VOLUME 21 ISSN 2456-9704

CYBER CRIMES IN CORPORATE WORLD

By Muskaan Bindra
From Amity Law School, Noida

ABSTRACT

In today's era, the pace of technological development is increasing. The people have turned completely dependent on the internet. It has turned into a necessity in human lives. The more the usage, the more is its development. But the question is, IS THIS DEVELOPMENT AN OPPORTUNITY OR A THREAT?

The Internet has made it easier for people to connect, but every coin has two sides. So does the internet. With the growth of it, there are some drawbacks such as cyber defamation, cyberbullying, fraud, cyberstalking, phishing scams, and many more. This article aims to provide an insight into those crimes that are taking place over the internet and effecting lives of many, laying major emphasis on Cyber Defamation.

Keywords:
Cyber-crime, Cyber Defamation, Internet, Computer, Technology.

INTRODUCTION

"All I know is that the internet will transform the world" – Alfred D. Chandler, Jr.

The internet has drastically changed the lives of people. In this technology-driven society, people are severely addicted to the internet. Gone are those days, where people use to go out to shop and stand in a long queue for billing. The Internet has made it all so smooth and simple. It connects people all over the world, is easy to use and economical. But, it can pose some threats which can have a derogatory impact on the people.

Cyber Crime as the name suggests is the crime related to the internet. Cyber Crime is a very dangerous crime that involves usage of computers or other digital devices, in which such device can be either the tool of crime or the target or it may even be the evidence of the crime. The cyber-world in itself has a virtual reality where anyone can fake or hide their identity. Initially, such acts were committed mainly by individuals or other small groups. But as technology is advancing, there can be seen a rise in the activities. These small groups have turned into highly complex cybercriminal networks and have become a major threat today.[1] Cyber Crimes is emerging as a serious threat to society. This crime has expanded its roots to almost every aspect of the life of a cyber surfer. Cyber Crime is a very comprehensive term and thence cannot be explained in just a few sentences. If we take a look at the nature of these crimes, we can simply say that these types of crimes are rapidly increasing due to our dependency on the internet, even for the most basic activities such as shopping groceries, ordering food, buying tickets, making payments, etc. Where there are such uncontrollable

[1] Rajat Singh, CYBER CRIME AND TERRORISM , Legal Service India, August 20, 2020 10:30 am http://www.legalserviceindia.com/legal/article-2436-cyber-crime-and-terrorism.html

dependencies people are definitely going to take the advantage of the situation.

We come across contrasting cyber-crime cases being committed on a daily basis all over the world through newspapers, televisions and journals. It is very important to educate people and make them aware of these crimes so that they can safeguard themselves from being a victim. There are different types of crimes taking place over the internet. Some of them are Hacking and Unauthorized access, Phishing, Cyber Defamation, Pornography, Cyber Terrorism and many more.

CHAPTER: 1 CYBER-CRIME AND ITS CLASSIFICATIONS

1. HISTORY OF CYBER-CRIME

Computer networking was evolved in the 1990s. Since then Hacking was the most famous method opted to attain information about the systems. They aimed at breaking through the broken software in order to attain information. Hackers, in order to win the race against one another and become the best hacker, caused harm to many networks. They left no networks unharmed, right from commercial organizations to military to social media platforms. Initially, these attempts were brushed off as mere nuisance as they did not cause any long term threats. But later, this hacking software's turned more harmful, making the network systems slow. With the passage of time, hackers became more skilful, they started using their knowledge and expertise to gain benefit from victimizing and exploiting others.[2]

2. DEFINITION OF CYBER-CRIME

Cyber Crime is any criminal activity taking place over the internet or by using other technologies as recognized by the Information Technology Act, 2000.

"Cyber Crimes means any criminal or other offences that's facilitated by or involves the utilization of electronic media or information systems, including any device or the web or any one or more of them."[3]

The Indian Legislature does not provide the exact definition for Cyber Crime

The internet has been successful in bringing the world closer but it has also managed to create problems for people who spend long hours browsing the internet. The law enforcement agencies are trying their very best to tackle this problem, but this issue is growing rapidly and many people have become victims of such crimes. One of the ways to avoid being a victim of cyber-crimes and protecting the sensitive information stored in your computers is by using impenetrable security system software's that use a unified system of hardware and software to authenticate the information that is sent or accessed over the internet.

3. NATURE AND SCOPE OF CYBER-CRIME

Crime is an activity connected to the society which cannot be eradicated in true sense.

[2] CYBER CRIME, Cross Domain Solutions , August 18 , 2020 12:00 pm http://www.crossdomainsolutions.com/cyber-crime/

[3] SA LAW- Electronic Communications and Transactions Amendment Bill,2012 , Cybercrime.org.za , 18,2020 12:40pm http://cybercrime.org.za/definition

We cannot think of or experience a society without cyber-crimes. The nature and the scope of cyber-crime vary from society to society. Thinking of building a crime-free society is a myth. Crime cannot be segregated from society.

The nature of the crime is dependent on the nature of society. The complexity of crime is determined by the complexity of society. In order to reach to the root of a crime, it is very essential to understand the factors influencing and contributing to the crime.

