COMBAT CYBER CRIMES AND RELATED PROBLEMS

Radhy Sham

Research Scholar, Faculty of Law, Tantia University, Sri Ganganagar

ABSTRACT

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both -- i.e., target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks.

A primary effect of cybercrime is financial; cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals may also target an individual's private information, as well as corporate data for theft and resale. As many workers settle into remote work routines due to the pandemic, cybercrimes are expected to grow in frequency in 2021, making it especially important to protect backup data.

Keyword: *technologies, cybercrime, network, remote work, backup data, internet*

1. PROBLEM

The convergence of computer network and telecommunications facilitated by the digital technologies has given birth to a common space called ‘cyberspace’. This cyberspace has become a platform for a galaxy of human activities which converge on the internet. The cyberspace has, in fact, become the most happening place today. Internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment. There is hardly any human activity that is not touched by the internet. The growing importance of Information Technology can be visualized from the fact that in India for the first time a Delhi based businessman has made a digital will of the secret information saved in his e-mail account. Digital will is a foreign concept which is gaining momentum in India also.

Therefore, Internet has something to offer to everybody and in the process it only increases and never diminishes. The ‘cyber manthan’ has bestowed many gifts to humanity but they come with unexpected pitfalls. It has become a place to do all sort of activities which are prohibited by law. It is increasingly being used for pornography, gambling, trafficking in human organs and prohibited drugs, hacking, infringing copyright, terrorism, violating individual privacy, money laundering, fraud, software piracy and corporate espionage, to name a few.

Despite such a great influence of computers and internet on day-to-day lives, the fact remains that only a fraction of people know what computer and internet is all about? There is a paucity of systematic study which elaborately discusses the basic concepts of cyber world like meaning, evolution, generations, types, characteristics and major components of computers; forms of networks, history of Internet in India, services and limitations of Internet etc.

Most of the books and thesis directly deals with the concept of cyber-crimes without thinking that to understand computer and internet crimes, one needs to understand first the computers and internet. This study is a sincere effort in this direction. Well, the new medium which has suddenly confronted humanity does not distinguish between good and evil, between national and international, between just and unjust, but it only provides a platform for the activities which take place in human society. Law as the regulator of human behaviour has made an entry into the cyberspace and is trying to cope with its manifold challenges.

Though various countries have their domestic cyber laws, but the problem is that most of the books deal with cyber laws of individual nations. In this research work an attempt has been made to do a comparative study of the cyber laws of different countries. A legal framework for the cyber world was conceived in India in the form of ECommerce Act, 1998. Afterwards, the basic law for the cyberspace transactions in India has emerged in the form of the Information Technology Act, 2000 which was amended in the year 2008. The IT Act amends some of the provisions of our existing laws i.e. the Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. Though since 2000 the IT Act is in place in India for curbing cyber-crimes, but the problem is that still this statute is more on papers than on execution because lawyers, police officers, prosecutors and Judges feel handicapped in understanding its highly technical terminology.

Through this thesis the researcher has tried to interpret its technical provisions into simple language which can be understood even by laymen. Since cyber-crime is not a matter of concern for India only but it is a global problem and therefore the world at large has to come forward to curb this menace. As a saying in criminology goes – "a crime will happen where and only when the opportunity avails itself." Until recently, we were aware of only traditional types of crimes like murder, rape, theft, extortion, robbery, dacoity etc. But now with the development and advancement of science and technology there came into existence machines like computers and facilities like internet. The internet has opened up a whole new virtual heaven for the people both good and bad, clever and naive to enter and interact with lot of diverse cultures and sub-cultures, geography and demographics being no bar. The very same virtues of internet when gone in wrong hands or when exploited by people with dirty minds and malicious intentions, make it a virtual hell. Stories of copyright theft, hacking and cracking, virus attacks and plain hoaxes etc. have mounted up in the last few years.

There is no single text available which provides a coherent and consistent exposition on the various categories of cyber-crimes, their nature, scope, features and essential ingredients. It is fascinating to study cyber offences like cyber hacking, cyber fraud, cyber pornography, cyber terrorism, cyber stalking, cyber ragging6 etc. and also the US, UK and Indian approaches towards these offences. As a result of the rapid adoption of the internet globally, computer crimes are multiplying like mushrooms.

The law enforcement officials have been frustrated by the inability of the legislators to keep cyber-crime legislation ahead of the fast moving technological curve. At the same time, the legislators face the need to balance the competing interests between individual rights such as privacy and free speech, and the need to protect the integrity of the world's public and private networks. Moreover while investigating cyber-crimes, the investigating agencies and law enforcement officials follow the same techniques for collecting, examining and evaluating the evidence as they do in cases of traditional crimes.

