LEGAL METRY LAW JOURNAL

ISSN: 2582-9963

CONCEPTUAL ANALYSIS OF CYBER TORTS

YASHIKA GUPTA*

ABSTRACT

"When we talk about "cyberlaw," we're referring to all of the cases, laws, and constitutional provisions involving individuals and organisations that regulate access to the internet, give admittance to the internet, or foster the equipment and programming that permits individuals to get to the internet or go "online" and enter cyberspace."[1] Briefly stated, cybercrime refers to any unlawful conduct in which a computer is utilised as a weapon, as the target of the criminal action, or as both. Cybercrimes may encompass traditional criminal behaviours like burglary, extortion, and fraud just as criticism and mischief, which are all covered under the Indian Penal Code[2]. Because of improper use of computers, there is seen to be an explosion of new sorts of criminal activity. Cyber torts are the most recent and, in many ways, the most sophisticated issue to arise in cyberspace. Cyber torts are those types of torts whose variety is the ordinary torts and in which either the PC is an item or the subject of the behaviour creating the tort are considered to be cyber torts, according to this definition. These issues, as well as the resulting challenges and legal requirements, will be addressed in this research paper.

Keywords: - Cyber ,Torts, Cybercriminal.

INTRODUCTION

Cyber Torts are torts that are committed through the internet, as the name suggests. Cyber torts include trespass to chattels, transfer, cyberstalking/harassment, and cyber defamation, to name a few examples of what they are. All of the malware, spam emails, and scrapers that you may come across from time to time are deemed trespass to chattels under California law. On the

[*] 1st year student at Dharmashastra National Law University , Jabalpur

[1] Radhakrishna Tatavarty, 'July 2018 Literary Endeavour.Pdf' (*Academia.edu*, 2021) https://www.academia.edu/38196377/July_2018_LITERARY_ENDEAVOUR_pdf accessed 14 June 2021.

[2] The Indian Penal Code (Act No. 45 of 1860)

web, whether or not a court is qualified regarding website activity and, subsequently, regardless of whether it can practice purview over a litigant who doesn't have an actual presence in the forum state is at present a fervently discussed topic in tort (such as infringement) cases that have been committed. The internet has transformed people's lives. Technological advances are a benefit to humanity. E-mail allows people to connect all over the world. In a matter of seconds, the data can be downloaded or sent to any place. Social networking sites have made it easier to stay in touch with friends and family. On the internet, businesses are conducted. on the internet, Almost everyone is familiar with the virtual world and has access to it. However, much like the real world, the virtual world is not without its share of criminal activity. The perpetrators of the crimes are well-versed in technology. Social crimes, such as cyberstalking; financial crimes, such as credit card fraud and intellectual property theft; and crimes against the state, such as embezzlement, are examples of the types of crimes that can be committed. Card frauds, intellectual property violations, and crimes against the state, such as cyber terrorism, are all examples.[3] The crimes may be directed at the computer system or the computer itself. It may be used to commit crimes. It was impossible in such a situation. To leave cyberspace in an uncontrollable state.[4] The Information Technology Act of 2000 was enacted as a result of this. The Act included fewer cybercriminals at first but was revised in 2008 to include a few more. It amends the Indian Evidence Act of 1872 to grant electronic evidence legal recognition. The Indian Penal Code, 1860[5], the Bankers' Books Evidence Act, 1891,[6] and the Reserve Bank of India Act[7] have all been amended by the Act. the interpretation of evidence in electronic form necessitates expert expertise, which contributed to the growth of the field of cyber forensics. The police face a difficult challenge in enforcing the law because they must rely on new technologies and techniques to investigate cybercrime. The cybercriminal also goes unpunished because the crime can be committed from anywhere in the world, making it difficult to exercise jurisdiction over the accused. Extradition arrangements with other countries are required to prosecute the accused. If the act committed by the accused is not a crime in that country, extradition would be impossible.

Cyber Tort can simply be described as tort or violation of a right done over Cyber Space. "Example of Cyber torts are Email & Text harassment, Cyber Stalking, Dissemination through the internet of obscene, offensive or prohibited material inclusive of indecent exposure,

[3] 'Cyber Torts - Advocatespedia' (*Advocatespedia.com*, 2021) https://www.advocatespedia.com/Cyber_torts accessed 14 June 2021.

[4] Ibid.

[5] IPC (Act No. 45 of 1860)

[6] The Bankers' Books Evidence Act, 1891 (ACT NO. 18 OF 1891)

[7] Reserve Bank of India Act, 19341 (As amended by the Finance Act, 2019).

pornography, Defamation, Online Impersonation, Taking unauthorized control or having unauthorized access over computer System (Hacking), Distribution and dissemination of pirated software." Cyber torts would also include denial of service attacks and vulnerability to potentially malicious applications such as spyware. It will be best to take as many steps as possible to help prevent the company from succumbing to either of these threats.