Computers have been a boon to society. They have transformed society in the last few decades. It has made things convenient. The modern technology has put an end to the barriers of space and time. But, it is also a bane to society. The jurisdictional issue has been a major hindrance while determining the transnational transaction over the internet. The courts face a lot of difficulties when subjected to the questions pertaining to jurisdiction. Certain cyber-crimes are very difficult to trace as the location is unknown and so the local machinery is unable to solve the crimes of such nature. Thence, the global dimension of the cyber-crime has made it difficult for law enforcement to handle and deal with it. Our knowledge and regulation of such crimes cannot be national but has to be international. It is important to enact laws and preventive, defence mechanisms globally, in order to protect society from this evil.

4. CHARACTERISTICS OF CYBER-CRIME

As stated earlier, the nature of cyber-crime is quite different from traditional crimes. Due to the advancement of Internet Technology, such crimes have gained serious attention. So, it is necessary to critically examine the characteristics of cyber-crimes:

4.1. SPECIALIZED KNOWLEDGE: Cyber-Crimes are committed through digital platforms and technology. Thus, in order to commit crimes of such kinds, one has to be very skilled and needs specialized knowledge in computer and internet. Such people need a deep understanding of the usability of the internet.

4.2. GEOGRAPHICAL CHALLENGES: The cyber-crimes take place over the internet, reducing the geographical challenges or boundaries to zero. A cyber-criminal can commit the crime in no time sitting in any part of the world. For example, a hacker from India hacking the system in the United States.

4.3. EVIDENCE COLLECTION: When it comes to cyber-crimes it becomes very difficult to collect evidence and prove them in court due to the nature of the crime. The criminal attempting the crime invokes jurisdictions of several countries while performing the malicious activity and at the same time he is sitting at some safe untraceable place.

4.4. MAGNITUDE: The magnitude of such crimes is unimaginable. Cyber-crimes can cause injury/ harm or loss of life to an extent which cannot be imagined. These crimes can destroy the websites or steal data of the companies in no time.

5. CATEGORIES OF CYBERCRIME

Cyber-crimes are categorized into the following three categories:[4]

5.1. Crime against Individual
5.2. Crime against Property
5.3. Crime against Government

INDIVIDUAL: The crimes against individuals include cyber-stalking, distribution of pornography, cyber defamation, trafficking. The legal departments take such crimes very seriously and laws are being amended from time to time to tackle such criminal activities.

PROPERTY: In the cyberspace, the criminals try to steal or rob one's bank details, or misuse the credit card to make numerous online purchases, or to use malicious software to gain access to one's website and disrupt the system of organization, thus causing harm to the property.

GOVERNMENT: The crimes against the government are termed as cyber terrorism. The criminals try to cause panic amongst civilization. They hack government or military websites and transfer information causing riots.

6. ***CLASSIFICATION OF CYBER-CRIME***

6.1. CYBER DEFAMATION: The tort of cyber defamation is an "act of intentionally insulting, defaming or offending another individual or a party through a virtual medium. It can be both written and oral. Cyber Defamation is one of the worst forms of cyber-crime which takes into its ambit all parts of life and endangers /causes damages upon the institution and individual's name and fame."[5]

6.2. CYBER PORNOGRAPHY: Cyber Pornography is defined as "the act of using cyberspace to create, display, import or publish pornography or obscene materials. With the advancement of cyberspace, the digital pornographic content has now replaced the traditional pornographic content."[6] The advanced technology has made it very easier for such criminals to create and distribute through the internet.

6.3. CYBER STALKING: The term stalking means harassing or threatening the other person. In layman's language, cyber-stalking is a physical form of stalking which is committed over the internet. E-mails, chat rooms, WhatsApp groups, and other platforms are being used to stalk the other person. The Wikipedia defines Cyber Stalking as a crime "where the Internet or other electronic means are used to harass an individual or to stalk him/her, a group of individuals, or an organization. It includes the making of false accusation or statements of facts (defamation), monitoring, making threats, damage to data or equipment, the solicitations of an under-aged child for sex, or gathering sensitive information that may be used to harass."[7]

[4]CYBER CRIME, Cross Domain Solutions , August 20 , 2020 2:30 pm http://www.crossdomainsolutions.com/cyber-crime/

[5] MILLER COLLINS, THE LAW OF DEFAMATION

[6] Gorman, L. and Maclean, D. Media and Society in Twentieth Century, Blackwell publishing, 2003.

[7] Cyberstalking, Wikipedia, August 20,202 4:30pm https://en.wikipedia.org/wiki/Cyberstalking

6.4. CYBER TERRORISM: According to NATO (2008), cyber terrorism is "a cyber-attack which is attempted by using or exploiting computers or communication networks to cause sufficient harm to induce fear or intimidate a society into an ideological goal."[8] Cyber Terrorism has become a threat to the global population as through this; the terrorists are spreading fake propaganda in line with political and religious ideologies.

6.5. HACKING: Hacking is considered as one of the most serious cyber-crimes. It is a criminal trespass into a computer (that is private property). Unauthorized entry into another's computer is termed hacking. The term Criminal trespass means "entering into someone else's property with intent to insult or commit an offence, annoy any person in possession of the property, by unlawfully remaining there with the intent thereby to intimidate, commit an offence, annoy or insult any such person."[9]

6.6. VIRUS: Such crimes involve direct or unauthorized search access to the system by introducing malicious programs known as viruses. The IT ACT, 2000 under section 43-C, section 66 and section 268 of Indian Penal Code provides provisions for such crimes.

