Cyber Crimes in India and related laws

Prof. Prabir Kumar Pattnaik[1], Dr. Itishree Mishra[2]
[1]Professor, Faculty of Legal Studies, Siksha O Anusandhan
[2]Asst. Professor, Faculty of Legal Studies, Siksha O Anusandhan
Email - [1]prabirpattnaik@soa.ac.in, [2]dritishreemishra@soa.ac.in

ABSTRACT

The remarkable growth of the knowledge society and its dependency on worldwide internet use an especially in India is accompanied laterally by society's susceptibility to cybercrime. Cybercrime are not constrained by geographical constraints as cyberspace is massive, free-flowing and borderless fixed issue. Local regulations can't stop these crimes, India is like sitting ducks in these situation. India to the Cybercrime counter actors have engaged in various ways bilateral agreements such as the cyber-deal with Russia and a framework agreement with the United States, resent visit India's Prime Minister Mr. Modi to Israel to sign IndoIsrael 's cyber agreement is yet another Indian attempt to streamline its cyberspace. Ces accords bilatéraux have limited reach and are inefficient and inadequate tackling cybercrime. India wants a multilateral agreement this will harmonize its laws by means of a common convict Law, and manage foreign collaboration Combating Global Cybercrimes. India should sign the convention to combat cybercrime, even the US and Israel with whom India is having bilateral agreements to combat cybercrime have joined Budapest cybercrime convention. The paper defines the concept of cybercrime and laws against that.)

Keywords
Bilateral agreements, Cybercrime Convention, Cyber, India, law

Article Received: 10 August 2020, Revised: 25 October 2020, Accepted: 18 November 2020

Introduction

The concept of crime is not a new phenomenon, but it exists since eternity. Yet the definition and essence of criminality has evolved from time to time. In fact, it has modified the definition of crimes accordingly. In the age of the 20th century and with the introduction of computers, the perpetrators shifted manner in which the offences were performed from traditional techniques to machine driven methods. The first cyber-crime reported was in 1820! There is no mistake taking into account the fact that the abacus is thought to be the oldest version of a Machine, was around from 3500 B.C. Japan, China and India. Indian Law The device is now at a state of growth. The legal system of India enshrines the law with the change of situation. Prof. Allen justifiably said, the law is not it's all about orders, but it's something important. The view demonstrates the position of law is wider than that command. This legal position is more important nowadays Place. Criminal justice is closely linked to the single citizen of society. In Cyber law, the age of information technology, needs hours. Cyber law stands for the cyber crime.

The concept of cybercrime is not defined anywhere, in the modern context, the general discussion on Cyber Crime does not depart from criminality and for the form used for Crime commission. Cybercrime is not important to categorize, because there are different types of IT violence. If the IT is done, significant steps will be sought for the specialized. Consequently, the broad concept of cybercrime can affect the public interest. The word cybercrime can not still be specified. Mostly every cybercrime is protected by the official description and forms of crime, since it is simple that one thing happens with in crime. However, changes and developments in society have taken place obstructed to enact new laws.

Cybercrime law typically covers the communication function and indeed the regulatory aspect of the Internet. The cyber law is the area of law that controls the legal dimension of the Cloud. The transformation in IT has created an electronic environment, which is the main problem for the system on earth. It means "everything to be upset about linked to or every legal activity of the net consumer in cyber space under cyber law." The framework has been set on the verge of re-thinking paperless contracts, digital signatures, monetary communication, although this Internet has utterly been lacking in geographical limits.Because of this modern era, criminals now have different forms of crime. In view of evolving the existence of cybercrime, several international organizations have made mandatory provisions on the implementation of cyber law for all Nations. The decree concerned explicitly contracts, which are carried out in the modern world through all the Net.