Most of the books are silent on the issue of electronic evidence. In this study the researcher has critically analysed the admissibility and evidentiary value of electronic evidence in addition to the methods of its procurement and examination. Further complicating cyber-crime enforcement is the area of legal jurisdiction. Like pollution control legislation, one country cannot by itself effectively enact laws that comprehensively address the problem of internet crimes without cooperation from other nations. While the major international organizations, like the OECD and the G-8, are seriously discussing cooperative schemes, but many countries do not share the urgency to combat cyber-crimes for many reasons, including different values concerning piracy or espionage or the need to address more pressing social problems.

These countries, inadvertently or not, present the cyber-criminal with a safe haven to operate. Never before has it been so easy to commit a crime in one jurisdiction while hiding behind the jurisdiction of another. Though the issue of jurisdiction in cyberspace cannot be settled spontaneously, but still a global effort in this direction is the need of hour.8 The present researcher has made an attempt to exhaustively analyse these jurisdictional riddles and has suggested the evolution of a uniform international law applicable to transnational cyber-crimes. Apart from tangible rights, some intangible rights called as 'intellectual property rights' such as trademarks, copyrights and patents etc. are also infringed in the cyberspace.

There is no dearth of specific books on IPRs, but books on IPRs vis-à-vis cyberspace are not much in number.

2. SOLUTION AND ITS ANALYSIS

This study has tried to undertake a collaborative approach on IPRs and cyber world. The purpose of this study is to cover the complete scenario of internet crimes, their magnitude and nature, and make an insight into the people who are responsible for it. This research work will also take a comprehensive view of the governmental efforts being done in India and abroad to stop such crimes and will look closely on their success and failures. An effort will also be made to vigorously analyse the various perspectives of IT Act, 2000; its ins and outs including its shortcomings and the possible means and ways to overcome them.

It has been generally accepted that procedural aspect of the criminal law is the main hurdle in tackling the problem of cybercrime effectively but at the same time, substantive part of the cybercrime also needs to be redefined to fight against ongoing cyber criminality. Out of a variety of cybercrimes, the European Convention has chosen ten specific cybercrimes and urged the member states to include them in their information technology laws and provide a concrete mechanism to fight against them. But it is rather unfortunate that many cybercrimes of a particular country are not treated as crime under the criminal law of other countries, which really pose a problem when cross-country cybercrimes are involved. The solution to this problem lies in enacting a global cyber law uniformly applicable to all the countries of the world.

The crux of the matter is that universally accepted standard cybercrime preventive laws should not vary from place to place. A nation wise survey of cyber law indicates that only a few countries have updated their cyber law to counter the cyberspace crime effectively, while many of them have not even initiated steps to frame laws for policing against these crimes. This divergent approach of world nations towards the desirability of cyber law poses a real problem in handling the internet crime and at the same time provides ample scope for the cyber criminals to escape detection and punishment. All the nations should therefore, realize the need and urgency for generating awareness about the dangerous nature of cyber-crimes which are perpetuating illegal online activities in cyber space.

Cyber criminality is perhaps the deadliest epidemic spread over the world in the new millennium which has to be curbed by adopting a global preventive strategy. An overall global view of the cyber law indicates that many countries do have their national legislation for combating cyber criminality, but they radically differ from each other as a result of which, a particular cyberspace activity which is considered as a criminal offence in one country may not be necessarily so in another country. This variation in law provides loopholes for the cyber offenders to escape punishment. Therefore, there is dire need for international cybercrime legislation which could be uniformly acceptable by all the countries to tackle the problem of cybercrime. Not only that, there should also be an international policing agency for countering cyber offences. The solution to the problem therefore, lies in the concerted and united efforts of nations around the world and their mutual cooperation in fighting against cyber criminality. Broadly speaking, the law enforcement agencies all over the world are confronted with four major problems while dealing with cybercrimes in a network environment.

The detection and prosecution of cyber criminals online is hindered by the challenges, which may be technical, legal, operational and jurisdictional. As regards technical challenges, cybercrimes such as hacking of a website, stealing data stored in computers, espionage, exchange of pornographic material, blackmailing etc. involve detection of source of communication which is a complicated task. Therefore, the cyber criminals find it easy to impersonate on the internet and hide their identity. The legal challenge emerges from the fact that cyber criminality is no longer confined to the developed countries alone but it has assumed global dimensions in recent decades. The conventional legal techniques of investigation of cybercrimes are inadequate particularly, in case of cross-country crimes. The problem becomes more complex because of lack of any universally accepted definition of cybercrime. Therefore, a cybercrime in a country may not necessarily be a crime in another country.

There are hardly 20 countries in the world which have enacted comprehensive cyber laws. In the absence of an adequate cybercrime laws, the cyber criminals carry on their illegal activities undeterred. Therefore, effective handling of cybercrimes requires a legal framework which is equally applicable to all the countries. The cyber laws should also be responsive to the fast developing information technology.

