ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Cyber Crimes in India: Emergence of Laws with Emerging Trends

Kiran Dennis Gardner[1]

Department of Law, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh, India[1]

dean.law@Galgotiasuniversity.edu.in[1]

ABSTRACT: There is a universal saying that, every coin has two sides, same goes with the facility of internet provided to the major masses of public. On the other hand, it is also witnessed that, every facility has its own advantages and disadvantages, and the major disadvantage of internet nowadays is “Cyber Crimes”. Thus, this paper initially begins with describing the term “Cyber Crime”. Any sort of an illegal activity or crime committed, with the help or assistance of internet, in order to breach someone’s privacy, is known as Cyber Crime. Further the paper moves on to discuss regarding the ambit or scope of “Cyber Crime” in India, as in what all types of activities constitute as “Cyber Crime”, such as, fraud with respect to online transactions, phishing; hacking; trafficking etc. The paper concludes while discussing various anti-measures; regulatory provisions or prevention strategies, which are required in order to curb the increase in the rate of “Cyber Crimes” within India.

KEYWORDS: Cyber Crime; Cyber Law; Internet; Information Technology Act, 2000; India.

I. INTRODUCTION

Nowadays majority of our day-to-day tasks are performed through digital platform. Since we all realize, this really is the age in which much of the stuff is usually done over the phone, beginning with the online purchase. Because the internet is known as the worldwide level, from everywhere, everyone can access the internet services[1]. Internet has been used by the few for illegal acts such as inappropriate access to the network of others, fraud, etc. Any illegal activity or internet-related offensive system is considered cyber-crime. The word "Cyber Law" was used to deter or prosecute cyber criminals[2].

Cyber law can be defined as being part of the legal structures that connect with the Network, cyber warfare, and legal problems. It addresses a wide variety of subjects, including several sub-topics, and also freedom of speech, accessibility to and use of the Web, online privacy and security. Generally, it is referred to as the law of the internet[2].

Computer's invention has created life simpler for humanity, it is used for different purposes from the user to major organizations around the globe. In basic terms, we can describe the machine as the unit which can save and control people the user's directed information and instructions. For decades, many internet users have used the computer for the wrong reasons, either for their own gain or for the advantage of others. "Cyber Crime" gives rise to this[3].

This has contributed to the participation of society in practices that are immoral. Cyber Crime may be described as the offenses perpetrated using machines or computer systems and, in particular, the Internet, typically take place over cyber space[4]. The expression "cyber law" does not have a defined meaning, but we can describe it as the laws regulating digital world in a single phrase. Cyber regulations are the laws regulating the cyber industry. The Cyber Law recognizes cyber criminals, digitalized signatures, data security and privacy, etcetera[3].

Computer's brainchild has made human lives calmer, it has been used for many reasons, ranging from the individual to large organisations around the world. In basic terms, we can refer to the device as the system that can store and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

operate/process information or user-trained instruction. For special occasions, most device handlers use the computer either for their own gain or for the benefit of others since time immemorial. This helped in the birth of cybercrime[5].

This has contributed to the meeting of activities that are unlawful to society. Cybercrime can be described as the crimes that are keen to use mainframes or computer network and generally gross over cyber space, primarily the Internet. The word Cyber Law is now evolving. It doesn't have a static meaning, but it can be explained in a humble way as the rule regulating cyberspace. The rules governing the cyber zone are cyber laws. The Cyber Law acknowledges cyber criminals, visual and electronic fingerprints, personal protection and isolation, etc. The first Indian IT Act, which was based on the 'United Nations Model Legislation on Electronic Commerce' (UNCITRAL) model, was proposed by the UN General Assembly[6].

Cybercrime should not be termed as a singular definition, as a collection of actions or activities, it is better thought out. These activities are based on an item of material criminality that disturbs the data or systems of the machine. There are prohibited activities where a tool or target is a computer interface or content framework or the combination of both may be a mixture. Cybercrime is also classified as e-crimes, computer-related crimes, crime in elevation technologies, data age crime, etc. We may describe "cybercrime" in clear terms as a crime that happens over electronic communications or computer structures[7].

