International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 4 Apr. 2021, pp: 577-583 www.ijaem.net ISSN: 2395-5252

A brief study on Cyber crime and laws with reference to new technology in India.

Rambha Kumari
Assistant Professor Harlal School oF Law; Greater Noida

Submitted: 15-04-2021 Revised: 28-04-2021 Accepted: 30-04-2021

ABSTRACT: The word "cybercrime" is in the mouths of almost everyone involved in the use of the computer and Internet, be it individual, corporate, organization, national, multinational or international. The notice accorded cybercrimes is not farfetched; on the one hand. It is partially rooted in its inevitable nature as a result of the fact that medium via cyberspace is the exact means by which social synergy, global trade, and commerce transact. On the other hand, the economic losses to which all citizens stand revealed whether now or in the nearest future. Besides financial losses, other consequences of cybercrimes include. This paper presents that, it is not as if proper laws and regulations are not in place because some advanced countries in the world have in one form or another, laws against cybercrimes, yet, the challenge of cybercrimes remains intractable and bewildering. As countries across the globe strive to curb cyber crimes through the instrumentality of the law, so are the cybercriminals devising new and sophisticated techniques to further their trade, thereby rendering impotent, the existing legal measures.

Keywords: Cybercrimes, cyber criminals, challenges, enforcement, economic losses

I. INTRODUCTION:

The Origin of Computer has made the life of humans easier, it has been used for numerous purposes starting from the individual to large organizations across the world.. In simple terms we can define a computer as the machine that can store and manipulate/process information or instructions that are instructed by the user. Most computer users are utilizing the computer for the erroneous purposes either for their personal benefits or for others benefit since decades ``Cybercrime" unites the term "crime" with the origin "cyber" from the word "cybernetic", from the Greek, "kubernân", which means to lead or govern. The "cyber" environment comprises all forms of digital activities, regardless of whether they are carried through networks and without boundaries. This enlarges the previous term "computer crime" to encircle crimes perpetrated using the Internet, all digital crimes, and crimes including telecommunications networks. This more recent terminology includes a broad variety of aspects, leading to different ways, depending on the prevailing culture of the experts, making it look either diminished or enlarged, in varying dimensions, dispensing with rising problems that also show its heterogeneity. Crime is a social and economic phenomenon and is as old as the human in society. Crime is a legitimate notion and has the command of the law. Crime or an offence is "a legal wrong that can be accompanied by criminal procedures which may end in punishment." The sign of culpability is that it is a transgression of the criminal law. As per Lord Atkin "the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences".

A crime may be said to be any conduct followed by act or omission forbidden by law and significant rupture of which is sensed by penal consequences. Cyber Law took birth in order to take control over the crimes committed through the internet or cyberspace or through the uses of computer resources. Description of the lawful issues that are related to the uses of communication or computer technology can be termed as Cyber Law.The increasing extent of computers and the internet has made it easier for people to stay in touch over long distances and help for aims associated with business, education, and culture among others. Despite, the means that let the free flow of data across boundaries also give rise to a concerning high number of reckless behavior. Any technology is able to beneficial uses as well as misuses. It is the job of the legal system and regulatory agencies to keep pace with the same and ensure that newer technologies do not become instruments of exploitation and harassment. However, important legal questions have risen in many circumstances. The World Wide Web allows users to disseminate content in the form of text, images, videos, and sounds. Websites are built and updated for many useful purposes, but they can also be used to share offensive content such as pornography, hate speech, and defamatory materials. In various cases, the intellectual property rights of authors and artists are infringed by the illegal distribution of their works. There have also been arising cases of financial fraud and cheating in connection with financial activities carried online. The digital interface provides the suitable shield of anonymity and fake identities. The itinerant persons become more invigorated in their offensive act if they think that they will not bear any consequences. In recent years, there have been many records of internet users getting gratuitous e-mails which usually receive obscene language and amounts to harassment. Those who post personal information about themselves on job and marriage to websites or social networking websites are usually at the receiving end of ‘cyber-stalking'. Women and minors who post their contact details become chiefly vulnerable since lumpen elements such as sex-offenders can use this data to target probable victims . The principal target of my paper is to spread the knowledge of the crimes or offences that take place through the internet or cyberspace, along with the laws that are imposed against those crimes and criminals. We are additionally trying to focus on the safety in cyberspace.

II. FEATURES OF CYBER CRIMES:

2.1 Technological Aspect of Cybercrime:

From a technological aspect, other experts look out the basis for a general term, such as "electronic crime" or "e-crime", thanks to the confluence of ICT, including mobile technology, telephony, memory, surveillance systems, and other technologies, in addition to nanotechnology and robotics, which must be taken into account from now on. These electronic media will be targeted frequently more usually and will also be used to hide, perform, or assist crimes and offences. Particularly the positive acts for which one or more means were utilized to do one of the ingredients of the offence can be included.