Also, there seems to be no difference between cyber-tort and traditional tort. However, after careful consideration, we may conclude that there is a narrow line between the traditional tort and the cyber tort, which is perceptible. The line between cyber tort and other types of tort is drawn by the participation of the media in the case. The participation of the virtual cyber medium, also known as cyberspace, at any step of the legal process is a requirement for a cyber tort to be established.

RESEARCH QUESTIONS

- How cyber torts has been evolved in the law of torts?
- What are the essentials to claim the right to cyber tort?
- What is the position of this defence in the Indian context?
- What are some of the famous case laws on torts?

REASONS FOR OCCURRENCE OF CYBER TORTS

- *Capacity to store data in a small amount of space*

The device has the unusual ability to store data in a small amount of space. This makes it much easier to delete or extract knowledge from a physical or virtual medium.

- *Easy to access*

When it comes to guarding a device against unauthorised access, the problem is that there is always the possibility of a breach, and not because of human mistake, but because of the intricate technology involved in securing the item. Hidden logic bombs include keyloggers that may plunder access codes, powerful voice recorders, and retina imagers, to name a few examples.

- *System Complexity*

Operating frameworks, which are made out of millions of lines of code, allow computers to function properly. The human mind is prone to error, and it is inescapable that there will be a slip in judgment at some time in one's life. These weaknesses may be exploited, resulting in the compromise of computer security systems.

- *Negligence*

It is inextricably linked to human behaviour. It is also very likely that when securing the computer system, there will be some negligence, which will provide a loophole for gaining access and control of the computer system, and thereby misusing it.

- *Evidence Loss*

Since all data is frequently deleted as part of the data destruction process, this is a very frequent and obvious problem.[8]

THE METHOD AND MANNER IN WHICH CYBER TORT IS COMMITTED

The act of gaining unauthorised access to computer systems or networks (also known as hacking) is generally referred to as hacking in a wide sense. While the architects of the Information Technology Act of 2002 did not use this phrase, the word "unauthorised entry" has a wider connotation than the phrase "hacking."It is possible to steal electronic information if it is kept on computer hard drives, portable storage media, magnetic discs, flash memory devices, or other comparable devices, among other things. Theft may occur via the physical appropriation or misappropriation of data, as well as via the manipulation of data via the virtual medium.

An email bombing operation involves sending large volumes of email to a target, which might be a person, an organisation, or even mail servers, to cause them to fail. In this form of attack, raw data is modified shortly before it is processed by a computer, and then the modified data is restored after the processing has been completed. It was discovered that the Electricity Board had been computerised when a similar problem with data manipulation surfaced. Salami assaults are more prevalent at financial institutions or when financial crimes are being perpetrated, according to the FBI. The fact that the alteration is so subtle that it would normally go

[8] 'Gregory C. Mosier' and 'Tara', "Cyber Tort" (2021) American Journal of International Commercial Law and Technology.

undetected is a distinguishing feature of this kind of criminal activity. The Ziegler case, for example, included the planting of a logic bomb in the bank's computer system, which caused ten cents to be deducted from each account and deposited in a specified account.

The victim's device is bombarded with more requests than it can handle, resulting in the device's failure to function properly, DDoS (Distributed Denial of Service) assaults are a sort of forswearing of administration assault in which the wrongdoers are numerous and broadly dispersed, and they are another kind of denial of service assault. Viruses are PC programs that append themselves to a PC or a record and afterwards spread to different documents and PCs on a network. Worms are computer programs that replicate themselves. They often have an impact on a computer's data by altering or deleting it. Worms, in contrast to viruses, are not required to have a host on which to attach themselves. All they do is create useable duplicates of themselves and repeat the process as many times as necessary to absorb all of the available RAM on a computer. Consider the love bug virus, which influenced in any event 5% of the world's PCs at that point of its release. It was predicted that the losses would be in the neighbourhood of $ 10 million. It was the Internet worm, which was put on the Internet by Robert Morris sometime in 1988, that became the most widely distributed worm in the world.

System failures are caused by logic bombs. These systems are occasion-driven. This infers that these frameworks are customized to react just when a specific occasion (alluded to as a trigger occasion) happens to perform their functions. Examples of logic bombs include viruses that stay passive for the bulk of the year and only become active on a specified day, such as computer viruses and computer malware (like the Chernobyl virus). Trojan horse attacks are also common. The term "trojan horse" is derived from the phrase "trojan horse assault." According to the software industry, this is the phrase used to describe an unauthorised application that takes passive control over another's equipment by appearing as a legitimate application. The most often used form of Trojan installation is through an e-mail message. During a conversation, for example, a Trojan horse was planted on the computer of a female film director in the United States. By using the webcam that was installed on the device, she was able to share her naked images with the cyber-criminal. He persisted in harassing this particular lady.