6.7. PHISHING: Phishing is "a form of social engineering, characterized by attempts made by someone to fraudulently acquire sensitive information stored in the computers or saved on the internet, such as credit card details, CVV, passwords, by impersonating as a trustworthy person through emails or an instant message."[10]

6.8. CYBER CRIMES RELATED INTELLECTUAL PROPERTY: The cyber-crimes related to intellectual property means causing harm or stealing of copyrights, patents, trademarks or trade secrets using the internet and computers. Copyrights and trade secrets are the two form of intellectual property those us frequently stolen.[11]

7. CAUSES OF CYBER-CRIME

Whenever you find an opportunity with low risk, you're bound to find people who are willing to take advantage of the situation. For example High rate of return on investments with low risk. This is what happens in cases of cyber-crime. Accessing personal data and sensitive information results in a rich harvest of returns and catching such criminals is difficult. This is the reason that cyber-crime is rapidly spreading its roots across the world. Internet networks are vulnerable, so they require strict laws to protect and safeguard them against cybercriminals. The computers are easy to access, hackers easily steal the access codes, advanced voice recorders or the retina images, etc. that fool the biometric systems to get past the security systems. The computers have data saved in small storages and it becomes a lot easier to steal data from such small spaces. The operating systems on which a computer runs are programed of millions of codes.

[8] NATO, (2008). Cyber defense concept MC0571. Brussels, Belgium

[9] Indian Penal Code, 1860., s. 441

[10] Lance James, "Phishing Exposed", Elsevier 2005.

[11] Intellectual Property Theft, Cyber Crime , August 22, 2020 7:30pmhttp://law.jrank.org/pages/11992/Cyber-Crime-Intellectual-property-theft.html (as on 22 August 2020.)

The cybercriminals take advantages of the gaps and fulfil their agenda.

CHAPTER: 2
CYBER DEFAMATION

"The internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had."- Eric Schmidt

The term defamation means wrongful and intentional publication of something either orally or in writing about a person to harm his goodwill/reputation in the society.

The technological development has made things easier for us. Things have become a piece of cake for all of us. But everything that is easily available has some pitfalls. These facilities may sometimes lead to misuse. Cyber Defamation is one of the worst forms of cyber-crimes which takes into its ambit all the walks of life and endangers, causes damages upon institutions and individuals' goodwill, to a larger extent. The users can publish and disseminate information through social media which causes great harm to one's existence. Defamation has become a subject of major concern. With the rise in the cases of attempt to share or post information on certain social networking sites and commenting on them with the motive of insulting the other person has increased the risk of Cyber Defamation.

The term defamation is defined under section 499 of the Indian Penal Code as "Any individual who in writing or spoken, gestures or signs publishes any imputation on any person with an intention to harm the reputation of that person. The person making such statement should have knowledge or reason to believe that such publication will ruin the reputation of the person"[12]

In other words, Cyber defamation means publication of false information about an individual or institution in cyberspace that has the ability to injure or demean the reputation of that individual. Cyber defamation can also be termed as internet defamation or online defamation as it is defamation in the world of technological development, internet and its users.

Today, the internet has turned into a platform where people are given the opportunity to share their opinions on various matters globally. One can easily post something and it can go viral within minutes. This opinion of theirs can be insulting, defaming or offending. For instance, an angry employee of a company posts some defamatory remarks about the company on a popular platform or sends slanderous emails, defaming the company or its management to the clients across the globe, causing huge damage to the company in a very short span of time. Taking into consideration, the recent Gurugram Suicide case, a 12th class boy commits suicide, when a girl posted an Instagram story, accusing him of rape. She posted this statement without proper evidence and people started supporting the girl. The court of Instagram pronounced the boy guilty. This social media law society cost that boy his life. The sad part is that people forget the difference between opinions and facts.

Removing barriers to freedom of interactions has given unfettered

[12] Indian Penal Code,1860

capabilities, to people who pot false statements on social networking sites, thereby damaging their reputation. Such an act, though popularly known as "trolls", actually amount to defamation.[13]

1. WHEN CAN A STATEMENT BE CONSIDERED AS DEFAMATORY?

A statement will be considered as defamatory if the following essential elements are fulfilled:

- There must be a *publication of the defamatory statement:* The term publication here means that it comes to the knowledge of a third party. In other words, when somebody else reads the defamatory statement referred to the plaintiff, there will be a valid publication. In the case of Mahendra Ram v/s Harnandan Prasad,[14] the defendant sent a defamatory letter to the plaintiff written in Urdu, knowing the fact that the plaintiff didn't know Urdu and the letter will very likely be read by some other person. The court held the defendant liable.

- The statement must *refer only to the plaintiff:* In a case for defamation, the burden to prove the statement is on the plaintiff. If he succeeds in proving the statement made against him, the defendant will then be held liable. In the case of T.V. Ramasubba Iyer And Anr. v/s A.M. Ahamed Mohideen[15] the statement stated that a particular person carrying business of Agarbati's to Ceylon has been arrested for the offence of smuggling. The plaintiff was the only person in that particular region carrying such business and thus, his reputation was damaged. The court held the defendant liable.

