LEXFORTI LEGAL JOURNAL | [ISSN: 2582 2942]
VOLUME II -ISSUE III

CYBER ISSUES IN INDIA

- ***AKANKSHA NEGI***
- ***SAATVIK SRIVASTAV***

ABSTRACT

Despite the advantages of Cyber Law, it is necessary to provide legal recognition for transactions conducted through electronic data and other electronic communication methods and to promote the use of the Internet. In addition, with the development of technology, issues related to domain names, privacy, intellectual property rights, encryption, electronic contracts, online banking, e-commerce, hackers, etc. have emerged, and have posed new challenges to the entire existing legal system. General laws prevailing in the country are almost incapable of solving problems posed in the realms of cyber world. Hence, in addition, to the constructive use of the computer, the same has also been utilized for destructive purposes. Computers are used for various crimes. Although some of them are new, computers have even been used to commit conventional crimes. Therefore, many conventional crimes are now in digital form, posing new challenges to investigative agencies. This Paper will further discuss the Realms of Cyber world and its ambit in India by understanding the meaning of Cyber world and its various facets in brief.

Keywords: Cyber Law, Crime, Privacy

INTRODUCTION

The invention of computer and its merger with information technology has been one of the most phenomenal achievements in the history of mankind. It paved a way through which humans could interact with each other through the electronic means of cyber space. "Cyber space is a world of virtual reality". It is like a world preset in another dimension devoid of any geographical boundaries, but, is a place where the entry is not bound by geographical boundaries. The interactions done in this world takes place virtually and, hence, intangible. Instead of traditional papers, people from various walks of life are increasingly using computers and the internet to produce, distribute, and store information in electronic form, and they are gaining profit in terms of time, cost, productivity and effectiveness. It is frugal, easier to access and use i.e. a friendly and user friendly interface, and speedier to communicate. The way people transact with each other is evolving. Information technology is a rapidly growing technology all over the world. The growth and reach of Internet has become one criterion for measuring the growth and strength of the economy of a country, in the current times. In addition, as the development pertaining to the cyber world continues, significant issues pertaining to the facets of spamming, e-commerce, computer vandalism, encryption issues, e-contracts, Intellectual Property Rights etc. exist.

Cybercrime can be understood as the criminal activities in which computer and/or network are used as instruments. Cybercrime was not defined under any statute passed by the Indian Parliament up-till early nineties. As advancement inn technology happens, it becomes one among the various factors promoting cybercrime. Scholar Hart, very well emphasized in his work that a rule of law is required for safeguarding the various vulnerabilities of human-beings. Applying the same principle in cyber world makes the computer system vulnerable to cybercrimes and thus, laws are required for safeguarding it.

CLASSIFICATIONS OF CYBER CRIME

It is broadly categorized into three categories;

ON THE BASIS OF SUBJECT OF CRIME

Subject of crime may be any individual or their asset or property, some of the crimes which fall under this category are[1]:

- Cyber stalking: A crime in which a computer connected to a network is used for stalking an individual or rooting out information regarding them.[2]
- Defamation: It can be stated as the most common crime committed by any individual knowingly or unknowingly, defamation in cybercrime can be understood as the practice of using a system for publishing derogatory statements regarding someone.[3]
- Harassment via emails, Dissemination of obscene material, Indecent exposure, unauthorized control over a computer system etc. are some other cybercrimes committed against an individual as its subject.
- Net-trespass, Transmitting Virus, Intellectual Property Crimes, Internet time thefts etc. are some of the cybercrimes committed against an individual's property as its subject.
- Cybercrime can also be done against Organizations such as a firm, company or even against the Government; some of the crimes which include them as its subject are unauthorized possession of information, Cyber terrorism, Dissemination of Pirated software etc.
- Pornography (majorly child pornography), trafficking, sale of illegal objects, online gambling are considered as cybercrimes against the society at mass.

Similar to how technology improves by the day, cybercrime also goes through a constant evolution. Hence, the list mentioned above is not exhaustive in nature.

[1] Cyber Crime India: Types of Cyber Crime, Cyber Security, Cyber Attacks and Thefts, The Economic Times, https://economictimes.indiatimes.com/tech/internet/newslist/60870273.cms (last visited Jan 8, 2021).

