Cyber Security and Safe Computing: Need of an Hour which needs to be solved

Sunidhi Kashyap[#1], Kuldeep Chand[*2]

[#] *Law Department, Maharaja Agrasen University*
Solan, Himachal Pradesh-173212

[1] nidhi1813@gmail.com Contact no.-9625062432
[2] dogra.kuldeepchand@gmail.com Contact no.-8219279952

***Abstract*— As a popular statement which always says in criminology that a crime will occur only when the favourable circumstances account itself to do so. Till now, all of us were familiar of only conventional types of crimes which includes felony, forced sex, stealing, burglary, break-in etc. But today with the advancement and growth of science and technology which came in this era through machinery like computers and convenience like internet. The world of cyber has unlocked an entire fresh virtual paradise for the public, which is both right and wrong, and childlike to access and communicate with many different civilization and sub-civilization, topography and census being no hurdle. The similar honour of www when went to wrong hands or when abused by public with corrupted minds and wrong goal, make it a virtual misery. Description of copyright stealing, hacking, and cracking, bug attack and plain trick etc. have grown up in earlier years. As a conclusion of the fast acceptance of the internet worldwide, computer crimes are boosting like mushrooms. The authority has been disappointed by the failure of the administrator to keep cyber-crime law in front of the quick moving technological arc. At the same time, the government aspect the requirement to equal the challenge between individual privilege known as privacy and free speech and the want to safeguard the sovereignty of the globe public and private networks. The globally thing of internet today has become a correspond type of life. The computer network is becoming part of life.**

***Keywords*–** Cyber Security, Internet, Prevention, Cyber Problems, Legislations

I. Introduction

Internet has empowered the requirement of website exchanging information, e-mail, and a lot of period Information Technology resolution for the welfare of mankind. Cybercrime is appearing as a severe danger. Universally officials, police authority and intelligence units have begun to respond. Eagerness to check cross border cyber danger are taking structure. Indian police have started special cyber cells beyond the country and have also initiated the personnel. Crime and criminality have been merged with individual since his fall. Crime means mysterious and ever struggle to conceal itself in the face of advancement. Various nations have approving different planning to fight with crime depending on their nature and range. One thing is confident, it is that a country with huge occurrence of crime cannot evolve or advance. That is so because crime is the oversee opposite of growth. It left with bad civil and financial result. Cybercrime is characterized as crime which is done on the internet using the computer like a tool or a targeted sufferer. It is difficult to categorize crimes in common into separate entities as many of these crimes develop every day. Even in the actual nature, atrocity like forced sex, killing or staling does not obligate to be disconnected. Nevertheless, all digital offences include both the data processing machine and the human behind its suffering; it just relies on which of the main compulsion is there. Therefore, the computer will be visually seen either as an instrument or the main aim to do crime. For instance, hacking draw in assaulting the computer's details and other assets. It is significant that coinciding appears in many cases and it is difficult to have an ideal categorization system. The word cybercrime is a misnomer. This part has not been explained in any statute or act passed by the Parliament. The aspect of cybercrime is not completely dissimilar from the aspect of traditional crimes. Both contain action whether it is act or breach which causes the violation of rules of law and it equals by the legislature of the state. Before assessing the approach of cybercrime, the traditional crimes be discussed and the headings of same abnormality between both these types were there. When computer is used by the person as an instrument as the main goal it can be taken as a form of cybercrime, the Personal Computer can be treated as tool rather than the object. These offences are commonly including fewer high-tech specialist as the destruction done exhibit itself in the actual world. People defects are commonly abused. The injury deal is mainly intellectual and unreal, making juridical action against the variable impossible. These are the crimes which have presented in the previous ages offline. Swindle, cheating and the likes have been living even before the advancement in technology supplies. The same offender has been given a device which boost his promising pool of sufferer and makes him all existed to handle and capture. These computer crimes are done by a picked group of offenders. Unlike crimes using computer as an instrument, these crimes obligate the high-tech ability of the criminal. These crimes are basically recent, having been in presence for only if Personal Computer have which details how unaware the society is and the globally in general is towards fighting against these crimes. There are number of crimes of this nature done daily on the cyberspace.[1]

II Review of Literature

The review of literatures plays an important part in any research work, the review of previous marks the work of the scholar in its own way. Under this topic, an attempt has been made to review the literatures which are available and to put some efforts for the meaningful research work. The researcher finds few books, journals, articles related to this topic. Much credit is to be given to those whose work not only makes the students understand about the topic but also clears the basics of the related subject.