- The statement must be *defamatory in nature:* This is the first essential of the offence of defamation. Until the statement is not known to the public at large and tends to lower the reputation of the party, it cannot be considered as a defamatory statement. In the case of Ram Jethmalani v/s Subramanian Swamy,[16] the court held S.Swamy liable for defaming the plaintiff Ram Jethmalani by stating that he received money from a banned organization in order to protect the CM of Tamil Nadu in case of the assassination of Rajiv Gandhi.

2. WHAT ARE THE DIFFERENT FORMS OF DEFAMATION?

Before the advancement in technology, there were only two types of communications – spoken and written. Slander means spoken defamation and libel means written defamation. It depends on the judge, in a defamation case to decide the category a statement fits into.

Defamation can be divided into two categories. Those are:

LIBEL: A statement that is defamatory in nature and is published in a written form. For example: Defaming a person through a representation made in permanent form like

[13]Meril Mathew Joy and Shubham Raj , DEFAMATION ON SOCIAL MEDIA – WHAT CAN YOU DO ABOUT IY? , Lexology, September 07,2020 , 12:30 pm https://www.lexology.com/library/detail.aspx?g=d3075f4d-afb5-4920-bf59-26cf5d054ab8#:~:text=Defamation%20has%20been%20defined%20under,believe%20that%20such%20imputation%20will

[14] AIR 1958 Pat 4

[15] AIR 1972 Mad 398

[16]AIR 2006 Delhi 300, 126 (2006) DLT 535

printing, writing. If the statement is a libel, the plaintiff needs to prove that-

- ❖ The statement by the defendant was defamatory in nature.
- ❖ The statement was published.

No other requirements are to be fulfilled as the law presumes that once the publication is in writing and available to the public at large, it would continue to cause damage to the business for a long term.

SLANDER: A defamation statement in verbal form. For example: Defaming a person by the way of gestures or words. Slander is further divided into two categories- *slander and slander per se.* In the first kind, the burden is on the plaintiff to prove the defendant made a defamatory statement and the plaintiff suffered harm due to such published statement. The term slander per se does not require the plaintiff to prove the actual harm or special damages. Slander per se involves categories of defamatory statements that are presumed to be damaging in nature. Some common slander per se categories are:

- ❖ Imputing criminal conduct to the plaintiff
- ❖ Stating that the plaintiff is suffering from some communicable disease
- ❖ Any harmful statement about the plaintiff's profession.

3. HOW IS CYBER DEFAMATION DIFFERENT FROM PHYSICAL DEFAMATION?

A mere defamatory statement cannot be categorized as defamation. The statement should be published to amount to defamation. Cyber defamation transpires when a desktop connected to the internet is used as a medium or tool to demean or injure one's reputation. For instance, publishing a defamation statement against someone on social networking sites such as Instagram, Facebook, Twitter, etc. or sending emails containing defamatory content about a person with the motive of injuring one's reputation. Given the wide range covered by the internet and the rate of dissemination of information on social networking platforms, it becomes very difficult to ascertain the extent of damage caused in terms of money.

The medium through which such an act is committed is the internet, which means this act is committed in the digital world, but the law of defamation applies the same. The liability regarding cyber defamation lies on:

- ❖ The author of the defamatory material published online ;
- ❖ The service provider or an intermediary. However, as per section 79 of the Information Technology Act, 2000, it is important to understand that an intermediary shall not be liable if it does not initiate or modifies such defamatory content but merely acts as a facilitator. This protection provided to the intermediary is subject to the condition that he shall comply with guidelines stated by the government and function with due diligence. The intermediary should also remove any unlawful content on being notified by the agencies or on receiving actual knowledge about the same.

The ease with which people defame others by using social networking platforms, mobile phones, laptops and computers, hiding their identities and settling scores by defaming the other person has become a serious problem. This requires an urgent

need to amend the legal provisions to bring remedy to those who suffer.

4. WHERE TO LODGE A COMPLAINT ABOUT CYBER-DEFAMATION?

The aggrieved party can file a complaint to the Cyber Crime Investigation Cell. The Cyber Crime Investigation Cell is a brand of the Criminal Investigation Department. These departments deal with the offences related to the computer, Internet, Computer networks, computer devices, etc.

5. DEFENCES AVAILABLE IN DEFAMATION SUIT

- **Defence of Justification of Truth:** The party held can plead with a complete defence in civil proceedings the truth of a defamatory statement. A publication based on verifiable facts can extinguish the liability for defamation. It negates the charge of malice and thus, the plaintiff is not entitled to recover damages.

- **Defence of Absolute privilege:** The term "privilege" means that a person stands in such a position to the facts that he is justified in saying or writing anything which might amount to libel or slander is made by anyone else. The general rule of this defence is the common convenience and welfare of the society or to safeguard the interest of the society.

- **Defence of fair comment:** A fair and bona fide comment on a matter of public interest does not amount to libel. The defence of fair comment on the matter of public interest is made available only if the matters in question ha legitimate public interests, directly or indirectly, locally or nationally.

- **Consent:** When the defendant has published the material with the consent of the plaintiff or the plaintiff himself invited the defendant to repeat the defamatory word, the defendant can plead the defence of consent.