Interception of Internet time robberies also a type of cyber attack. In this form of theft, the victim's Internet surfing time is frequently taken up by someone else. This is performed via the acquisition of a login ID and a password. Example: In the instance of Colonel Bajwa, the Internet hours were taken up by someone else. This was perhaps one of the earliest incidents of cybercrime in India to be publicised, and it was a significant milestone. Following the conclusion of this case, the police became well-known for their failure to recognise the existence of cyber torts and for their failure to investigate them. Web jacking is a concept that derives from the word "hijacking," which means "hi-jacking." These sorts of crimes occur when a hacker acquires access to and control over another's website via deception. He has the power to modify or mutilate the information that is posted on the internet. This may be done to attain political objectives or to gain money. Examples include the recent hacking of the MIT (Ministry of Information Technology) website by Pakistani hackers, which resulted in the posting of some filthy content on the website. Aside from that, a hacker gained access to the Bombay Crime Branch's website. This scenario dubbed the "GoldFish Scenario," is yet another example of online jacking. In this particular instance, the website was hacked, and the data concerning goldfish was changed. A payment of $1 million had also been requested in addition to the ransom.

WHO ARE CYBERCRIMINALS?

Cybercriminals are partitioned into numerous classes and classifications. This division could be legitimized dependent on the article they're contemplating. The following is a list of cybercriminals by category:

- *Children and teenagers aged six to eighteen years*

The simple explanation for this type of delinquent standard of conduct in children is their voracious craving to learn and find new things. Another plausible explanation is to demonstrate that they are superior to the other children in their class. Furthermore, the causes may be psychological. For example, the Bal Bharati (Delhi) case resulted from the delinquent's friends harassing him.

- *Organized hackers*

These hackers are typically gathered to accomplish a particular objective. It very well might be for an assortment of reasons, which includes political predisposition, fundamentalism, etc. The Indian government was recently attacked in the same way. Furthermore, hackers are constantly targeting NASA and Microsoft websites.

- *Hackers who work professionally*

The shade of cash propels their work. These types of hackers are commonly used to break into rivals' websites to obtain credible, reliable, and useful information. Furthermore, they are used to break into the employer's system to find vulnerabilities to make it safer.

CLASSIFICATION OF CYBER TORTS

- *Harassment through e-mails*

Harassment by e-mail is not a new phenomenon, and it is becoming more prevalent. Harassment by letters is a kind of harassment that is fairly similar. Recent email correspondence from a woman who voiced her discontent with the current situation was sent to me. Her ex-boyfriend was always sending her emails, and he was often verbally blackmailing her and threatening her with violence. This is a pretty common kind of e-mail abuse that occurs.

- *Cyber-Stalking*

The second kind of stalking is cyber-stalking. According to the Oxford dictionary, stalking is defined as "following covertly." Stalking someone on the internet involves tracing their online travels by posting comments (often threatening) on bulletin boards frequented by the target, accessing chat rooms, and other methods.

- *Pornography*

Third, indecent exposure/ scattering of obscene material/profane openness/sexual entertainment (basically child pornography)/revolting openness/foul openness. Pornography on the web might be found in a variety of formats, depending on the source. Also included in this category is the hosting of a website that includes these prohibited items. These disgusting items are created with the usage of computers. Obtaining pornographic content through the internet is a common practice. Because they can deprave or corrupt the psyche of a teenager, these obscene matters should be avoided at all costs. Bal Bharati and the Bombay instances are two well-known incidents of pornography in which two Swiss couples forced slum children to appear for pornographic images. In both instances, slum children were forced to pose for pornographic images. Mumbai's police department

- *Defamation*

It is the act of putting false information about another person into the public domain to reduce that person's status among right-thinking members of society, driving him to be evaded or kept away from, or exposing him to disdain, disparagement, or hatred Cyber slander is like customary maligning, except for the utilization of a virtual media to communicate. To provide an example, Rohit's email account was hacked, and emails concerning his involvement with a lady were sent from his account to some of his classmates to defame him were forwarded him from his account.

- *Unauthorized access to or control of a computer system*

The word "hacking" is used to denote this kind of criminal activity. Since a result, we will not use the phrases "unauthorised entrance" and "hacking" interchangeably to prevent misunderstandings, as the phrase "unauthorised entrance" used in the Act of 2000 is significantly wider than "hacking" under Indian law.