II. RESEARCH QUESTION

What is Cyber Crime? What all does it includes?
What are the Cyber laws in India?
What are the Cyber Crime prevention strategies adopted by India?

III. DISCUSSION

In order to get rid of offenses perpetrated via the web or virtual reality or via the use of computational methods, Cyber Security was born. Cyber law may be defined as a summary of legal issues relating with the use of networking or digital technologies. In this new transmission of development, cyber law plays a very significant role. As it covers almost all forms of events and transactions that actually occur whether it's on the internet rather than other contact devices, this is essential. Not whether we are conscious of it, but in Cyberspace every move and every response has certain ethical and digital legal opinions[8].

In order to remain aware of online fraud, one has the latest details once: one must study the cyber-crime extensively; basic understanding of the Web and the protection of the Web; read reports of online fraud. One should be informed of those offenses by reviewing such scenarios; Secure program from a trustworthy platform could be used to secure one's confidential details or knowledge; the effect of innovation on crime[8].

For illegal activity, cyber-crime is the most frequently identified. Cyber-crime is a tech professional's traditional methods, such operations are carried out by hackers to rob other information, access accounts, disrupt network and move money to accounts there. Cyber-crime involves criminal practices such as data intrusion, device intervention, e-mail harassment, hacking of passwords, theft by deception and computer theft[8].

Cyber rules are used to identify the problems connected with communication technologies. Likewise, digital world is the remote field legislation of the manner in which certain legal areas, including intellectual property, anonymity, freedom of speech, are property or material. Cyber law is an effort to structure the tiny, human actions that have taken place on the internet, with the real environment. Cyber legislation has a significant influence on operations which provides a broad cyberspace network[9].

Cyber law is a legal framework that addresses the network, cyber warfare, and the conflicts involved. It spans a wide field, covering many issues and subcategories, including freedom of speech, internet connectivity and use, and online privacy. It is also possible to refer to cyber law as the vulnerable internet. The IT Act, 2000 is classified as the cyber

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

statute, as revised by the IT (Amendment) Act, 2008. In Chapter XI, designated "Offenses" in which cyber-crime has been deemed prohibited by detention and fines as criminal offences. There are several good things to the 2000 IT Act. It also allows us to consider the crucial issues of defence[9].

The prohibited practices in which a processor and a network are complicated are basically certain kinds of fraud. The sizes of cybercrime cases are now the due to the proliferation of the internet, since there is no longer a need for the bodily appearance of the perpetrator while binding a crime. The unusual trait of cybercrime is that there will never be any interaction between the prey and the criminal. In order to minimize the risk of detecting and investigating, cybercriminals often prefer to act from countries with absence or poor cybercrime regulations.

There is a saying among people that only the World Wide Web or the Internet can be stubborn about cybercrimes. In fact, cybercrimes can also be tackled without intervention in the cyber environment, and it is not mandatory for the cybercriminal to stay online. Privacy in software may be seen as an example[10].

In order to turn over the offences committed over the internet or cyberspace or through the use of electronic assets, cyber law confiscated the homeland. Cyber Legislation may be considered an explanation of the legalized difficulties involved with the use of information or computer technologies. In this modern age of technology, cyber law plays a very vital role. It is relevant since it covers virtually all forms of events and communications that take place on the internet or other networking devices. Whether or not we are aware of it, but there are certain valid and cyber lawful opinions for each act and each answer in cyberspace[10].

IV. CONCLUSION & IMPLICATION

While seeing and witnessing changes and growth with respect to technology these days, the criminals or cyber offenders are also adopting and embracing with various new techniques and methods in order to commit the crimes and violating the privacy of the public, by phishing, hacking and various other frauds within the networking and internet sector. Therefore, with the increase in the rate of cyber-crimes, there is a high time to alter or amend existing laws and regulations in order to control the rate of cyber fraud with the change or growth in technologies.

