Journal of Law, Ethics & Society
A Publication of Jus Dicere & Co.

Issue 4 Publisher: Parag Agrawal

Cyber Law and Ethics: Issues, Impacts and Practices

Arvind Singh Kushwaha[1]

Abstract

The world in which we are living is more connected through computer networks than in social or physical manner. From the beginning of this 21st Century, we are living in the Cyber connected world, where almost each and everything works on cyber basis. But is this cyber too advantageous for us? Or it comes with disadvantages? The misuse of such information transmitted or available on internet also gave rise to cyber-crimes. Several countries made their own cyber laws to control and regulate these crimes. In addition, ethics are always seemed in an ideal position. By personal experiences, each individual can infer that the Cyber Law scenario is globally seems more complicated than any other traditional laws owing to the cause that the range of these activities which are to be governed by acts or laws are for the most part technology driven; an area which is not static rather changing dynamically and somehow is beyond anyone's control. However, the enactment of these cyber related laws lays opportunities for all nations. Threats of cyber crime is left unchecked will be disastrous on the nation, society, economy and security. In this paper, the researcher attempts to primarily bring in the understanding of the concept with some ongoing impact and practices including privacy and data protection issues with analyzing the Information Technology Act, 2000.

[1]Student B.A., LL.B.(Hons.), 2014-19, National University of Study and Research in Law (NUSRL), Ranchi.

Issue 4 Publisher: Parag Agrawal

Hypothesis

By the cyber means, we can operate within internet framework which specifies with the legal status of information and data transmitted. However, there are certain threats to this data protection which are not even covered the cyber laws of the country and if left unchecked it will be disastrous. It is the collective responsibility for all of us to ensure that technology is not abused in any possible manner.

Research Methodology

The research methodology opted for the purpose of this research is the doctrinal in nature. The relevant research used in this project is for the most part collected from secondary sources. The data includes Report of NCRB, Articles, Case-laws, Journals and Survey Reports etc. The proposal intends to capture the cyber essence in today's word while keeping in mind the lacuna in the IT Act, 2000 as well.

Introduction

The term 'Cyber' generally refers to the characteristics of the culture of computers, information technology, and now includes virtual reality too. The history of the computer dates back to the abacus and then calculation based tool, even its genuineness used to recognize in terms of the calculation speed. But, it was the internet which connected computers in a network consisting of a worldwide network of other computer that uses the TCP/IP network protocols to facilitate data transmission and exchange. It gave a huge access of information and data transmission to its user, but it is also having own pros and cons. This information could be classified in various forms as per the requirement of the user. However, information to one could be harm to another or affect in any form, which requires to be regulate and control, thus hereby the ambit of Cyber law arises.

When our country was hit by Globalization in 1990s, it was the era where the world was introduced with substantially growing internet; links were created in pattern of World Wide Web (WWW). The Computer Misuse Act 1990enacted by the United Kingdom was one of the earliest of such legal enactments which was enacted with purpose of securing computer material against any type of unauthorized acts, access or modification.2In today's world, it is difficult for us to survive without the Internet living in a city, whether it may be ordering food, calling cab, home delivery, booking tickets etc. Somehow, the Internet has become the Superpower in its own way and any being over the globe can access it, by just mere requirement of an instrument to access. Thus, Internet has turned out to be the Ultimate power and its developers know it.

However, with the growth of the information technology the misuse of it has also been expanding to the optimum level. Such misuse constitutes a form of new developed crimes; examples of such misuses are stalking, harassment, fraud, defamation etc. through cyber means i.e. by the use of information technology. Other methods obtained toward the 'misuse' goals are through spam, hacking, trafficking, and distribution of data. The posting and sharing of obscene material including indecent exposure and pornography (especially child pornography) also does constitute a misuse of information technology. It is estimated that losses through cyber crime are over $600 billion worldwide per year.[3] There is also corporate espionage by professional hackers in terms of $70 million ranging of proprietary information leaks and misuse. Although there are strict and new provisions under the IT Act for the cyber crime concerned, but the absolutely poor rate of cyber crime conviction does not helped the cause of regulating cyber crime in total.