- **Apology:** Apology is available as a defence in actions for libel if the publication is made in newspapers and the newspaper displays a sufficient apology and adheres to certain other conditions. When there are an apology and an acceptance, the defendant can resist the plaintiff's suit for reimbursement for defamation.

CHAPTER: 3

LEADING JUDICIAL PRONOUNCEMENT WITH RESPECT TO CYBER DEFAMATION IN CORPORATE WORLD

Cyber defamation has become a serious issue due to its aftermath surfacing from the wide-spread coverage, anonymity, impersonation and instantaneous communication. The impacts of such activities can be aggravated by fake videos, morphing, the manipulations that have become so easy due to the use of advanced technology and artificial intelligence, which also makes their detection difficult.

India's first cyber defamation case came into light in the year 2001. *SMC Pneumatics India Pvt. Ltd. (plaintiff) V/s Jogesh Kwatra*

(defendant) [17] was the first case in a court of Delhi over a matter where a corporate firm's reputation was being defamed through emails.

The case was instituted on 22nd June 2001 in the Delhi district court.[18] The decision for the case was announced on 12th February 2014.

FACTS:

Abusive, embarrassing, vulgar, humiliating and defamatory emails were received by the plaintiff. The plaintiff with the help of a computer expert traced one of the e-ails received on 2nd April 2001. The emails were traced back to the cyber cafe located in New Delhi. The owner of the cyber cafe was enquired and with the help of a photograph put forward by the plaintiff he identified the defendant as the same person who sent the mail.

The emails were forwarded to the higher officials of different levels of the SMC worldwide. The mails were sent through the sales department especially to Australia to defame the plaintiff who was a very educated and hardworking person. There could be seen as a clear intention and mens-rea to defame the plaintiff in the eyes of people who hold him in high esteem. Copies of the emails were sent to the group companies Managing Directors. Regard the same a police complaint was filed by the plaintiff on 11th May 2001 which stood pending for proceedings due to the uncertainty of the criminal jurisdiction to which it pertains. The plaintiff on the same day terminated the services of the defendant on account of his act and violation of the rules stated in the appointment letter. The suit was filed a seeking perpetual injunction against the defendant.

Written Statement was filed by the defendant who stated that the allegations levelled by the plaintiff are false and the plaintiff has no evidence proving his statements. The defendant in his statement mentioned that the information provided by the plaintiff regarding the path followed by the mails from the originating server to the destination server, the contact number used to connect to the originating server and the number dialed to connect to the originating server, the time of sending of the alleged mails, is incomplete. In absence of all the above-stated information regarding the three emails, the defendant cannot be connected to the complaint filed against him. The defendant in his statement prayed for the dismissal of the suit.

In the counter statement filed by the plaintiff, he rejected all the allegation of the written statement and reaffirmed the contents of the plaint.
On the basis of the pleadings of both the parties, the issues were framed on 10th February 2004 and the corrections were made on 24th April 2008. The correction made to the issues was a clerical mistake.

ISSUES:

The issues raised in the case stated above were:

- Whether the plaintiffs are entitled to the relief of perpetual injunctions as prayed by them? The onus to prove was on the plaintiff.

[17] CS (OS) No. 1279/2001 (Delhi High Court, 2001)

[18] SMC Pneumatics (India) Pvt. Ltd. V/s Jogesh Kwatra , suit no. 1279 of 2001

- Whether the plaintiff has made false allegations, which have not come to the court with clean hands? The onus to prove this was on the defendant.
- Relief to be granted.

JUDGEMENT:

The plaintiff to support his statement examined six witnesses. On the other hand, the defendant to defend himself examined himself. He presented his evidence by the way of affidavit. The arguments of both the counsels were heard.

Judgement on issue 1: The judge invoking section 67 of the Information Technology Act, 2000 [19]passed an ex-parte ad interim injunction observing that the prima facie case had been made out by the plaintiff. The court restrained the defendant from sending any such defamatory emails either to the defendant or to the subsidiaries. The defendant was also restrained from publishing or transmitting any information in the actual world and cyberspace which is defamatory in nature.

Judgement on issue 2: The court called off this issue as infructuous because there was no specific pleading presented by the party except for the general objection based on the factors that would determine whether the plaintiff has any cause of action or not.

Judgement on issue 3: The court after taking onto consideration the above discussions and the facts, circumstances of the case dismissed the suit of the plaintiff. No order as to costs.

CONCLUSION

This order passed by the Delhi High Court holds tremendous significance as this was for the first that an Indian Court assumed jurisdiction in a matter relating to cyber defamation and granted an ex parte interim injunction restraining the defendant from performing any such defamatory act.

CHAPTER: 4
LEGAL PROVISIONS TO CURB CYBER CRIMES

India has a well-developed legal structure like other western countries and is still developing and growing with time. In spite of having a well-built legal; system, the nation is facing the problem of the traditional notion of the jurisdiction which turns out to be a great difficulty for the laws related to the cyberspace.

With the rise in the IT sector in the nation, the possibility of a rise in crime relating to the internet/cyberspace has also increased. The legislative actions to curb the crime rate and keeping a check on e-commerce have become essential. The Indian legal system enacted the Information Technology Act, 2000 for combating the cyber-crimes.[20]

Before the introduction of the IT Act, the crimes related to the computers were covered under the Indian Penal Code, Law of tort and Criminal Procedure Code. But in order to build a stronger legal system against the rising cyber-crimes the IT Act, 2000 was introduced. The rules formulated under this act helped the Indian Legal system to maintain its legal status internationally.