2.2 Humanistic Perspective of Cybercrime:

From a humanistic perspective, cybercrime begins from several populations and displays socio-educational, socio-economic, and techno-ideological factors and their creations, as well as morbid looks like an obsession. The disorder of the education system may add to the rise of new kinds of cybercrime or wrong methods and ways with different levels of austerity, including cheating and reputational harm, which can be associated to disappointments and the redefinition of substance and citizen values, incompatible with what is required when addressing and leading an adult life. Difficult socio-economic conditions also include the Internet as a place for expressing psychological troubles with socio-economic origins, including theft, child pornography, and calls for uprisings, violence, and hatred. With regard to techno-ideological factors, one must consider sites and networks aimed at propaganda, destabilisation, and individual and mass psychological manipulation using methods that involve the digital processing of images, videos, and audio.

2.3 Cardinal Aspect of Cybercrime:

From a cardinal aspect, cybercrime is seen as an offence to cyber-security, particularly attacks to digital networks for the purpose of seizing control, paralysing them, or even destroying infrastructures that are vital to governments and sectors of vital importance.

III. IMPACT OF CYBER CRIME:

This section shows the results regarding the impact of technological revolution and gain of dominance–or rather, of the increase–of cybercrime during the 2010 to 2020 decade.

3.1 Study of the Impact of Cybercrime:

The impact of cybercrime is tough to recognize. Yet, there is progress in the growth of information technology and the accomplishment of susceptibilities among cybercriminals, a gap between legal and nefarious countries, and an ambiguity related to technological advancements and findings. It is always important to recognize that technology itself is inactive. Still, its use can be defined as adverse or real. This is notably true in cryptography, adopted for acquiring transactions and data exchange as well as to ensure information including unlawful actions and the endowment of evidence. History reveals that new technologies, remarkably regulated and not wholly impeccable, are both utilized for good and bad.

The next ten years will be considered by flux, with the need for an opportunity, real-time interface, accordance, and a dependency on digital identity devices and peril. This decade will also add controlling robots operations and more new perils.

3.2 Antagonistic Progress With Respect to Cybercrime:

The proposed growth, which may have an adverse bearing on cybercrime, bring small contrast between work life and private life, using, for example, the problem of finding information for a company and Web applications with cloud computing, targeted secrecy malware, and more frequently, the extensive use of new technologies, including mobile and wireless technologies, and a simple exposure to social engineering, social networks, and mobile downloads carried out less securely than in the past. We must emphasize the volatile nature of finding data as evidence and the difficulty of reporting offences to the sources, with no legal means, because cybercriminals are acclimating alongside new technologies.

3.3 Assertive Advancements with Respect to Cybercrime:

Security measures based on these same technologies could have a true impact. Security is fundamental to the problem and must be based on policies and be strictly enforced. It will be a major challenge with cloud computing, due to the intricacy of where data is saved and the diverse rights including, main hazards linked with administration and territoriality. The adequate level of quality security will be a pivotal part in the approval of these new services.

IV. CYBER CRIMES AGAINST INDIVIDUALS:

Against Individuals: –

Harassment via emails a) Email spoofing (Online a method of sending email using a false name or e-mail address to make it appear that the email comes from somebody other than the true sender.) b) Cyber pornography (exm.MMS)

Cyber-stalking.

Dissemination of obscene material.
Defamation. Unauthorized control/access to a computer system.
Indecent exposure
Email spoofing
Cheating & Fraud Breach of Confidentiality

4.1 Computers as a Target of Crimes:

Due to the Home PC, the use of computers has expanded extensively, such computers can enhance the target of crime both in the material or in a practical way, i.e. parts of the computer can be stolen, for example the hard disk thus pointing to physical break-ins. Illegal access to the computer heading to intimate data loss will amount to the virtual targeting of the computer, this will amount to a 15% crime of data theft, which is described as hacking in the normal parlance. The other kinds of crimes in which the computer is the target cover offences such as–Blackmail based on the information stolen in the form of medical information, personal data etc. this section can also add offences like the theft of Intellectual property, or, data of corporations like the marketing information etc. Moreover, these crimes could also be committed with a vicious intention by creating delays in the business plan. The expanding access to the government accounts and obtaining false passports, driver's licenses, manipulating the tax record, land record, accessing the intelligence files etc. The type of victims targeted also assists in building the typology of the Cybercrimes Individuals: Most of the cybercrimes fall under this type, cyberstalking is an example of an individual being harmed by internet, or an individual may be impaired even though he may have nothing to do with the cyberspace but nevertheless be victimized for example online baking transaction frauds perpetrated by hackers who gain entry into the computer systems of the banks.