J.W.C Turner (1966) explored the ongoing series of elementary legal studies. This book outlines the understanding of the rules of criminal law as to make the clear idea of the practical task confronting the prosecution and defence in the trial of specific people. Its emphasis on the law and legal history made the author book more special in the law field.

R.C Nigam (1965) examines the particularity of crimes in India and their effect in society. His work mainly in the doctrine of mental element of crime and the act committed by the criminals are the main highlights of his book. While the study reported factors such as mind, crime and how the society mainly dealt with these types of conflicts in the culture of our country.

Talat Fatima (2011) supports the conduct and identifies the special legal problems which the Internet has created and examines the ways in which these are dealt with under Indian law. It includes various types of cyber crimes description like Cyber defamation, Cyber bullying, Cyber Squatting etc. The protection of Intellectual Property Rights has also been included which now-a days are the most common topic in Internet. Cloud Computing and Information Technology Amendment Act have also been analysed and discussed in the light observation of the Hon'ble Supreme Court. It also highlights the common principles which are used globally to regulate the use of net and compares it with Indian Scenario.

H.L.A Hart (2012) is widely recognized as the most important work on the concept of law and legal philosophy in the twentieth century and also remains the starting point for most students coming to the subject for the first time. It mainly tells about the subsequent developments in social and political philosophy and highlights the central work on the law, commands and orders, the variety of law, justice and morality, law, and morals etc. It also clarifies the modern social and political theory.

III Objective of the Study

The following are the main objective of the study are as follows: -

- To study the concept of safe use of computer and digitalisation.
- To analysis the reason of cloud computing in the era of Internet
- To examine the factors for crime like men's rea and actus reus.
- To find out the latest laws in the country for the prevention of the crimes in the cyber world.

IV Research Methodology

Since it is a doctrinal research, the study is based on purely based on the theory work. The methodology is based on method of case study which are concerned with primary sources and secondary sources which includes the judgements which are passed by the Supreme Court and High Court and it also includes the help of other sources like Books, Articles, Indian and foreign Journals, Literature Review, Newspapers, Debates, Commentaries and many other websites. Various Codified Laws, News Weekly, International Conventions has been studied an analysed to gather information about this research. In short, it can be said that the work is based on theory research to analyse the study.

V Doctrine of Men's Rea & Actus Reus in Cyber Crime

As far as Traditional Crime is concerned Men's Rea and Actus Reus are the two most important elements to crime. Actus Reus means "Such result of human conduct as the law seeks to prevent".[2] There must be commission or omission to do an offense. As far as men's rea is concerned, it means "A guilty state of mind".[3] The mental element forms the other important ingredient of crime. The act remains the same while the state of mind makes the act 'reus' and hence an offence. Almost all the crime requires proof of mental element of some sort. As far cybercrime goes it is impossible to determine the men's rea in cybercrimes. In Cybercrimes, one should see what the state of mind of hacker was and that the hacker knew that the access was unauthorised. Thus, a "Particular Computer" needs not to be intended by the hacker, it is enough if the unauthorised access was to "any computer". Awareness on the side of the hacker becomes easier to prove where he is an outsider and has no authority to access. But where hacker is already has limited authority as ion the case of the employee of a company, it becomes difficult establish that he exceeded his limits and was even aware of the case that he is exceeding it. Actus Reus in cybercrimes has become a challenge as the complete action is done in abstract environment. The perpetrator may leave some footmarks in the machine itself though it becomes a herculean task for the law enforcement machinery to prove it in the courts, as it is considered to be in physical form or in such a form where it becomes admissible in evidence.[4]