[2] Vartika Vasu & Krishnapriya G, Cyber Crime Against Women: A Cyber Exploitation, II LexForti Legal Journal (2021), https://lexforti.com/legal-news/wp-content/uploads/2020/09/Cyber-Crime.pdf (last visited Jan 13, 2021).

[3] Right to Freedom of Speech and Expression - LexForti Legal Journal, , LEXFORTI LEGAL NEWS & JOURNAL (2020), https://lexforti.com/legal-news/freedom-of-speech-and-expression/(last visited Jan 13, 2021).

ON THE BASIS OF NATURE OF CRIME

Traditional crimes like theft, fraud and forgery involving a computer system along with the crimes like web-jacking, data diddling, E-mail bombing, Salami attacks etc. intensified due to the use of computers falls into this category of classification.

- Cyber Theft[4]: An individual when fraudulently moves or interchange something from the target's computer without his authorization is construed as Cyber Theft.
- Cyber Trespass: By cracking up the passwords through any means and entering into the target's property comes under the ambit of Cyber trespass.
- Cyber Obscenity: Publishing any obscene material on the internet. Many organisations are trying to find effective methods for combatting this.
- Cyber Violence: When there is a violent effect being observed due to certain cyber activity over a single person or a group or country then it becomes the crime of Cyber violence.
- Cyber Forgery & Fraud: Forging any kind of document which holds some evidentiary value of any kind or deceiving someone with a fraudulent intention comes under the ambit of Cyber Forgery & Fraud, ex. Credit-cards frauds, forging mark-sheets etc.
- Intellectual Property Crimes: It includes the crimes which infringes or violate the rights of a person dealing with trademarks, copyrights, designs and patents.

ON THE BASIS OF EMERGENCE OF NEW CRIME

With the advent of time many new crimes have emerged which needs to be regulated.

- Cyber Pornography: The first case in India dealing with this crime was observed in the case of *Air Force Bal Bharti School & Another v. Delhi School Tribunal & Others*[5], where a student created a website which contained materials with explicit sexual details about teachers and girls. This case was then registered under section 67 of the Information Technology Act, 2000 with Delhi Police Cyber Crime Cell.

[4] The 12 Types Of Cyber Crime | Chapter No. 2 | Fasttrack To Cyber Crime | Digit, Digit, https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html (last visited Jan 8, 2021).

[5] Appeal No. 48 of 2005 | 16-01-2013

- Unauthorized Access: Access control signifies the restriction of entrance to a room or the property of the person in authority and hence, unauthorized access refers to the access of a person without any authorization by the person in authority through a computer network. Some of the renowned common techniques of unauthorized access are:
    - Packet sniffing[6],
    - Tempest attack[7],
    - Password Cracking[8],
    - Buffer overflow[9].
- Hacking: The most known cybercrime globally is hacking. No computer has ever been made or will be made in the near future which is or will not be vulnerable to hacking. Section 66 of Information and Technology Act, 2000 defines Hacking. Some essential ingredients necessary for hacking:
    - Mala-fide intention of causing damage to any person,
    - Knowledge that the said act will cause harm to the targeted person
    - The data of the targeted system must be altered or deleted or affected injuriously.
- Virus & Worms Attack: The attacks in which programs like Viruses are used which on entering the host computer gets attached to a file and then starts to grow so that the whole system becomes corrupt or unusable while in case of worms the file acquires the all the empty space of the system's memory by making functional copies of themselves.
- Salami Attacks: The attacks which are generally observed in financial sector come under the ambit of Salami attacks. *The Zeigler case* in which a logic bomb attack was used to enter

[6] Packet sniffing is the practice of gathering, collecting, and logging some or all packets that pass through a computer network, regardless of how the packet is addressed. In this way, every packet, or a defined subset of packets, may be gathered for further analysis.

[7] TEMPEST is the study of vulnerabilities of compromising emanations from communications and other electrical equipment that contain data. A radio receiver can be placed near an emanating machine and pick up the signals, usually harmonic frequencies, emitted by the equipment.

[8] In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system in scrambled form.

[9] A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

into a bank's system, which then deducted 10 cents from every account and added them all to a specific account.