[19] IT Act, 2000, Section 67 – Punishment for publishing or transmitting obscene material in electronic form.

[20] P.K. Singh, LAWS ON CYBER CRIME(2007), Pg. 23

I.INFORMATION TECHNOLOGY ACT, 2000: The advancement in the IT sector called for some strong steps to regulate electronic communications. The Indian Parliament recognized the need to introduce some enactments and that is when some amendments were made in the Indian legal structure and Information Technology Act, 2000 was introduced. The main objective of the Information Technology Act is to regulate commercial activities through electronic medium and also facilitate legal re-organization. The IT Act is based on United Nations Resolution[21] and the UNICITRAL model on e-commerce. This is the only act in the Indian legal system, which is known as cyber law. The act mainly deals with the regulation of electronic commerce.

The Information Technology Act was formulated to meet the requirements of new and rapidly expanding digital technology as well as communication technology. The Act provides penalties for illegal use or misuse of technology. It proposes to introduce civil and criminal liabilities for breach of the provisions of the act. Chapter XI of the IT act deals with certain offences and the punishments for the same. For Instance, Section 65 of the act talks about the offence of tampering with the computer source document. It states that "anyone knowingly or intentionally destroying, concealing or altering or causing another to do the same with any computer source code use for a computer programmer, computer network or computer system when the code is required to be maintained by the time being in force shall be held and punishable with imprisonment up to three years or fine which may extend up to two lakh rupees or both"[22] This offence deals with the privacy of the computer source documents. The section 65 of the act tries to curb the actions given to the computer to destroy or alter the programs or to cancel them in a way that they cannot be used by the owner of the program.

Sections 65 to 75 of the IT act deals with the offences such as hacking into the systems or obscene publications in electronic forms. These sections focus on the cyber-crimes and punishments for those crimes.

The act cannot fulfil the need of the time and the cybersecurity problem that the country is facing. Therefore, the IT act, 2000 was amended in the year 2008.

THE INFORMATION TECHNOLOGY (AMENDMENT) ACT,2008 brought remarkable changes in the IT Act,2000. The act was made effective from 27 October 2009. Certain important definitions were added to the act. For example, In Section 2(ha) - The term "communication device" is included which brings into ambit the cell phones. This amendment brought all communication devices such as iPod, tablets or other devices that are used to send or transmit any audio, visual data or texts. Section 2(w) of the act was also amended and the service providers were also under the preview of cyber-crime.

The IT (Amendment) Act, 2008 added new provisions in section 66. The provisions introduced were:

- Section 66A: Sending offensive or false messages.

[21] United Nations Resolution no. A/GES/51/162, 30th January 1997.

[22] Section 65, The Information Technology Act, 2000

- Section 66B: Receiving stolen desktop resources,
- Section 66C: Identity theft
- Section 66D: Cheating by personation
- Section 66E: Violation of privacy
- Section 66F: Cyber Terrorism

For all the offences covered under section 66 of the IT (Amendment) Act, are punishable with imprisonment generally up to three years and fine up to two lakh rupees. These offences are cognizable and bailable. Punishment under the offence of Hacking (section 66) got enhanced, imprisonment up to three years and a fine of two lakhs to five lakhs fine.

Another new section 84B that is abetment to commit a crime is made punishable under the act. Section 84C of the act makes attempt to commit and offence as a punishable offence with imprisonment for a term, which may extend ½ of the longest term of imprisonment under that offence. Section 67 of the act deals with the offence of publication of obscene information. The term of imprisonment under the said offence is reduced from five years to three years and the fine has been increased from one lakh to five lakhs. Other new provisions introduced in section 67 are:

- Section 67A: Publishing material containing sexually explicit content
- Section 67B: Offences relating to Child Pornography

The act states that even browsing and collection of child pornography a punishable offence.

The IT (amendment) act, 2008 has been a very positive change in the history of Indian Legal system. The act covered various crimes committed through computers or other communication networks.

II. INDIAN PENAL CODE, 1860:

According to the I.P.C, an act constitutes a crime when there is a guilty intention and the act performed is prohibited under law. The cyber-crimes that are not covered under the IT Act, the I.P.C is applicable to them. I.P.C. due to its universal nature covers all the crimes. The I.PC. has also been amended after the amendments made in the Information Technology Act. The amendments are made with the aim of taking into consideration the offences involving electronic devices. The meaning of fabricating false pieces of evidence to include any false records or statements has been amended in section 192 [23]of the Indian Penal Code.

Section 383 of the Indian Penal Code takes into ambit all the offences committed using the computer as a tool. Crimes like threatening emails, web-jacking, etc. are also covered under section 383 that deals with extortion.

Most of the cyber-crimes are categorized as a fraud . The IT Act does not define the concept of fraud henceforth; most of the offences are covered under the Indian Penal Code. When a cyber fraud is committed, it amounts to cheating which is defined in section 415 of the I.P.C. The crimes related to personation are covered under section

[23] Section 192 , Indian Penal Code- Fabricating false evidences (whenever any electronic record is falsely made and is provided for the judicial proceedings, it amounts to fabricating false evidence)

416 [24]of the Indian Penal code. Various other sections of I.P.C that cover the cyber offences are section 405,406,463,465. Section 354(D) of I.P.C deals with stalking, 354(C) deals with Voyeurism, and these offences are subjected to all the communication devices.

