital devices such as telecommunication or electronic mediums.

This begins with the meaning of 'Electronic Evidence'. It deals with the type of evidence which is described as 'digital evidence' or 'computer evidence'. Digital Evidence tends to be more voluminous, more difficult, more difficult to destroy, easily modified, and easily duplicated and more readily available9[9]. In order to prove the contents of a document, either it is primary or secondary evidence, it must be offered.

[7] Information Technology Law (Cyber Law) p.491

[8] The Indian Evidence Act has been amended by virtue of section 92 of Information Technology Act, 2000

Cybercrimes are committed in cyberspace. Evidences in these crimes is almost / always recorded in a digital form. Evidences from tech devices continues to play an important role in the search for justice.

Sec – 2 (t) of the IT Act,2000 defines "Electronic Record": means data, record or data generated, image, sound stored, received in an electronic form or computer form.

After incorporation of these amendments, the concerned amended sections are as follows:

- Sec -3: Evidence
- Sec -17: Admission
- Sec -22A: when oral admissions as to contents of electronic records are relevant
- Sec- 34: Entries in books of account including those maintained in an electronic form with relevant
- Sec – 35: Relevancy of entry in public records
- Sec – 39: when statement forms part of conversation, document, electronic record, book or letters.
- Sec – 47A: Opinion as to digital signature when relevant
- Sec – 65A: special provisions evidence relating to electronic record Sec – 65B: Admissibility of electronic record
- Sec – 73A: proof as to verification of digital signature
- Sec – 81A Presumption to Gazettes in electronic form
- Sec – 85A Presumption as to electronic agreements
- Sec – 85B: Presumption as to electronic records and digital signature
- Sec- 85C: Presumption as to digital signature certificate
- Sec- 88A: presumption as to electronic messages
- Sec – 90A: presumption as to electronic records five years old
- Sec – 131: production of documents or electronic records which another person having possession, could refuse to produce.

Indian Penal Code ,1860 –

The Indian Penal Code,1860 not originally meant to deal with the cybercrimes, and has been adopted to deal with the advent of new crimes. It was amended to include the term 'electronic'. Interestingly IPC deals with many of the cybercrimes which are penalized by the

IT Act. Apart from punishments in the IT Act, certain crimes are attracted by IPC provisions as well.

The provision of section 378 of IPC would be correspondence to section 43 & 66 of the It acts. Section 378 of the IPC deals with "Theft" of movable property, would refer to the theft of any data online or otherwise. The statutory punishment of theft under section 378 of the IPC is three years in prison or a fine.

Section 424 & 425 of the IPC deals with damaging the computer systems and data theft or it also denies access to computer systems.

Section 411 of the IPC prescribes' the receipt of stolen property'.

Section 415 of the IPC deals with 'Cheating'. It means an offence under which a person induces another person to deliver the property or commission of an offence with the intention of deceiving the person.

The provisions under section 463,465,468 of the IPC deals with forgery for the purpose of cheating and can be similarly used as to deal with the cases of identity theft.

Section 469 of the IPC-

[9] http://www.likenndin.com/pulse/electronic-evidence-cyberlaw-india

It deals with whoever commits forgery intending that the document or electronic record forged, shall harm the reputation of any party, or he is likely to use it for any purpose.

Section 470 of the IPC-

A false document or electronic record made wholly or in part by forgery is designated a 'forged document or electronic record'.

Section 471of the IPC-

If any person fraudulently or dishonestly uses as genuine any10[10](document or electronic record) which he knows or has reason to be forged.

Section 474 of the IPC-

If any person who has possession on any document or electronic record and knowing the same to be forged and intending that the same shall be fraudulently or dishonestly used as genuine, shall if the document or electronic record is one which is mentioned in section 466 of the said code. And if the document is in the description of section 467 of the said code, then it shall be punished with (imprisonment for life)[11] or with imprisonment for a term which may extent to seven years, and shall also be liable to fine.

Section 477 of the IPC-

If someone fraudulently or dishonestly with the intention of causing damage or injury to public, or to any person or cancel or destroys or attempt to destroy any document which purports to be a will, or an authority to adopt a son, or any valuable security, or commits any mischief with such documents.

Section 477 A of the IPC-

If a person being a clerk, officer, servant or employed or acting in the capacity of clerk, officer, willfully and with the intention to destroy, defraud, alters or manipulates any book,electronic or valuable security or account which belongs to or in possession of his employer, or has been received by him or on behalf of employer with the intention to defraud, destroy or abets the making of false entry particular in book, electronic record or valuable security.