It is very simple for someone in today's day and age to talk with various opinions on all sides of the globe, even sharing their existence because of certain facets including its Internet and because of them, not only the country, but companies and individuals around the world are facing multiple issues and challenges. Such structures thus awaken and seek to establish such laws in order to safeguard the welfare of the entire society. This new department of law was thus combined, as for crime committed through machine or the internet, the conventional approach for decouraging crime is useless. There were no laws regulating cyber sector in india is expected until 1999.Yet the internet impacts the electronic world because with the case in the fields of communication & e-commerce. This pushed the program to lay the groundwork for cyber space exploitation. And with such troubling internet usage, some alerting countries around the world are formulating the regulation. This is the group of India. Process or within country, which could be dubbed cyber laws, implemented some enactment

and amendment in criminal laws. Cyber-crime, however, is not different from traditional crime, but some new strategies are required to regulate and monitor the virtual-world.

Discussion

Concept of cyber-crime

The word cyber-crime is not described, this definition is vary because, any crime which is going to committed by using any means of communication or internet can be named as a cybercrime. The abuse over the machine or the internet is not specific therefore; cybercrime is not defined properly. To get a clear concept of cybercrime, firstly, it is necessary to see the concept of crime, which is, attached with computer and the internet. The concept on whole crime is not different from the concept of conventional crime. Both the branch of crimes include the conduct "whether act or omission which causes breach of rules of law and counter balance by the state?"

The term cybercrime is not defined, this meaning is different as any crime that takes place in any media and also the website can be referred to as cybercrime. Therefore, cybercrime is not well described and harassment over the network nor the Internet is indeed not unique. First, it's important to look at the notion of crime which itself is connected to personal computers to go get a better conception of cybercrime. The entire crime concept is no different from the typical crime model. Both the crime division involve actions "either act or omission that induces violations of the constitution and the establishment to counterbalance? The crime has been very distinct from the beginning and relies on the will of the sovereign competence. Culture today is extreme and consists of political activities that varies from human culture. The definition of crime is, in addition to its progress, legal and dissuasive. Crime now needs a misunderstanding from the public. Originally, while religious groups were more strong it is somewhere false about the faith. Sin and crime were not differentiated. Although the meaning of sin has been diluted and sin or misunderstanding is protected by misdeeds."

To constitute some criminal there would be some act or negligence and that should be strictly prohibited and punished. The word cybercrime is development of the information technologies words, now technological innovation is an important part of the daily lives in modern scenario without all of this technology it is not practicable to cater for the needs with human being, though it is difficult in nature however need for such hours. Cyber crime was generated by the use of the machine or the internet. Cybercrime may be said to be the sort that is a conventional crime and where the computer is an entity or a part of crime-making behaviour. When the term cyber arrives, the machine or just any network is always involved. This is cyber-crime when you use this tool or network to commit an offense. Computers against cybercrime are a device that can deter crime.

Newly created terms are cybercrime and cyberspace. This is not seen in a real existence known as online space in cyber space and use the Internet to accomplish anything. The cyber space is called Cyber Crime Committee of someone using this facility. In general, crime means any act that will be committed in society and will therefore worry the minds of society or build up mistrust within society. Cyber safety is not unique, just like a conventional crime. Cybercrime, therefore, assumes that crime can be considered cybercrime when someone using the internet or the machine conducts illegal acts in compliance with criminal law.

As per today's era of rapid growth, information technology embraces everything, lifestyles from around the world. Such technical advances brought about paperless transaction. Now, new speed standards, efficiency and, contact precision have been developed, which have become main tools to improve innovations, innovation, and efficiency also increase in overall ratio. The use of omnipresent is for the storage of political, social and economic or personal confidential data which benefit society tremendously. Computers are used in increasing manner, and growing in numbers of users which are connecting to the Internet. Since, in these circumstances the Internet and the machine are easily available. Hence, the criminals were beginning to misuse the computer or the internet for criminal activity. The internet is a convenient conduct for anyone to reach, exploit and kill others data, the operation is nothing more than cybercrime.

There is no clear difference between cybercrime and traditional terrorism. On a deep introspection, however, it can be suggested that there is a good line between demarcation of the medium's participation in cyber-crime. Cybercrime relates to the cyber room. Offences in cybercrime are known to be committed through information technology. This piece of knowledge Cyber-based infrastructure including machine is not subject to commitments Cyber delinquency. The role of human hand in these computer crimes is less while the major activities are carried out by automated machinery. Whereas the Internet is wonderful gift of knowledge to humanity, it also becomes a sanctuary for Crimes.