VI Factors Responsible for Cyber Crimes

Professor H.L.A. Hart in his meaningful work named 'The Concept of Law' had enacted that individuals are exposed to illegal acts which are felony in the eyes of law and rule of law must be there in order to safeguard them against such illegal activities. Applying the similarity to cyberworld, the PC despite being high technology devices are more exposed. This automation can efficiently be utilized to harass an individual or his network by illegitimate entry to it. The damage so caused to the victim may be direct or indirect result of abuse of computer systems. In the state of not being present of any solid proof mechanism to assure and preserve innocent computer users against cyber criminality, the cyber criminals indulge in criminal activities through networks unabated without any fear of being apprehended and tried for the offence committed by them.[5] The following are the factors responsible for the evolution of cybercrimes. Huge Data Storage Capacity is the first reason which is responsible for the emergence of cybercrimes. The computer has a capacity to store huge amount of data on a small space. A small micro-processor computer chip can store lakh of pages in a CD-ROM. The data stored in ROM will always remain safe and not destroyed even if the power is turned off. A cybercriminal can intentionally get the large scale of secret or official data from the other person personal computer within a few minutes. This leads to increasing cybercrimes. Computer System's Complexity is the second factor which is responsible for the emergence of cybercrimes because the computers work through operating systems which are consist of abundance of secret language system. Due to the fallible nature of Human's mind there is always a chance for lapse at any level of processing. The cyber criminals are always ready to take undue advantage of these chances of lapse and get access into the computer system. These types of criminals are known as hackers on the cyber space who tries to exploit the weaknesses in existing operating systems and security devices. Negligence of Network user is the third reason which is responsible for the cybercrimes because negligence is closely related to human conduct. There is always a probability that there might be any negligence on the component of network user while he is trying to protect the computer system. This negligence leads to a chance for the cybercriminal to gain unauthorized or illegal access or control over the computers and commits crime. Evidence unavailability or loss is the fourth reason which is responsible for the emergence of cybercrimes**.** Now the digital computer processing and network technology have replaced the traditional methods for producing, storing, transmitting, and disseminating information or records. Due to the emerging nature of cybercrimes the issue raises before the law enforcement and investigating agencies is for procuring and preserving evidence against the cyber criminals. As compare to traditional offences, it is exceedingly difficult to collect sufficient evidence of a cybercrime for found him guilty of the cybercrime beyond doubt. Due to the anonymity, providing by internet, the cyber criminals are encouraged to indulge in criminal activity without leaving any evidence and if in some cases the evidence is left then it is hardly possible to convince the police for registering a case against that criminal. In the modern time due to the inadequacy of traditional methods of evidence and crime investigation it becomes necessary to adopt the new techno-legal procedure called cyber forensics. In the cybercrimes, the forensic experts are playing an important role in collecting and presenting admissible electronic evidence and search and seizure of material evidence relevant to the cybercrime under investigation. Instead of this hard work there are still certain grey areas which enable the cybercriminal to make tampering with the evidence for the purpose of misleading the investigating agencies. Broad approach to details is the fifth reason which is responsible for the emergence of cybercrimes. Computer is defined as an electronic device which performs function through complex technology rather than manual actions of human beings. The connection to information assets is the main gain of computer networking in the cyber age. More and more organizations are resorting to networks for providing easily accessible information to their employers, customers, and parties with which they deal. In the present information age this is the reason why networking and cyber activities are increasing day by day. Due to the information dissemination through World Wide Web, new resources have been created for faster and cost-effective access to information throughout the world. This facility leads to involve in crime commission on the cyber space. Jurisdictional uncertainty is the last factor which is responsible for the emergence of cybercrimes**.** Cybercrimes cut across territorial borders which undermine the feasibility and legitimacy of applying domestic laws which are normally based on geographic or territorial jurisdiction. Cybercrimes are committed through cyberspace network interconnectivity and therefore, they do not recognize geographical limitations because of their transnational in nature.[6]

VII INFORMATION TECHNOLOGY AND INDIA

Responding to initiative, India drafted her first law on electronic commerce; the Electronic Commerce Act, 1998 with Electronic Commerce Support Act, 1998. It recalled the rapid development of Information and Communication Technology revolutionizing the business practices; the transactions accomplished through electronic means-collectively electronic commerce creating new legal issues; the shift paper-based to electronic transactions raising question concerning recognition, authenticity and enforceability of electronic documents and signatures; and the challenge before lawmaker of striking a balance between conflicting goals of safeguarding electronic commerce and encouraging technological development.