2 Computer Misuse Act 1990, Available at: https://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf. Last Accessed on Feb 10, 2019 2000hrs.

[3]Economic Impact of Cybercrime Report | McAfee, Available at: https://www.mcafee.com/enterprise/en-in/solutions/lp/economics-cybercrime.html. Last Accessed at Feb 21, 2019, 1820hrs.

Issue 4 Publisher: Parag Agrawal

According to Robert Morris and Frank William Abagnale, many hackers intend to make use of their skills for their own better purposes. These types of trend continue even more now where companies hire the brilliant hackers as their security analysts. The enticement to use professional hackers for industrial espionage had also stems from the very fact that the physical presence required to gain access to numerous important documents is rendered needless if hacking can somehow ultimately retrieve those.

There is no particular definition of the cyber crime, however as the terminology states, it can be infer as any illegal act committed over or by using a computer network (especially through the means of Internet).Consequently, the cyber law refers to all of the legal and regulatory aspects relating to Internet and the World Wide Web (WWW). Thus, anything concerned or related or emanating to from any legal expressions or issues concerning any activity in and concerning Cyberspace comes within the ambit of Cyber law. The objectives of cyber law are to provide a comprehensive framework of societal and commerce by enabling laws which encompass aspects concerning security of information and network integrity and reliability and to create the right development of the communication and multimedia industry by keeping the view of content service.

It can also be inferred that although every crime is not inevitably a cyber crime, but the law enforcement shall become much more computer literate enough to be able to keep up with the criminal element transacted through information transmission. These cyber criminals may be a teenager, organized hackers, professional hackers or even crackers. According to BBC, the cyber criminal ambit also includes teenagers who have gone from simply trying to make a background for themselves, in order to actually working in unlawful manner. The financial incentive and benefits thereon attracts criminal use of internet and computer technology.

Usually in these types of cases, the law enforcement agency lacks the information and the tools which are needed to tackle the matter. Traditional laws neither does neither provides

for it nor fit the cyber crimes related. Moreover, during the judgment of privacy as a matter of fundamental right[4], several debates were ongoing over privacy issues being hampered. In his opinion, even Justice D.Y. Chandrachud referred to the breach of privacy over cyber information. Recently in Congress Google Hearing, the black box algorithms and privacy related issues were also put by the congress against Google. In this same hearing, Google CEO Sundar Pichai said that Google filters the entire world's information and then provides it.

With the change in application and law related to the cyber crimes, there is a need to acquire "cyber-jurisprudence" based on which "cyber ethics" can be substantially evaluated and criticized too. Furthermore, there is a dreadful need of constituting the code of ethics on the cyberspace, discipline and its application. In India, the first enactment of such nature is the Information Technology Act, 2000 which was passed when the country was facing the growing problems related to cyber crimes. As, the internet is the source for huge information and many of the communications around the globe, it somehow becomes necessary to take certain reasonable precautions while using it.

The Ethics refers to a set of moral principles or values, but where it is associated with cyber, it means the moral principles or guidelines that govern practices associated with the use of information and information systems. In this type of ethics, the cyber user(s) need to consider the moral standards or ethics applied when creating electronic publications, when storing, communicating and disposing of data and information.

Before the enactment of the Information Technology Act, 2000 (hereinafter referred as 'IT Act'), even an electronic mail (also commonly referred as email) was not accepted as legal form of communication and as evidence in a court of law under the prevailing statues of India. But the IT Act changed this scenario by giving legal recognition to the information

[4]See Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors., (2017) 10 SCC 1.

transmitted through cyber format. The cyber crime associated words such as hacking and damage to the computer code are defined under the IT Act to ascertain the act which could constitute cyber crime, as it is the statutory definitions of specific crimes which charges a criminal with the offence committed.

Prior to the enactment of the Indian cyber law, the corporate sector was helpless as there was no legal measures to address such issues, while they requires further use of technology in order to compete in sector. But the enactment after 2000had changed the view altogether. By the implementation of the enactment, in corporate sector, the companies were able under the IT Act to carry out e-commerce related business activity using the legal basis as provided. Prior to it, the growth of e-commerce was impeded in India; as there was no specific legal structure to control or regulate commercial transactions done online. It allows the companies to use digital signatures to carry out their transactions online, including digital signatures which have been given legal sanction under the IT Act.