The operational challenges faced by the law enforcement agencies because of lack of adequate cyber forensic technology for dealing with cyber-crimes constitute another in-road which renders it difficult to collect and preserve sufficient evidence against the person accused of cybercrime, thereby resulting in his acquittal by the court. The traditional modes of procuring evidence are unsuited in case of cybercrime investigation because most of the evidence exists in electronic form. Therefore, there is dire need to develop suitable computer forensic mechanism for effective handling of cyber-crime investigation.

In the context of electronic evidence, it is significant to note that despite the fact that digital signatures have facilitated e-commerce by reducing paper-work and ensuring quick transactions, it has not been widely accepted in India because of the technicalities involved in it and therefore, people in general still believe that paper-based documents are more dependable and trustworthy than the paperless electronic records. The reason being that former are tangible and serve as best piece of evidence before a law court. However, with the expansion of e-commerce and legal recognition of e-contracts in business transactions, there is change in the mindset of the people and they are gradually adapting themselves to the new e-environment and finally switching over to paperless electronic transactions.

The jurisdictional challenge impeding the efficient handling of cybercrime investigation result out of widespread inter-connectivity of the computer networks and the supporting infrastructure such as telecommunication information dissemination on the website etc. In fact, jurisdiction is a broad concept which refers to whether a court has power to adjudicate, i.e., whether it has personal jurisdiction to try the case and territorial jurisdiction over the location or place where the crime is committed or the parties concerned reside. In case of cross-country cyber dispute or crime, the problem often arises as to the law of which country would be applicable to the case in hand.

3. SUGGESTIONS

In view of the expanding dimensions of computer-related crimes, there is need for adopting appropriate regulatory legal measures and gearing up the law enforcement mechanism to tackle the problem of cybercrime with stern hands. Even a short delay in investigation may allow cyber criminals enough time to delete or erase the important data to evade detection, which may cause huge loss to the internet user or the victim.

That apart, the peculiar nature of cybercrimes is such that the offender and the victims do not come face to face, which facilitates the criminals to carry on their criminal activities with sufficient sophistication without the fear of being apprehended or prosecuted. It is for this reason that a multi-pronged approach and concerted efforts of all the law enforcement functionaries is much more needed for effective handling of cybercrime cases. A common cybercrime regulatory law universally acceptable to all the countries would perhaps provide a viable solution to prevent and control cyber criminality. The process of crime prevention essentially requires cooperation and active support of citizens, institutions, industries and the government alike. Therefore, a sound strategy for prevention of cybercrimes necessitates mobilization of community participation in combating this menace. This calls for participative role of all those who perceive that the growing incidence of cybercrime is a potential danger to the society as a whole.

The suggestions are:

1. Net Security by Tightened Up
2. Use of encryption technology
3. Intrusion management
4. False E-mail Identity Registration be Treated as an Offence
5. Self-regulation by Computer and Net Users
6. Liberalization of Law Relating to Search and Seizure
7. Use of Voice-recognizer, Filter Software and Caller-ID for Protection against Unauthorized Access
8. Development of Cyber Forensics and Biometric Techniques
9. Need to Establish a Computer Crime Research & Development Centre
10. Need for a Universal Legal Regulatory Mechanism
11. Global Code of Digital Law for Resolving IPR Related Disputes
12. Need for Universalization of Cyber Law
13. Interpol and Emergency Response Computer Security Team
14. Combating the Menace of Cyber Terrorism
15. Special Cyber Crime Investigation Cell for Hi-tech Crimes
16. E-Judiciary and Video- conferencing for Speedy Justice

REFRENCE

1. "Ab E-mail Accounts Ki Bhi Hui Wasiyat", Navbharat Times, April 5, 2010, p. 5
2. "Byte Replaces Bullets On Cyberspace", Hindustan Times, September 18, 2006, p. 11
3. Dr. S.C. Sharma, "Study of Techno – Legal Aspects of Cyber Crime and Cyber Law Legislations", Nyaya Deep, 2008, p. 86
4. Justice T. Ch. Surya Rao, "Cyber Laws – Challenges for the 21st Century", Andhra Law Times, 2004, p. 24
5. S.K. Verma, "Controlling the Internet Crimes", CBI Bulletin, August, 2001, p. 17
6. "Cyber Thieves are Caught, But Conviction is Wobbly", Hindustan Times, August 9, 2006, p. 18
7. "Cooperation and capacity building are vital for Curbing Cyber Crime", The Pioneer, March 18, 2008, p. 7.
8. https://shodhganga.inflibnet.ac.in/bitstream/10603/7829/18/18_chapter%209.pdf.