I J R S S I S, Vol. (IX), Issue (1) Jan 2023: 521-525
A Double-Blind Peer Reviewed Journal
OPEN ACCESS
e-ISSN 2347 – 517X
Original Article

Reg. No. : MH-NGP/0000167

INTERNATIONAL JOURNAL OF RESEARCHES IN SOCIAL SCIENCE AND INFORMATION STUDIES

www.ijrssis.in

CYBER CRIMES: A BANE TO THE MODERN SOCIETY

Suwarna Sachin Mangrulkar
ShantaramPotdukhe College of Law, Chandrapur.
*Corresponding Author: suwarna.mang@gmail.com

Communicated : 20.12.2022 | Revision : 08.01.2023 Accepted : 20.01.2023 | Published: 30.01.2023

ABSTRACT:

Crime is an illegal act which gets punished by the law of the Land. Crime is considered as inevitable. In fact crimeless society is regarded as a myth. In the characteristics itself, law changes from time to time and place to place. Crime and Law, both are dynamic concepts which changes from time to time and place to place too. In early days the crimes were committed in the factual world. People used to fear the criminals but now because of technology we are not able to see the criminals as their presence is seen only in the virtual world. The cyber crime is a new invention of crimes made by some intellectual, intelligent, knowledgeable, educated in short sophisticated criminals. One can clearly observe that the cyber crimes started to operate when technology reaches it's the highest point and took new shape to satisfy human wants and desires. As we know such types of crimes are done in the virtual world in the borderless world. Most of the time, the netizens remain unaware about the identity of persons to whom they are chatting and sharing personal information. Boundaries vanish when any person connects to the Internet and computers. Smart phone is another step when the whole globe can be connected with a device in your pocket. This is a challenging situation for the Law makers, the Investigating Agencies and the Judiciary too to give the Justice to the victims of Cyber Crimes.

Key words : Cyber Crimes, UNCITRAL Model Law, cyber attacks, E-Governance

INTRODUCTION :

In early days the crimes were committed in the factual world. People used to fear the criminals but now because of technology we are not able to see the criminals as their presence is seen only in the virtual world. The cyber crime is a new invention of crimes made by some intellectual, intelligent, knowledgeable, educated in short sophisticated criminals. One can clearly observe that the cyber crimes started to operate when technology reaches it's the highest point and took new shape to satisfy human wants and desires. Every coin has two sides. Though technology is responsible for making our life easy and comfortable, its negative side has come to its front. Such crimes are being committed with the help of machines and on arithmetical formulation need deep study and knowledge of cyber world and technology. These crimes contain the elements of blue collar and white collar crimes as well. These are blue collar crimes because these are not very different from other prototype crimes, though recognized by various names. These are also white collar in nature because crimes are usually committed by a class of criminals who are having deep knowledge about science and technologies. For this reason cybercrimes is a combination of blue collar and white collar criminals. The criminals of this advanced group endeavor to commit these new crimes with the help of computers through Internet by exploiting cyber space. This is a new subject and the world facing problem to tackle the situation.

Cyber Crimes and issue of Jurisdiction

In the real world, the concerned Government is having power and the existing Court is having authority but the thing changes in the cyber world. There is major issue of Cyber Crime Jurisdiction in the investigation of Cyber Crime. At this stage of development of the world, the legal concepts on the Internet Boundaries disappear. The Law can be enforced properly if this issue is clear. As we know such types of crimes are done in the virtual world in the borderless world. Most of the time, the netizens

remain unaware about the identity of persons to whom they are chatting and sharing personal information. Boundaries vanish when any person connects to the Internet and computers. Smart phone is another step when the whole globe can be connected with a device in your pocket. The cyber criminals are nothing but the masters of using the modern Science and Technology with an ease and in such cases our Investigating agency found it very much complicated and difficult at the same time to implement the law effectively. It is not hyperbole to say that the technology is responsible to hide the criminal from his real identity.

The statistics of Cyber Crimes in India is collected and published here under the following heads by the National Crime Records Bureau.

- Offences registered under Information Technology Act, 2000
- Offences under the Indian Penal Code related to Cyber Crimes
- Offences under Special and Local Laws related to Cyber Crimes