Thus the I.P.C covers almost all the cyber-crimes, which have not contended in the Information Technology Act.

III. CRIMINAL PROCEDURE CODE AND THE INDIAN EVIDENCE ACT:

These two very important procedural laws in the Indian Legal System deal with the procedures of criminal proceedings. Various amendments were made by the Parliament in these acts as well. In the Indian Evidence Act, the words "Digital Signature" and "Digital Signature Certificate" under section 3 were substituted by "Electronic Signature" and "Electronic Signature Certificate."

In Criminal Procedure Code, 1973, a new section 198 B was inserted which stated that "No court shall take cognizance of an offence covered under section 417, 419 and 502 of the I.P.C, expect upon receiving a complaint by the person aggrieved."

Apart from these, there are various other laws existing in the country dealing with the issues of cyber-crimes. These laws are relevant to certain misuse in cyberspace. They are[25]:

- Common-Law (governed by the general principles of Law)
- The Reserve Bank of India Act,1934
- The Banker's Book Evidence Act,1891
- The I.T. (amendment) Act, 2008 & 2009
- The I.T. (removal of difficulties) Order,2002
- The I.T. (certifying Authorities) Rules, 2000.
- The I.T. (certifying Authorities) Regulations,2001
- The I.T. (securities Procedure) Rules,2004
- Laws relating to IPRs.

Therefore, the Indian legal structure has various laws in place concerning cybercrimes. There is no specific manner in which the internet is misused and so it becomes difficult for the legal system to meet with the needs. The cyber law cannot function without international co-operation and so laws relating to the transnational jurisdiction are important. The I.T. Act does have provisions regarding the transnational jurisdictions, but it can only function smoothly if all the countries put in efforts t recognize the cyber-crimes.

COMPARATIVE ANALYSIS ON LAWS IN INDIA AND THE UNITED KINGDOMS

The cyber laws in functioning across India and the United Kingdom when compared shows some common points and some differences. The different approach adopted by the countries in formulating the laws creates variations. India has observed a tremendous increase in cybersecurity as an

[24] Section 416, Indian Penal Code- When any person attempts any crime by cheating and using internet to hides his identity.

[25]CHAPTER-III, THE LAW RELATING TO CYBER-CRIME IN INDIA , 29 September 2020 10:19 pm (https://shodhganga.inflibnet.ac.in/bitstream/10603/203654/8/08_chapter%203.pdf)

essential policy concern. On the other hand, the UK has been concerned about cyber security for a more extended time period than India and has very developed processes and systems. The framework is more comprehensive in the UK as compared to that in India.

When it comes to cybersecurity, the UK is more open to multi-stakeholder inputs in order to form policies, while India remains divided between the government initiatives and private sector which focus on national security concerns. The Indian government needs to become a lot more flexible to comply with practices followed for cyber-security and spread awareness for the same. The strict laws and regulations should not be mandated. International agreements should also be taken into consideration by the country. The international agreements play a vital role when investigating cyber threats.

ANALYSIS OF DEFAMATION LAW UNDER THE INDIAN CONSTITUTION AND ENGLISH LAW

The Indian Constitution includes the expressions libel and slander covering various species of these words such as obscene libel, seditious libel, etc. The law of defamation does not infringe article 19 (1) (a) that states -the right of freedom of speech. This is safeguarded by Article 19(2)[26] of the constitution. The law relating to tort of defamation, from the point of view of the distribution of legislative power, falls under the head "Actionable Wrong" in Entry 8 of the Concurrent List in the 7th Schedule of the Constitution of India.

In the English Common law, reputation is protected and remedy is provided in the civil law by awarding damages to the aggrieved party after the trial is complete. The law of Defamation aims at safeguarding the interests of the parties concerned. These are the rights that a person has to his reputation in relation to the right to freedom of speech. The law provides defences to the wrongdoer such as truth and privilege protecting the right to freedom of speech and expression.

CHAPTER: 5

JUDICIARY ON CYBER-CRIME CASES

Cyber-crimes have been increased due to technological advancements. The development of technology cannot be halted but the rate at which these crimes are increasing in the world can be curbed. The various laws formed by the government to reduce the spread of these crimes have been very helpful. Some cases which portray the role of the judiciary in curbing these crimes are as follows:

I. Shreya Singhal v/s Union of India[27] : In this case Section 66A[28] of the Information Technology act, 2000 was repealed by the Supreme Court. The court quashed this section due to ambiguity in the definition of the word "offensive". The section related to the restrictions on online speech and stood

[26] Article 19(2), Constitution of India- Authorizes Government to impose by law, reasonable restrictions on the right to freedom of speech and expression.

[27] SUPREME COURT OF INDIA- WRIT PETITION (CRIMINAL) NO. 167 OF 2012 , 29 September 2020 6:55 pm (https://indiankanoon.org/doc/110813550/)

[28] Punishment for sending offensive messages through communication services

unconstitutional on the grounds of violating Section 19(1) (a) [29] of the Constitution of India. Section 66A was misused by the government in suppressing the freedom of speech and expression that the citizens hold.