Definitions

Cybercrime and computer crime are interchangeably used in popular Speech. The word 'computer-crimes' has a broader scope, as it does not just involve crimes committed online, but also crimes committed in connection with computers or with the help of them. Don B Parker differentiates between computer crime and cybercrime concepts and defines the terms in the following word. Crime with computers: meaning a crime in which all the victim uses unique computer technical skills.

Cybercrime can simply be described as "Computer- or Computer-based Crimes." though in this plain and restricted definition the nuanced nature of cybercrimes can not be conveyed adequately.

"Computer related crime" has been described by the economist intelligence unit Cooperation and Development (OECD) as "any unlawful, immoral or non-authorized conduct in the automated processing and exchange of funds."

Also, this definition cannot cover the frontier dimension of the true nature of the Cybercrime, though it describes cybercrime, includes only the criminal activities with respect to data transmission. But the cybercrime isn't just

about the transmission of data requires any criminal activity by machine.
The conclusion can be drawn on all of the above definition that cybercrime is much border and broad term, but there is no appropriate definition of this term. The different Nation enacts different cyber laws, but no nation can provide Cyber Law units which cover the entire field of cybercrime.
Cyber-crime can be described as' a crime by computer manipulier of the cyberspace which creates, distributes, alters, robs, misuses and destroy the data, without using force or violence and against will or the desires of the victim."

Cybercrime and offences under Indian penal code:

When culture evolves, crime definition grows along with time and invented the cybercrime. As it is already mentioned, cyber-crime is a criminal act that machine or network is either aim or device, or both. Indian Penal Code means criminal law, it is a complete code deals with all types of offences, even though the concept of crime is modern and technological but, the Indian Penal Code still functions and protects all kinds of crimes. This modern criminal law is therefore adequate to tackle all kinds of crimes.
The idea of crime is that with time as society grows and cybercrime developed. As stated earlier, cybercrime is now a criminal act, which is the target or computer of a machine or a network or both. Who is thinking in cyber law and the IT Act, 2000 about cyber-misuse. The Indian Penal Code also contains the offences laid down in this Act in the various clauses of the Indian Penal Code.
After the enforcement of Information Technology Act on the 17th of the year 2000. In the substantive 2000 relevant provisions were incorporated Indian criminal procedure. India's substantive criminal law means Indian Punishment Code, because the different offences in this law are too similar to the offenses which are known as cybercrime, only because of the technology used to commit such crimes specific laws also demand that the crimes be brought to court this File is a sample. The amendment brings any new word into the Indian Penalty Code only for the purpose of effectively implementing provisions. These crimes are committed through the use of information technology.
The IT Act 2000 includes a broad variety of crimes, including machine thermal treatment, posting offensive messages, privacy infringement, posting pornographic content, etc. All these activities are now criminally known as both an crime under the Indian Penal Code. These parallels should be addressed mostly in way they are; related offenses are also protected by the Indian Penal Code.

- Section 503 of IPC- define Sending threatening
- Section 499 of IPC- Sending defamatory messages by email
- Forgery of electronic records- Section 463 IPC
- Bogus websites, cyber frauds- Section 420 IPC
- Email spoofing - Section 463 IPC
- Web-jacking - Section 383 IPC
- E-Mail Abuse - Section 500 IPC
- Online sale of Drugs define in NDPS Act
- Online sale of Arms defines under Arms Act
- Pornographic Section 292 IPC