- *Spoofed e-mails*
- A spoofed e-mail is one in which the sender's identity is misrepresented by the sender. It illustrates that the source of the problem is distinct from where the problem originated.
- *Cheating and fraud*

Cheating and hacking on the internet have become one of the most profitable professions in the modern world of information technology. It may manifest itself in several ways. It has been shown that credit card fraud, contractual fraud, labour offers, and other sorts of internet fraud and deceit are all taking place. The Court of Metropolitan Magistrate Delhi[9] recently convicted an engineer who was a 24-year-old working in a contact centre guilty of illegally acquiring Campa's credit card information and using the information to purchase a television and a cordless phone from the Sony website.

There are several types of cyber-terrorist assaults against government organisations, including the following: The need to distinguish between cyber terrorism and cyber torts may arise at this stage, it is possible to argue. Both of these activities are quite risky. There is, nevertheless, a strong need to distinguish between the two actions in question. Typically, a cyber tort has local repercussions with worldwide implications, but cyber terrorism is a worldwide concern with both domestic and international implications. On the Internet, terrorist strikes typically take the shape of circulated forswearing of administration attacks, disdain websites and disdain messages, attacks on critical PC networks, and other forms of cybercrime.

STATUTORY PROVISION

The Information Technology Act of 2000 (IT Act) of India is one of those laws. In May 2000, the Indian Parliament enacted the Information Technology Bill,[10] which had been supported by

[9] 'Official Website : Delhi District Courts' (*Delhidistrictcourts.nic.in*, 2021) https://delhidistrictcourts.nic.in/ accessed 14 June 2021.

[10] 'The Information Technology (Amendment) Bill, 2006' (*PRS Legislative Research*, 2021) https://prsindia.org/billtrack/the-information-technology-amendment-bill-2006 accessed 14 June 2021.

the two chambers of the legislature. The bill was officially recognised as the Information Technology Act of 2000 when the measure was signed into law by President Clinton in August of that year. The purpose of this Act is to give the legitimate establishment to internet business in India. Indian digital guidelines essentially affect e-organizations and the computerized economy, according to the Economic Times. As a consequence, it is vital to understand the many points of view on the Information Technology Act of 2000, as well as what it is intended to accomplish. A secondary goal of the Information Technology Act of 2000 is to provide a legislative framework to guarantee that all electronic papers and other processes carried out via electronic means are accorded legal protection. Under the Act, unless otherwise agreed, a contract acceptance may be given using electronic methods of communication and is still considered to be legitimate and enforceable. An examination of the proposed modifications to the Information Technology Act of 2000, which includes a critical assessment The proposed revisions to the Information Technology Act of 2000 are neither desirable nor beneficial to the development of information and communications technology (ICT) infrastructure in India. They are riddled with defects and grey areas, and they should not be elevated to the status of national law. "The following are a portion of the seriously squeezing and real rules in such manner: The meaning of due constancy for organizations and their officials isn't obvious to the concerned fragments; The utilization of ICT for equity organization should be fortified and improved; The offence of digital coercion, alongside digital psychological oppression and other contemporary digital wrongdoings, ought to be added to the IT Act, 2000; The utilization of ICT for the everyday procedural issue should be thought of; The legitimate dangers of online business in India should be thought of; The standards of private assurance and forceful safeguard are missing from the IT Act, 2000; Internet banking and its lawful difficulties in India should be considered; Adequate and reasonable arrangements on "Internet Censorship" should be delivered in the IT Act, 2000; The utilization of private insurance for digital illegal intimidation ought to be remembered for the Information Technology Act of 2000."

CONCLUSION

The epidemic of PC wrongdoing is a multibillion-dollar one. Law implementation should discover approaches to forestall the inconveniences of the computer age from overshadowing its great potential. Cybercrime is a threat that must be actively addressed not only by authorities, yet in addition by clients who help out the law. The web's forefathers intended for it to be a gift to the entire world, and it is up to us to keep it that way and not transform it into a social blight. The epidemic of PC wrongdoing is a multibillion-dollar one. Law requirements should discover approaches to forestall the disadvantages of the computer age from overshadowing its great potential. Cybercrime is a threat that must be actively addressed not only by authorities, yet additionally by clients who help out the law. The web's forefathers intended for it to be a gift to the entire world, and it is up to us to keep it that way and not transform it into a social blight. We'd like to end with a word of warning for the pro-legislation camp: it's important to remember that the regulations of the cyber law aren't made so strict that they stifle the industry's growth and prove counter-productive, and that a close eye should be held on its misappropriation and subsequent consequences.