4.2 National Security:

Email, as it is commonly pointed to, began enriching utilized for military purposes. By the expansion of the World Wide Web, this technology was initiated into the public domain. This is the starting point where the virtual means commenced being utilized for criminal actions, and with the expansion of terrorism, the terrorists also have embraced this technology. The terrorist's organizations all over the world have begun using the internet to disseminate their doctrine, and also for causing an inefficiency to their treacherous actions against any nation or society at large. Moreover, there are efforts done by terrorist organizations to obstruct the information centers of the states, so that their actions could be brought with excellent impact causing harm. In the context of national security, notably viz. military applications information operates a significant role, on the basis of which military victories become definitive. This contest of intelligence and counterintelligence is brought out in the virtual medium as utmost of the military actions and the information administration of most of the advanced nations is based on the application of computers and the internet. Therefore interrupting the information's network of the forward nations by the virtual medium has become a cost-effective technique exercised by nations who do not have military supremacy.

4.3 Economic Crimes:

This is one of the most broadly committed crimes and with the society with every passing day more and more members of the society holding e-commerce as a means to do commerce, crime in the virtual medium will be one of the main quandaries which will inevitably be expected to be carried by the power of law. Major economic crimes under this classification are: Hacking, Virus, Cyber frauds, Software piracy and violation of copyrights, Industrial espionage by rival corporations Forgery and counterfeiting etc.

The content of the information also sets the base for analysis in selecting the typology of the Cyber Crimes–The quantum of information being swapped on the internet is beyond insight. Not all the information being interchanged on the net has endured within the limits of public morality, so the net has grown a lush terrain for the exchange of immoral information further driving to abuse of the right of freedom of speech and expression.

4.4 Society is Dynamic:

However due to active technological progressions in communications and the computer technology have left the law tracking back to such an area that it is meeting the difficult hurdles set by the criminals of the new generation, who commit modern crimes with the aid of technology. The main advantage of the net is to transfer files, exchange emails, for video conferencing, and the latest to combine for these different purposes of communications is voice interface. These above-mentioned kinds of communications are brought out between the computer and a distantly accessible host computer. This form of communications matches all the more relevant in the age where E-commerce has grown an assured means of doing business.

4.5 Jurisdiction:

Territorial control on the internet becomes a peripheral character in the virtual medium as the web pages on the net can lead nearly every region in the nation and perhaps almost every nation on the earth. This is where the point of discord between the cyber world and the territorial world starts. As in the territorial world, there are barriers set up by the autonomy of the nation which is not the case in the cyber world. A legal system can work efficiently if it is well set; it is these laws that recognize every practical perspective of the legal system including the power of the courts. A court in order to achieve efficient decisions must have just and well-defined jurisdiction, as without a jurisdiction the court's judgments would be futile. Jurisdictions are of two types namely, Personal and Subject Matter Jurisdiction, and for a judgment to be effective both these types must exist simultaneously. Moreover, the common basis as to a party can sue another is at the place where the defendant resides or where the cause of action arises. This itself is the enigma with Internet jurisdiction as on the net it is difficult to prove the above two criterias with conviction. The problems of this type have added to the total complexity and inconsistency that pandemic legal decisions in the field of Internet jurisdiction.

The IT Act, 2000 passed in India is a classic example of the obscure law in the area of jurisdiction in the context of the Internet. Section 1(2) provides that the16 act shall enlarge the whole of India and, save as otherwise provided in this Act, it also refers to any offence or violation thereunder committed outside India by any person. So, Section 75(2) provided that this Act shall apply to an offence or infringement committed outside India by any person if the act or conduct establishing the offence or violation involves a computer, computer system or computer network located in India. Such a provision seems to be against the principle of justice. Moving to the next level, let's say even if the Indian court strongly advances jurisdiction and passes a judgment as per the above provisions of the IT Act, 2000, the other question that appears. Will the foreign courts implement such a judgment? In case of the above position, the only way to settle such a conflict is by means of having an extradition treaty with the host nation and India, further, it has been suggested by that the Indian court emerges legitimate terrain on which the extra-territorial jurisdiction may validly exercise, as done by the American Judiciary1. From the above, it is important to understand the complexities associated and thus it becomes essential to understand the nature of Cybercrime, and whether the present penal laws are sufficient. When Macaulay came up with the Indian penal code in 1860 the concept of Cyber Crimes was completely unexplored. Further, until the IT Act, 2000 was passed there was no legal provision viz. Cyber Crimes; this was the individual basis along with verifying activities brought on by means of electronic communications to expand e-commerce, with which the IT Act, 2000 was enacted. Moreover, a blanket provision was made under Section 77 of the IT Act, 2000 which provides that the penalties or confiscations provided under the IT Act, 2000 will not exempt an offender from obligation under any other law, in short, the substantive provisions of the IPC are still relevant to Cyber Crimes committed in India.