Today also there are no clear guidelines on the issue of Cyber Jurisdiction on the issue or event in the cyber space whether it is dealing with the laws of the State where website is located or through the laws of the State, where ISP is located, or the laws where the user is located or with any other specific laws in this behalf. In India the Jurisdiction in case of Crimes deals with the Indian Penal Code. Section 3 and section 4 of the Indian Penal Code, 1860 speak on Intra territorial jurisdiction while Section 4 of the Act deals with extra territorial jurisdiction. It clearly shows that the National Laws of the country deals with territorial and extra territorial jurisdiction but there is no any international instrument clearly speaking on Cyber Space Jurisdiction. In 1996, the UNCITRAL Model Law on E Commerce was adopted. It is recommended by the General Assembly that all the States should give favorable consideration to the very Model Law. India is also the signatory to it but it is the major drawback of the IT Act, 2000 that it is silent on the issue of Jurisdiction. Section 75 of the IT Act states that the Act applies to the offences committed outside India irrespective of Nationality if the offence or contravention involves a computer, computer system or computer network located in India Jurisdiction has been also mentioned in various Sections of Information Technology Act, 2000 under sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure connected. Section 80 speaks on the police officers' powers to enter, search a public place for a cyber crime etc. The main problem arise when the police is going to investigate into the Cyber Crimes where only the IP address of the Computer is identity of a criminal. The IT Act, 2000 is effective in case of Intra-territorial operation but the problem arises while applying Extra-Territorial jurisdiction. In case of Extra-territorial Jurisdiction, the Act is effective if India is having Extradition Treaty with the State where accused is residing or working for gain of business. The procedure for securing the Extradition is to be found in India in the Extradition Act, 1962.

There is also difficulty in ascertaining jurisdiction of the Court. If take an example that any crime which is committed outside the borders of India, but the offender is found within the country, it is still confusing whether he may be given up for trial in the country where the offence was committed i.e. extradition or he may be tried within India under Extra-territorial jurisdiction. On International Level there is a Convention speaking on Cybercrimes which was opened for the signature in the year November 2001 in Budapest known as Budapest Convention. This Convention is the most important step asking for the cooperation in the investigation and jurisdiction aspect of

Cyber crimes beyond the territory of any State. This Treaty also provides for the International Police and Judicial cooperation in case of accepting electronic evidence. India is the developing country struggling with the issue of Cyber crimes is not a party to the Convention. Jurisdiction and the investigations are still major issues in dealing with the Cyber Crimes.

The Issue of the Investigation of Cyber Crimes

Investigation, Inquiry, and Trial are regarded as the stages of any criminal case. Investigation is the starting point of a criminal case. The Investigating officers have to apply different methods and new techniques to investigate into a case. It requires special skill and knowledge too. The police officer conducts investigation in order to collect evidences. The Supreme Court held in the case of Jamuna vs. State of Bihar that the purpose of Investigation is to bring truth along with evidence. Section 157of Criminal Procedure Code speaks on the Investigation and its procedure. Investigation is regarded as the most essential function in order to give justice to the victims of crime. Traditional methods of Investigation result into low conviction rate. As the change is the rule of nature, cyber crimes are changing and challenging the traditional methods of investigation.

According to the Status of Policing in India Report 2019 , the digitization of the Police Station to track the records of criminals is playing the major role in bringing positive changes in the investigating procedure. The project CIPA i.e. Common Integrated Police Application has begun in the year 2004. CCTNS the Crime and Criminal Tracking Network System and CCIS Crime and Criminals Information System is responsible for maintaining the data of the criminal. These system links one police station to another so that the task of investigation should ne solves from micro to macro level. These National Intelligence Programs make the Investigation system more effective. CIPA is the national project in order to bring the computerized system of police station while CCIS is working on district level. The Maharashtra Government's initiative for digitalization of police stations is progressing positively. This is multilingual software aiding the investigating machinery. DCTC, the District Computer Training Centre has also been established in the various units of the State of Maharashtra in order to provide the training to police officers regarding the computer awareness.

The Report known as Crimes in India, 2021 by National Crime Record Bureau shows that there is increase of cyber crimes in India by 5.9% in comparing to the year 2020. The conviction rate of Cyber Crimes and Information Technology Act in the year 2021 is 35.2% while pendency is 98.1. The Report clearly shows that the Investigating Agencies still battle with the task of collection and proving the evidence before the court of Law. The Agencies have been needed still to work on Prevention of Crime, collection of electronic evidences, production of evidences before the court of Law in proper manner given under the Indian Evidence Act, arrest of accused and the security of the system etc.

Section 78 of the Information Technology Act, 2000 speaks on the powers given to Inspector. Before the amendment Act of 2008, the powers were given to Deputy Superintendent of Police to investigate into the cyber crimes. This is a positive step to mainstream the cyber crimes like other conventional crimes. This amendment has changed the gamut of investigation. Section 80 of the IT Act provides the power of police officer and other officers to enter search, etc. in case of cyber crimes. It is obligatory upon the occupant to afford the facilities required for search. It is expected that the authorities should be armed with the proper facilities to conduct

search so that there should not be any possibility of concoction in obtaining electronic evidence. Section 65A and 65B taken together provide for the admissibility of Electronic record produced before the court of Law. The E contents are proved according to the procedure provided under section 65B of Indian Evidence Act. It provides all the necessary conditions while obtaining E Record from the original source.