Changes or preventive measures and regulations, must also be adopted by various different companies within the corporate sector in order to protect their company from the cyber-attack or fraud, in order to keep their operations and working alive and to protect their image or status amongst the global corporate sector. The companies along with keeping themselves updated with respect to the existing techniques and laws related to cyber-crimes or any amendment or revision regarding the same, the companies should also update their computer hardware and software along with new changes and technologies, in order to keep themselves one step ahead as compared to the criminals.

On the other hand, there comes the responsibilities of the various educational institutions, schools, colleges and universities, in order to create awareness and to improvise the teaching syllabus and to educate their staff members and students, with respect to the existing cyber laws or any amendment or revision in the laws and the crimes or fraud related therein.

Mankind is facing a great amount of threat from the ever increasing cyber-crimes and attacks globally all over the world. The main reason behind the same, is that the criminals or cyber bullies nowadays are keeping themselves one step ahead with respect to amended or revised technologies day-by-day, and this is where our laws and regulations fails. Hence, introduction or adoption of various regulatory measures and prevention strategies are highly recommended in order to raise awareness amongst the public, as protection of the country against the rise of cyber-crime plays a major role in welfare of the country, be it socially or culturally.

Transient territorial borders above the internet could be created for every section of the ecosphere of cybercrime, generating both technological and legal challenges to investigate and impeach these offenses. In order to take steps on the path to cybercrime, globally consistent efforts, guidance and coordination between different nations are compulsory. Our primary tenacity in scripting this paper is to range among communal citizens the substance of

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

cybercrime. We need to state at the end of this paper that cybercrime will never be accepted. If someone drops in the cyber-attack survivor, please take a step forward and report a case in your nearby police department. If offenders do not earn a punishment for their acts, they will not refrain at any moment.

REFERENCES

[1] M. Surabhi, "Cyber Warfare and Cyber Terrorism," *SSRN Electron. J.*, 2012, doi: 10.2139/ssrn.2122633.
[2] P. N. V. Kumar, "Growing cyber crimes in India: A survey," 2016, doi: 10.1109/SAPIENCE.2016.7684146.
[3] V. K. Gunjan, A. Kumar, and S. Avdhanam, "A survey of cyber crime in India," 2013, doi: 10.1109/ICACT.2013.6710503.
[4] *Cyber Criminology*. 2011.
[5] C. M. Abhilash, "E-commerce law in developing countries: An indian perspective," *Int. J. Phytoremediation*, 2002, doi: 10.1080/1360083022000031948.
[6] B. Arora, "Exploring and analyzing Internet crimes and their behaviours," *Perspect. Sci.*, 2016, doi: 10.1016/j.pisc.2016.06.014.
[7] A. Thapa and R. Kumar, "Cyber Staking : Crime and Challenge at the Cyberspace," *Int. J. Comput. Bus. Res.*, 2011.
[8] R. Chouhan, "Cyber Crimes: Evolution, Detection and Future Challenges.," *IUP J. Inf. Technol.*, 2014.
[9] P. Vats, "A comprehensive review of Cyber Terrorism in the current scenario," 2017, doi: 10.1109/CIPECH.2016.7918782.
[10] D. Halder and K. Jaishankar, "Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK, and India," *Vict. Offenders*, 2011, doi: 10.1080/15564886.2011.607402.
[11] Vishal Jain, Mahesh Kumar Madan, "Information Retrieval through Multi-Agent System with Data Mining in Cloud Computing", International Journal of Computer Technology and Applications (IJCTA) Volume 3 Issue 1, January-February 2012, page no. 62-66, having ISSN 2229-6093 .
[12] Vishal Jain, Mahesh Kumar Madan, "Multi Agent Driven Data Mining for Knowledge Discovery in Cloud Computing", International Journal of Computer Science & Information Technology Research Excellence Vol. 2, Issue 1, Jan-Feb 2012, page no. 65-69, having ISSN 2250-2734.