II. Kalandi Charan Lenka v/s State of Odisha[30] : In this case, the petitioner was being stalked online and a fake account was also created in her name. Obscene messages were sent to her friends through that fake account by the culprit with the intention to defame her. The High Court of Orissa held that the accused is liable for the offence of defamation as he sent obscene images and texts by creating a fake account in the name of the defendant.

III. Cyber Attack on Cosmos Bank: In August 2018, the Cosmos Bank, Pune was drained of rupees 94 Crores. The culprits hacked into the main sever of the bank and transferred such huge amount to a bank in Hong Kong. The hackers made their way into the ATM servers of the customers of the bank and stole their card details. According to a case study, a total of 14,000 transactions were carried out internationally, to make this theft successful. The transactions spanned across 28 countries using 450 cards. Nationally, a total of 2800 transactions were carried out using 400 cards. This was the first malware attack that stopped all the communication signals between the bank and the payment gateway, in other words, neither the bank nor the account holders came to know that their money was being transferred.[31]

IV. Anvar PV v/s PK Basheer[32]: In this case, the court redefined, clarified the law pertaining to the electronic evidence in India. The court overruled the statement of the law on the admissibility of secondary evidence relating to electronic records, as held in the case State (NCT of Delhi) v/s Navjot Sandhu[33]. The apex court in this case further explained that the electronic records as secondary evidence shall not be admitted in the court of law unless the requirements under section 65 B of the IT Act are satisfied. Therefore, the CD, VCD, Chips, etc., shall be accompanied by a certificate stating that the requirements as under section 65B of the IT Act are fulfilled. If the certificate is not produced by either of the parties, the evidence stands inadmissible.

V. M/S Spentex Industries Ltd & Anr. V/s Pulak Chowdhary[34]: In this case, defamatory emails were sent by the defendant to the International Finance

[29] CONSTITUTION OF INDIA - Freedom of Speech and Expression

[30] HIGH COURT OF ORISSA, CUTTAK – BLAPL No. 7596 of 2016 , 30 September 2020 7:00 pm (https://indiankanoon.org/doc/73866393/)

[31] Rashmi Rajput , UN Security Council panel finds Cosmos Bank cyber-attack motivated by N Korea, The Economic Times , 29 September 2020, 8:30 pm (https://economictimes.indiatimes.com/industry/banking/finance/banking/un-security-council-panel-finds-cosmos-bank-cyber-attack-motivated-by-n-korea/articleshow/68589549.cms?from=mdr)

[32] SUPREME COURT OF INDIA- CIVIL APPEAL NO. 4226 OF 2012 , 30 September 8:32 pm (https://indiankanoon.org/doc/187283766/)

[33] 2005 , 11 SCC 600

[34] DISTRICT COURT, DWARKA, NEW DELHI – CIVIL SUIT NO. 219/18 , 30 September 2020 8:47pm (https://indiankanoon.org/doc/80844707/)

Corporation, World Bank, UZEREPORT[35] and the President of Uzbekistan The petitioner filed for a compulsory and prohibitory injunction order against him along with the recovery of Rs. 50, 00,000 as damages for the loss incurred in the business and reputation due to those emails. The case was filed in 2006 and judgement was passed in the year 2019 wherein the court ordered that the plaintiff to be awarded 1/10th of the cost prayed for as well as the cost of the suit to be paid by the defendant. The defendant was further restrained from making false and defamatory statements in any form (oral or written).

VI. Yahoo! Inc. v/s Akash Arora[36]: This was India's very first case of cyber-crime. The case was filed in the year 1999. In this case, defendant Akash Arora was accused of using the domain name that was already registered under Yahoo. Yahoo filed a suit stating that the defendant attempted to gain profits on the goodwill by generating a similar domain name and is liable for passing off. The court held the defendant liable for passing off and restrained him from using the deceptively similar domain name.

These notable judgements by the Indian judicial system proved to be helpful in enhancing the legal provisions with respect to the cyber-crimes in the country. These judgements and many other restored the faith of the citizens in the legal system of the nation.

CONCLUSION

With the advancement in the technology sector and the internet age, communication has been made very easy. We have heard that with great power comes great responsibility describes the use of technology and its misuse very well. The effortless transmission of information has made the internet critical hotspot for cyber-crimes.

Cyber defamation in the corporate world can have major impacts on the organizations growth and reputation. There are laws in place to deal with cyber defamation and the things have been eased by accepting the electronic records as evidence. In such cases, the onus lies on the defendant to prove him innocent. The cyber-crime investigation cells are also formed to deal with the cyber-crimes in the country.

Thus, the criminal justice systems all over the world must try to curb these cyber-crimes and put in their best efforts to identify the real cyber-criminals. International co-operation is very essential in such cases due to the transnational nature of the offence.

After researching, it can be said that the present laws in India are trying to curb the offences but can be made more flexible and applied to all media. It is not practical to apply policies introduced in the 18th and 19th century to resolve issues arising in the 21st century.

*****

[35] A news portal and publisher of monthly news reports.

[36] 1999 IIAD Delhi 229,78 (1999) DLT 285 , 30 September 2020 3:10pm (https://indiankanoon.org/doc/1741869/)