V. TYPE OF ATTACKS:

5.1 Attacks on Electronic Identity

Electronic identity theft, resulting from acts of blocking and data theft, will increase, especially through social engineering, currently carried out in cybercrime working malware tools and powerful methods, such as phishing and spamming. The personal data will remain to be prevented from personal systems, businesses, and communities over time, given their increasingly high tech nature, for financial gain and other reasons.

5.2 Attacks on Minors:

Child pornography is supposed to rest even in terms of material joined acts. This form of crime relies on "human material", with children victimised by acts of pedophilia or forced to engage in taking out offences. This is yet perilous for criminals due to legal pressure. What will improve in this field is the process in which images and videos will be reciprocated, with larger availability and concealment. Child pornographers often contend that they are not doing anything wrong, instead of considering themselves to be mere "voyeurs".

5.3 Attacks on Infrastructures:

The critical infrastructures will be targeted by cyberterrorism for different purposes. Power distribution networks, transportation networks, and communication networks are assumed to bear charges required to deaden a nation by denying it of its vital services. Such attacks could cause an unprecedented crisis on many levels, including the economy, safety, health, sanitation, civil peace, and more. In addition, hackers and other cybercriminals (even governments themselves) could further target their opponents. They may include attempts to attack informational sites, with a growing number of counterattacks by some governments or resistance groups.

VI. CYBER CRIMES AND THE NATURE OF EVIDENCE:

The nature of evidence in the real world and the virtual world is different. This disparity is conspicuous in all the stages of evidence detection, gathering, storage and exhibition before the court. The critical part is that all the investigation authorities that are responsible right from the stage of collection of the evidence to the presentation of the evidence before the court must understand the distinguishing attributes of the evidence so that they can preserve the evidence collected by them. In this regard, the role of the judiciary also becomes vital as the judiciary must also be in the position to appreciate the computer evidence presented before them. Contrary to the real world crimes where any tangible evidence in the form of fingerprints, the weapon of crime, blood stain marks etc can be traced, in the virtual world, such traces become very difficult to find. The science of computer forensics is gaining significance in the investigation departments, corporate world, government departments etc. Let us understand some of the challenges that are involved in the process of cyber evidence detection, gathering, storage and exhibition before the court.

It is considered more difficult to expunge the information from the computer system than what is generally contemplated. This can be done with the help of computer forensics who are able to gather evidence or even recover information which may have been deleted intentionally. It is vital that the victim reports the law enforcement agencies about the crime as early as possible. The process of preservation of cybercrime evidence lies within the understanding of an efficient and knowledgeable computer forensics expert because any carelessness in the process can lead to the diminutive value of the evidence. The most often faced impediment is that the victim–companies are more concerned with the restoration of17 their systems to full operational status rather than allowing proper evidence collection. Thus the timely assistance of the computer forensics expert can help collect evidence from the system within the shortest time possible. The cyber evidence is of physical or logical nature. It is the physical evidence that can be traced easily as the investigator just has to visit the scene of the crime and search for and take into his custody computer hardware, which may constitute mainframe computers to pocket-sized personal assistants, floppy diskettes, electronic chips etc. The facets of the logical component of the cyber evidence are of different nature. This entails a process described as Information Discovery' wherein the investigator scrutinizes through the log files, and tries to salvage the data from a computer system which has been affected. Once the required evidence is identified, then the investigator must ensure that the same is collected by adhering to the legal requirements, such as evidence is collected only after the requisite warrant for it is issued or if the information appears to be outside the scope of the warrant then additional warrant be issued. The evidence collected becomes valid in the courts of law only if the evidence is collected by legal means16. At the moment only officers not below the rank of a Deputy Superintendent of Police and officers deputed by the central government can be authorized to enter public places and collect evidence and carry out search operations and arrest17. This authority has been given to higher grade officers at the moment keeping in view the misuse of this power viz. right to privacy and ensuring the validity of the cyber evidence. As of now in India, the concept of ‘Reasonable Expectation of Privacy' has not been developed. The issues involved in this are whether an ‘individual's demeanor reflects a subjective expectation of privacy' or ‘the individual's subjective expectation of privacy is such that the society is ready to recognize it as reasonable. Another quarter which needs to be tested under the cyber evidence and which is inevitable is the appreciation of the computer generated evidence by all the authorities associated with the process of administration of justice. Thus not just the judiciary19 but also the prosecutors, the defence lawyers must become familiar with the technicalities, this is so because till now these authorities were dealing with evidence in the tangible form but the nature of evidence undergoes complete change under the virtual medium, they will have to adjust themselves to appreciate the evidence in logical format.