Additionally, there is also information stored by the companies on their respective computer system and network, apart from having a back-up. Under the IT Act, it is now be possible for companies to have a statutory remedy, in case, if anyone breach into their either computer systems or networks and causes any form of damage. Initially, the remedy provided by the act is in the form of monetary, by the way of compensation, but it doesn't exceeds INR 1,00,00,000.

However, there were negative impacts also; the foremost issue is related to conflict of jurisdiction as enactment at several instances likely to cause it. As the cyber world doesn't consider any boundary, it is a very difficult task to frame laws accordingly in order to cover each and every prospective. But, a balance has to be maintained in cyber world and the laws need to be evolved on regular basis so as to keep a check on emerging different types of cyber crimes. On the other hand, the ongoing E-Commerce market is mainly based on acquired system of domain names. The domain name is not been defined under the act, subsequently,

the rights and liabilities of domain name owners are not mentioned in the law. These domain names differ from one another in several aspects from country to country, content etc.; in this aspect, the enactment does not concern the issues regarding to the domain names.

The IT Act also does not deal with any type of issues relating to the protection of intellectual property rights (IPR) in the circumstance of the online usage of internet, rather it left out to be covered under 'ethics'. The disputatious yet very important issues regarding copyrights, trademarks and patents on internet have been left untouched by the IT Act, which ultimately produce many loopholes.

It can be seen that as the cyber law tends to be growing, so are the new classes, forms and manifestations of the cyber crimes. The offences related to cyber law defined under the IT Act, doesn't seems to be exhaustive in nature. Nonetheless, the drafting pattern of the relevant provisions of the act makes it seem as if the offences detailed therein are the only cyber offences possible and existing in the practical world. The act does not cover other several kinds of cyber crimes and crimes done by the means of internet, such as Cyber theft, Cyber stalking, Cyber harassment, Cyber defamation, Misuse of credit card numbers, chat room abuses etc. Another left ambit is that the act does not provide for any form of anti-trust issues. Furthermore, the IT Act has not undertaken other numerous vital issues pertaining to e-commerce area like privacy and content regulation on the websites. After the K. Puttuswamy judgment, the privacy issues even in the online world carries a fundamental importance which has been left untouched by the act, which can only be ratified by the way of amendment.

The gravest concern about the Indian cyber law is its implementation. As, the IT Act does not lay down any parameters for its implementation. Additionally, when the internet insight in India is extremely low; the Government and police officials, in general are not very used to cyber forms, the law more or less itself raises more questions than it had to answer. It seems that there is a high requirement of amendment in the act in order to remove these rising gray

areas. The Digital India is one of the best initiatives to educate and empower the nation and its citizens in digital form but there was no as such substantial impact. Also, this initiative is only related to 'empower' prospect only, not to the data protection or cyber crime.

Conclusion

At a time, computer and associated networks are one of the necessary requirements toward development. As mentioned above, it plays an important role in an individual's day to day life, regulation to it seems somehow necessary. As we are developing and growing toward the 'developed nation' form, we also required to diminish these cyber loopholes whether it may be concerned with practice, ethic or criminal in nature.

The latest statistics of the National Crime Records Bureau (hereinafter referred as 'NCRB') report, 2017 shows that cyber crime is on rise in comparison to the previous years. However, it shall also be kept in mind that many of the cyber crimes go unreported in India. Consequently, it cannot be said that cyber crime does not exist and that our society is safe from the cyber crime.

Also, there is a high necessitate of a new legislation which can cover all the aspects of the cyber crimes; should be passed so the grey areas of the law can be removed. New amendment(s) shall be introduced and new provisions shall be inserted in the IT Act, 2000 to make it substantially efficient and more active against the cyber crimes. The Government can maintain the necessary amount of control over "cyberspace" to ensure that public interest objectives are met and that cyber crime is minimized. Ultimately, it is always advisable to be a disciplined user.