- Web Jacking: When the entire website is hacked i.e. when there is an unauthorized forceful control is observed in a particular website then it is termed as web jacking
- Cyber terrorism: It is a global concern. Cybercrime in ordinary parlance can be understood as the disruptive threats or acts, thereof, done in cyber space with the intention to channelize it further by using certain social ideologies, political or religious affairs.
- Computer vandalism: The act which involve the destruction of the target's system or damage done to the target system

Some other cybercrimes which comes under the ambit of classification on the basis of new emerging cybercrimes are E-mail spoofing, Trojan attack, Logic bombs, Denial of Service attack etc.

INFORMATION TECHNOLOGY ACT, 2000

Information Technology Act, 2000 and cyber laws in India are considered as tantamount with each other. Since one nation cannot withhold the power of internet within its geographical territory, United Nations Commission on International Trade Law proposed uniformity up-to an extent within the legislations of each member countries. This gave rise to the adoption of Model Law on Electronic Commerce by the commission on its 29th session. Being one among the member countries India also incorporated the principles enshrined in the Model law and thus the Department of Electronics was given the task of instituting an enactment soon. These instances lead to the inception of having an Information Technology Act and give India the very first legislation in the field of Cyber space. The act received the president's assent on 9th June, 2000 and was enforced on 17th October, 2000. With the emergence of the Information Technology Act, 2000 and amendments of the Indian penal code 1860, there are two legislations present for instituting a criminal liability pertaining to electronic world. It also gave effect to amendments done in the Banker's Book Evidence Act 1891, Indian Evidence Act 1872 and the Reserve Bank of India Act 1934 so that a harmony and compatibility is maintained among all of them.

Information Technology Act is based on *"functional equivalent approach"* proposed in the Model Law on Electronic Commerce. It is framed after scrutinizing the functions and purposes of the present paper-based need with an aim of providing all these through e-commerce methods. This approach

was followed so that the incorporation or the substitution of paper by electronic devices does not give rise to an exorbitant prices and imposition of a stricter regime of security for the people than the previous paper-based system. The court of law does not discriminate between a traditional paper record and its functional equivalent proof and similarly considers the signature on the paper and any equivalent digital signature at par with each other.

AIMS AND OBJECTIVES OF THE INFORMATION TECHNOLOGY ACT, 2000

The preamble of the act states, "*An Act to provide legal recognition for transactions carried out by means of electronic communication, commonly referred to as electronic commerce which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies*". So, the prima facie aim of the Information Technology Act 2000 was to recognize all the legal transactions undertaken through any media of electronic nature generally partaking in the field of E-Commerce and making them legitimate just like the paper-based methods. The act is therefore recognized as a facilitating, enabling and a regulating Act[10].

INFORMATION TECHNOLOGY AS A FACILITATING ACT

This act is regarded as a facilitating act as it assists both e-governance and e-commerce sectors. As captivating as the Model Law of E-commerce is, still, there was no trace of e-governance present under it. It was because of the vision of Indian legislators who saw the need of it and therefore took e-governance under the ambit of the act. The act deals with e-governance and e-governance practices covering 10 sections of "*Chapter* III" covering the issues of e-governance. These sections give the basic structure of all the regulations and rights conferred to the government officials and apply for both Central and State Governments. This act is applicable for the whole of India and it is India's first legislation of its nature granting "e-governance right" to the people of India.

[10] Cyber Laws in India - IT Act - Cyber lawyers, Legalserviceindia.com, http://www.legalserviceindia.com/cyber/cyber.htm (last visited Jan 8, 2021).

INFORMATION TECHNOLOGY AS AN ENABLING ACT

The act[11] is considered as an enabling act because it enables and gives recognition to electronic records and digital signatures. For making an e-record legally binding, the transactions and communications made in furtherance of it must contain the essential requirements i.e. an authenticity of the sender towards the recipient for removing the doubts of illegitimacy in the mind of the recipient, the two message's integrity which enables the recipient for determining the authenticity of the message received whether it is fabricated in between or not and the third, non-repudiation, which ensures the credibility of the sender. The act further recognizes *Digital signatures* and makes it at par with the physical world signatures. Digital signature is a misleading term and therefore, shall not be considered similar to that of a scanned handwritten one. It needs a key and a hash function for the decryption of it. This encryption of the signature is done so as to prohibit or restrict the misuse of it. The amendment of the 2008 recognizes the digital signature as equivalent to that of physical handwritten signatures. "*Adhaar based e-sign*" is one of the examples of electronic signatures legally recognized.