VII. PREVENTIVE MEASURES TO AVOID CYBER CRIMES:

Cyber Forensics can be used to detect cyber Evidence. To make necessary amendments in Indian laws to control on Cyber Crimes

There is a strong need to harmonize some sections of IT act 2000 to curb cybercrimes and individuals to prevent cyberstalking to avoid disclosing any information pertaining to one. This is as good as disclosing your identity to strangers in public places. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs. Always use the latest and update anti-virus software to guard against virus attacks.

- Always keep backup volumes so that one may not suffer data loss in case of virus contamination.
- Never send your credit card number to any site that is not secured, to guard against frauds.
- Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or deprivation in children.
- It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
- Website owners should watch traffic and check any irregularity on the site.
- Putting host-based intrusion detection devices on servers may do this.
- Web servers running public sites must be physically separate and protected from internal corporate networks.

VIII. CONCLUSION:

Change is inevitable and the dilemmas that advancement in technology poses cannot be avoided, the truth is that the criminals have changed their method and have started relying on advanced technology, and in order to deal with society , the legal and law enforcement authorities, the private corporations and organizations will also have to change. Further such experts must not only be knowledgeable but must also be provided with necessary technical hardware and software so that they can effectively fight the cybercriminals. Thus necessary facilities must be established in various parts of the country so that crime in the virtual world can be contained20. Another aspect which needs to be highlighted is that a culture of continuous education and learning needs to be inculcated amongst the legal and the law enforcement authorities because the Information Technology field is a very dynamic field as the knowledge of today becomes obsolete in a very short time. Lastly the preamble of the Information Technology Act, 2000 provides that the act was passed with the objective to give legal recognition for transactions carried out by means of electronic data interchange and other means of e-commerce, further the act has also made amendments to the Indian Penal Code 1860, Indian Evidence Act 1872, The Bankers Books of Evidence Act 1891, and the Reserve Bank of India Act 1934 for facilitating legal recognition and regulation of the commercial activities. Though this objective of the act is 18 not to suppress the criminal activity, this act has defined certain offences and penalties to smother such omissions, which is understood to come within the characterization of cybercrimes. From this it can be inferred that the law cannot afford to be static, it has to change with the changing times and viz. cyberspace this is all the more required, as there many applications of the technology that can be used for the betterment of mankind, similarly it equally true that such application can also be used for the detriment of mankind as has been demonstrated by the Spycam case. The bottom–line is that the law should be made flexible so that it can easily adjust to the needs of society and technological development. 20 Cyber cells of the law enforcement agencies have started operating in metropolitan cities like Pune, Mumbai, Hyderabad, Chennai, Bangalore etc.

REFERENCES:

[1]. www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov guidelines_provisional2_3April2008_fr.pdf

[2]. www.consilium.europa.eu/ueDocs/cms_Data/docs/pressDa ta/en/jha/103537.pdf

[3]. http://userpage.fu-berlin.de/~jmueller/its/conf/Madrid02/abstracts/Ghernaouti -Helie.pdf

[4]. www.met.police.uk/pceu/documents/ACPOecrimestrategy. pdf

[5]. Guinier D, Dispositif de gestion de continuité – PRA/PCA: une obligation légale pour certains et un impératif pour tous (Continuity Planning – BRP/BCP: a legal requirement for some and a vital necessity for all). Expertises, no. 308, Nov. 2006, pp. 390-396.

[6]. CSIS: Securing Cyberspace for the 44th Presidency, CSIS Commission on Cybersecurity, US Center for Strategic and International Studies (CSIS), Washington DC, December 2008.

[7]. Verizon (2011): 2010 Data Breach Investigations Report, Verizon/US Secret Services, 2011.

[8]. Crimes in CyberSpace (Scams & Frauds) – By V D. Dudheja.

[9]. Intellectual Property - Cornish 3rd Volume

[10]. Computer & Cyber Laws - Nandan Kamath

[11]. Laws relating to Computers - Rahul Matthan

[12]. Indian Copyright Laws - Narayan

[13]. "Cyber Crimes against Individuals in India and IT Act.