VIII LEGISLATIVE LAWS ON CYBER LAW

The law regime of cyber law comprises the Information Technology Act, 2000, Indian Penal Code, 1860, Indian Evidence Act, 1872, Criminal Procedure Code, 1973, the Bankers 'Book Evidence Act, 1891, the Reserve Bank of India Act, 1934. Since the Indian Penal Code is the substantive criminal law of the country which was drafted centuries ago when even the computers were not in existence, therefore, the code deals with only the traditional crimes. To attune the Code with the genesis of the cybercrime and to encompass the cybercrimes within its ambit necessary amendments were introduced in the Code to make it effective in support of the I.T. Act. Similarly, necessary amendments have also been introduced in the Indian Evidence Act to take note of the documents which are preserved in the computer system and its accessories so that they can be admissible in evidence during the period of the trial.

IX CONCLUSION

It is made negotiable from the past surveys and evidence that with the increase in automation of cybercrimes also increases gradually. Expert individuals done offence more so there is requirement to be familiar with the principles and main PC morals which should be used in proper way. Cybercrime and hacking are not going to decrease rather it will increase day by day. By acknowledging the previous things, one can gain from them and utilize that detail to avoid future crimes. Cyber legislation is required to modify and emerge as speedy as hackers do if it has any longing of governing cybercrime. Statute must search an equilibrium among safeguarding people from crime and breach on their rights. The important criteria about the web is how fast and chargeless it is. There will forever be fresh and surprising dispute to stay one step forward from the cyber offenders and cyber terrorists, we can only win these battles from them only when mature partnership and merger is there between public and authorities. There are many things which can be done to make sure that the privacy, protection, and fiduciary computer surrounding must be there. It is important to our country well-being and for the security of our country crucial and economy. Yet India has taken a lot of steps to stop cybercrime, but the cyber law cannot afford to be static, it must change with the changing time. The tremendous growth of internet use in globe and mainly in India is escorted by the substantial surge in cybercrime and has made India vulnerable to such crimes. Cybercrimes are of global nature and criminals are not bound to a geographical area. Cyberspace is a demonstrative, inconclusive and not guarded by local geographical constraints. These offences cannot be blocked by the local legislation, India in such things are mostly sit idle. India in order to strike cyber-crime has merged itself in many bilateral agreements like the treaty of cyber with Russia and a foundation contract with the US, presently visited P.M. of India Mr. Modi to Israel to ratify Indo-Israel cyber building is another work of India to make its cyberspace.[7]

Acknowledgement

I would like to express my very great appreciation to my guide Kuldeep Chand for his valuable and constructive suggestions during the planning and development of this research work. His willingness to give his time so generously has been very much appreciated.

References

[1] Kamini Dashora, "*Cyber Crime in the Society: Problems and Prevention*", *JAPSS*, vol.3, pp.240-244,2011.

[2] J.W.C. Turner, *Kenney's Outlines of criminal law*, 19th ed., University Press, Cambridge, 1966.

[3] R.C. NIGAM, LAW *of Crimes in India*, Asia Publishing House, New York 1965.

[4] Talat Fatima, *Cyber Crime* 1st ed., Eastern Book Company, Lucknow,2011.

[5] H.L.A. Hart, *The Concept of Law*, Oxford University Press, England, 2012.

[6] Deepa Kurup Report, The Hindu, 2011.

[7]Shubham Kumar, Santanu Koley & Uday Kumar, "Present Scenario of Cybercrime in India and its Preventions", *IJSER*, vol.6, p.1975, APR.2015.