INFORMATION TECHNOLOGY AS REGULATING ACT

The act regulates cybercrimes. Cybercrime[12] as a term is a collation of cyber offences and cyber contraventions. This act not only defines offences but also provides a distinct redressing mechanism for the same. The act classifies cyber contraventions as the acts dealing with unauthorized access over a computer or a computer network. These are present in sections 43(a) to 43(j) along with 43A. Cyber contraventions generally results in a civil prosecution. On the other hand, the act also purports cyber offences mentioned between sections 65 to 74 which results in criminal prosecution.

SALIENT FEATURES OF THE INFORMATION TECHNOLOGY ACT

- E-contracts made legitimate
- Digital signatures are legally recognized

[11] Cherry TC, Cyber Jurisprudence Legalserviceindia.com, http://www.legalserviceindia.com/legal/article-3039-cyber-jurisprudence-.html (last visited Jan 8, 2021).

[12] Michael Aaron Dennis, cybercrime | Definition, Statistics, & Examples Encyclopedia Britannica, https://www.britannica.com/topic/cybercrime (last visited Jan 8, 2021).

- Provision for incorporating and adjudicatory tribunal for dispute resolution
- Procedure for electing the adjudicating officers
- Act applies to contraventions and offences committed outside the national territory of India
- Extends to whole of India

CONCLUSION

Cybercrime is one of the least-known forms of crime. Experts say that less than 10% of cyber crimes are reported to the authorities. In the traditional world, research has shown that the time taken to report a crime is one of the most important factors in determining the likelihood of arrest. Therefore, timely reporting of cyber attacks to the authorities is likely to strengthen legal rules and help deal with cyber threats in the long run. Some companies set a precedent for negotiating ransoms with cyber terrorists. It is estimated that gambling sites alone pay cyber blackmailers millions of dollars each year. The ransom sends a positive cognitive message and aggravates cyber attacks by making criminals more sophisticated and organized. With the skills, organization, and intelligence of criminals proportional to the possibility of evading crime, paying ransom will encourage the vicious circle of cybercrime. It also has some policy implications.

OBSERVATIONS

- There is no purely technical solution to the security related issues involving technology. Cooperation and collaboration among governments, computer crime authorities, and companies is essential to combat cyber-attacks. If governments work with each other and with the business community to modify institutions by defining appropriate policies for the security of the digital world, this will result in lower transaction costs. Some signs of success have been realized, but countries still have a long way to go before achieving moderate success. Enacting laws requiring organizations to deploy appropriate defense mechanisms and compulsory reporting of cybercrimes can help combat such crimes.

- Many countries are changing their regulations and systems in the direction of severe penalties. For example, the 2001 "American Patriot Act" brought cyber-attacks into the

definition of terrorism, with a maximum sentence of 20 years in prison. However, because traditional law enforcement agencies lack the skills required to deal with crimes, the possibility of arrest in cybercrime is very low. The severity of punishment is very important, but the more critical aspect of improving network security is the certainty of punishment. With more investment in the development of law enforcement capabilities, the likelihood of arrests may increase.

- Many underdeveloped countries lack the resources to investigate cybercrime. There is an urgent need for large and wealthy countries to provide assistance to these countries, especially those with a high rate of origin of cybercrime, in order to deal with global cyber threats from these countries. Therefore, managers and government officials can work individually or cooperate with eachother to eliminate or minimize the institutional forces that promote abnormal network behavior. In addition to formulating new laws to minimize cyber threats (changes in regulatory agencies), they can also develop strategies to change social norms (changes in regulatory agencies) that affect hacking. The whole industry is working hard to solve prevention, response and cooperation. All over the world, all walks of life are establishing Information Sharing and Analysis Centers (ISAC) to share real-time information about threats, vulnerabilities, attacks, and countermeasures. The nearest global. The Information Security Summit hosted by the World Information Technology and Services Alliance (www.witsa.org) brings together industries, governments and multilateral organizations from various economic sectors to share information and establish partnerships. The post-summit working group is now developing cooperative methods to solve the most critical information security issues.

However, it may be the legislative background of a country. Without the active participation and cooperation of global member states, the threat of cyber threats cannot be contained to the greatest extent. The nature of cybercrime itself has brought cross-border effects that undermine the wisdom of legislation. In India, since we do not have enough legislation covering all forms of cybercrime, it is necessary to join the respective international conventions and treaties so that we can formulate relevant municipal laws in this regard to enforce these regulations.