Cybercrime and criminal law of India

The IT Act 2000 includes a broad variety of crimes, including machine heating process, posting offensive messages, privacy infringement, publishing inappropriate videos, etc. All these activities are now criminally known as crime under the Indian Penal Code. The comprehensive penal law in India indicates Indian Punishment Code because the various crimes under this statute are too close to those known as cybercrime, but also because of the technologies used in committing such crime, particular laws often require that crime introduced to just the court throughout this file be a sample. The regulation is also based on the Indian Punishment Code. New communications technology modes will be used by the organization. The Internet makes the economy of businesses open to the easy and quick medium of communication. In addition, the Security Council needs to develop new ways to do business service in order to achieve business globalization. This globalization forces the world to ensure that only the Internet laws are in place. It relates to e-business control law and regulation.
This globalization is pushing the international community to ensure the regulation governing internet use. This isn't like a real universe, but it still intertwined the earth and turned it an earth village. This improved the legal system's work. As a welfare state, also in cyberspace, the State has a duty to protect its people. And cyber-space activities must be subject to the legal framework. This is not a country, but the existing cyber legislation mostly in world is however exposed to something like the transnational world culture.The Information Technology has invented the modern cyber space world. That's is world is 21st Century creation. This is not like a real universe, however, it nevertheless connected the world and made it a global village. Hence the function heightened legal system. As a welfare state, the State has a responsibility to protect the citizens even in cyber-space. Therefore the legal system needs to be governed the cyber-space operations. It is not the subject of any country but therefore the current cyber laws in the world are subject worldwide culture which is transnational.

Cyber laws in India:

There are many other laws and regulations deals with cybercrime, besides the Law on Information Technology and the Indian Penal Code, Still some civil laws are important for some cyber spatial misuse. However, fraud is usually present in cybercrime, and it involves criminal law, or even Tort Law is still applicable and may provide the redress to unauthorized persons. Except the Information Act,

2000 and the Indian Penal Code 1860, India has several other cybercrime rules. They are as follows:

- Common Law (governed by general principles of law)
- The Bankers' Book Evidence Act, 1891
- The Reserve Bank of India Act, 1934
- The Information Technology (Amendment) Act, 2008 and 2009
- The Information Technology (Removal of difficulties) Order, 2002
- The Information Technology (Certifying Authorities) Rules, 2000
- The Information Technology (Certifying Authorities) Regulations, 2001
- The Information Technology (Securities Procedure) Rules, 2004
- Various laws relating to IPRs.

Indian legal system have different cyber laws crimes: But cybercrime is technical in nature, so it requires the technical process in the proper sense of enforcing criminal law. Missing the technical process. Accordingly, the Indian legal system which is substantial in criminal law is appropriate. The fundamental problem in the case of cybercrime, there is a specific way of using the Internet Misuse; it is the offenders that are still misusing it in different ways, and the justice system cannot meet the needs. Beyond this the essence of cybercrime is transnational, so international cooperation is needed. Mere legislation isn't enough, cyber law can't operate without the foreign collaboration. The Informatics Act 2000 and all other laws transnational Jurisdiction clause.

Conclusion

The enormous rise in Internet use worldwide and particularly in lateral Indians accompanied by significant increase in cybercrime, and India vulnerable to such offences. Cybercrime is international character and criminals are not bound by its unique geographic area. Cyberspace is free-flowing, borderless and not covered by local authorities' geographical limits. Those can't be offences dismantled by state laws, India is in such a scenario like ducks sitting there. India to counter cybercrime has engaged in numerous bilateral deals, such as cyber partnership and arrangement with Russia agreement with the US, recent Prime visit India Minister Modi to Israel to sign Indo Israel's cyber agreement is yet another Indian initiative rationalizing the cyberspace. Those are bilateral agreements are inadequate and have limited scope yet Cybercrime is unsuccessful. India wants one multilateral treaty harmonizing its laws through a standard foreign policy, and international trade co-operation to fight global cybercrimes niveau. India should sign the convention to combat cybercrime, even the US and Israel with whom India is having bilateral agreements to combat cybercrime have joined Budapest cybercrime convention.

Reference

[1] Proprietary Articles Tread Association V. A.G.for Canada (1932).

[2] http://www.legalindia.com/cyber-crimes-and-the-law/.

[3] Joga Rao, S.V., Law of Cyber Crimes, 2004.

[4] Cyber Law &Crime :Barkha U Rama Mohan (2011) Asia Law House, Hyderabad. Page 1.

[5] 2http://catindia.gov.in/writereaddata/ev_rvnrbv111912012

[6] www.mondaq.com// Article by Rajkumar Dubey

[7] Section 198 A of Cr. P.C. 1973