5 Legal Challenges before Cyber World:

Sometimes we often think how wired we all are connected with each other. Almost everything in our life is connected with some technologies and gadgets. He ca snap down all our connections and turn us into Stone Age[12]. To fight against this war our Criminal Justice System should be alert.

Cybercrime is the new challenge for our Indian society, industry and also for law enforcement agencies. The nature of internet is anonymous which makes it an attractive medium to commit crimes and frauds[13].

In present position the cybercrime is growing to an extend as more and more people using are using the internet for their various purposes.
This type of dynamic environment of cybercrimes gives a hard challenge for security researchers to protect their data and information on the internet from various types of cyberattacks[14].

[10] Subs. By Act 21 of 2000, sec.91 and Sch. I, for 'document' (w.e.f. 17-10-2000

[11] Subs. By act 26 of 1955, sec.117 and Sch., for 'transportation for life '(w.e.f. 1-1-1956).

[12] See: The New Indian Express,21/06/2008. P.8

[13] Available at http://www.indiacycyberlab.in/knw_more/copawards2005-message.htm

[14] A survey on wireless security: technical challenges, recent advances and future trends.vol.104, no.9, pp.1727-1765, 2016

In present stage, Government and private sectors have offered an opportunity to its employees to connect from anywhere by developing the internet -based networks.

It is a challenge for security professionals to provide security from cybercriminals to the corporate or government sectors.

There is lack of awareness amongst the individuals or the organization about the culture of the cyber security.

The extensive use of mobile phones has widened the ecosystem and it a pose to new challenges for cyber across the world. With increasing mobile crimes, it becomes necessity to meet the legal challenges emerging with the mobiles.

The cyber security incidents and the attacks on networks are increasing which leads to breach of cyber security and likely to impact on the nation.

The mandatory provisions which help in preservation and promotion of cyber security in use of computers and communication devices.

Therefore, there should be a single technique that should protect all the layers of crimes from various known and unknown cyberattack.

4 Judicial Cases-

1. AVNISH BAJAJ V. STATE (N.C.T) DELHI[15]:

In this case CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was sold on the websites. The CD was also being sold in Delhi market. Later the burden was on the accused that he was a service provider but not the content writer. The CEO was arrested under section 67 of the Information Technology Act,2000 and his bail application were rejected by the trial court. to the CEO subject to furnishing two securities of Rs.1 lakh each.

2. PUNE CITIBANK MPHASIS CALL CENTRE FRAUD:

In this case, some ex-employees of BPO arm of Mphasis company defrauded the US customers of Citibank of Rs 1.5 crores. It is one of the cybercrimes which raised the concept of 'Data Protection '. It was committed with unauthorized access with the electronic account space. Since IPC is related with the use of electronic documents which can be considered as crime like cheating and conspiracy. So, under IT Act, the offences in under section 66 and 43 of the IT Act. The accused is charged under section 420, 425, 467 and 471 of the IPC. Accordingly, the penalty is given which is imprisonment up to 1 crore and also liable to pay damages.

3. PLAYBOY ENTERPRISES V. FRENE[16]:

In this case, the defendant has operated a subscription electronic bulletin board which was downloaded the unauthorized copyrighted photographs of the plaintiff. The court held that the unauthorized uploading of the photographs by the defendant knowing that they could be downloaded by the subscriber's which amount to distribution.

5 Conclusion:

The role of internet is increasing rapidly. It has done convenient for the consumers as everything can be done through by staying at home. With increasing in technology, criminals don't have to rob banks, nor they have to be outside in order to commit any crime.

It is easy to commit without any physical existence in global nature and due to this it become a challenge and risk to the crime fighter. Now-a-days their weapons are not gun, now they attack with mouse cursors and passwords. To avoid the information from hackers we secretly use passwords and change regularly. With the advancement of IT. Act,2000, the issue of crimes in cyberspace in India has been addressed very smartly but the proper implementation is still lacking. As the technology develops, the laws need to develop to detect who abuse and misuse the technology. We can therefore conclude that cyber law knowledge is the need of the person working with the computers, computer system and computer network and technology since these laws cover the aspects of information technology and ignorance of law is no excuse in the eyes of law. The Government of India in recent years have taken many measures to check cybercrimes and also enact legislations to deal with the any violation of the cybercrimes.

[15] Delhi on 21 December,2004 (2005) 3CompLJ364Del,116 (2005) DLT427

[16] 839 FSupp.152(M.D.Fla.1993).