National Cyber Security Policy, 2013

The Government of India has framed the National Cyber Security Policy, 2013 with the Department of Electronics and IT and Ministry of Communication and IT. The said policy is aiming towards protecting public and private sectors from various kinds of cyber attacks. This policy has accepted that the cyber space is really a complex environment. This concept of cyber security is an evolving task for the developing country like India. The Policy focuses on creating a secure cyber ecosystem. It is also provided in the said Policy that the Research and Development in this field should be promoted. The Government is supporting the development of E-Governance throughout the country but it should also be secured through the PK Infrastructure which is provided in the Policy.

There are various Objectives of the Policy including the regulation of framework to create trust in IT system, creating cyber secure ecosystem, safeguarding privacy of citizen's data and the most important enabling effectively the prevention, investigation and prosecution of cybercrime and enhancing the law enforcement capabilities through legislative intervention. The Policy is really helpful in providing umbrella to Cyber Laws in India, but it is also having so many shortcomings and limitations. Only Policy is of no use, if it is not implemented. The implementation date is nowhere given in the said Policy so this Policy is like tiger with no tooth and nails. Our Policy is missing the capabilities of Security in short. At this juncture, we have to accept that India is not Cyber prepared to provide security in the real sense. The Policy is needed to be framed in the form of Act so that it should be implemented in proper terms.

As per the data provided by the NitiAayog, India was ranked in the 5 topmost countries affected by the Cyber Crimes. The Union Bank of India was affected due to these attacks according to the Report. The Zomato also suffered from the Data Theft in the year May, 2017. The Report is clearly accepting that the challenges are increasing in the Cyber Space Domain which should be tackled urgently. Cyber security is the major issue in this arena.

In the case of Justice K.S. Puttaswamy (retd.) vs. Union of India , the Supreme Court held that the Right to Privacy is a Fundamental Right. Recently the Ministry of Electronics and Information Technology of the Government of India has come up with the Digital Personal Data Protection Bill 2022. This Bill is the revised version of the earlier the Personal Data Protection Bill, 2019 where new adaptations are brought again to meet the present challenges more effectively. Total 30 Clauses have been provided under the Bill. The Bill covers the Digital Data only. The Bill specially speaks on Data Fiduciaries who really need proper framework with regard to their rights, duties etc. India is already having the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (IT Rules), 2011. Both the Act and Rules together are not enough to provide security in the era of technological advancement. There is need of strong Legislation in the security of Personal Data.

Concluding Remarks

Though India is having Information Technology Act, 2000 specially, provisions like scope for adjudication process are never known to many including those in the investigating agencies. In cyber crimes, there is no cyber crime scene or spot as the crime has been committed in the virtual world but people have suffered in the factual. The investigating agencies cannot mark a place nor a computer nor a network even they cannot seize the hard-disk instantaneously and keep it under lock and key making it exhibit taken from the crime scene. There is need to provide guidance to the Investigating officers specially to conduct Search and Seizure. The criminals have become smarter with the time and these smarter criminals need the smartest investigation to detect the crime. Acquittal rate is high in the cyber crimes due to lacking in the investigating procedure. This should be checked with the smart technique. More thechnological advancement is needed in this regard.

Jurisdiction is the major issue which is not satisfactorily addressed in the Information Technology Act, 2000. Cyber Investigating Jurisdiction is the evolving issue. Though the extra territorial jurisdiction is mentioned but in practice it is not practically applicable beyond the territorial boundaries of India. Even the case laws are lacking in this field. Often, the investigators do not accept such complaints on the grounds of jurisdiction issue. In short one can conclude that within India the Act is effective but outside the world needs universally accepted International Best practices which will be necessary for the Law Enforcement Agencies to investigate, detect and prosecute crimes involving the cyber world within the ambit of existing laws of the land.

There is need to make the Law harsh on criminals but it is seen that the IT Amendment Act, 2008 has made majority of cybercrimes stipulated under the IT Act as bailable offences. This is the most bizarre situation of Indian Legislation dealing with the increasing Cyber Crimes. There is need to sort out the cases immediately. In fact Justice delayed is the justice denied. Alike Green Bench for the environment cases there is immense need for the special Bench dealing solely with cyber crimes. Each coin has two sides. Undoubtedly we have achieved a lot with the help of cyber technology but its negative side cannot be ignored. If we use this technology with cautious mind for the betterment of mankind, it will definitely be regarded as boon to us.

REFERENCES :

https://legislative.gov.in/sites/default/files/A1860-45.pdf

https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

https://indiankanoon.org/doc/576992/#:~:text=(1)%20Subject%20to%20the%20provisions,person%20irrespective%20of%20his%20nationality.

https://www.indiacode.nic.in/bitstream/123456789/1440/1/196234.pdf

https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/(1974) 3SCC174

https://www.commoncause.in/uploadimage/page/Status_of_Policing_in_India_Report_2019_by_Common_Cause_and_CSDS.pdf

https://ncrb.gov.in/sites/default/files/CII-2021/CII_2021Volume%201.pdf

https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

Writ Petition (Civil) no. 494 0f 2012 available on https://indiankanoon.org/doc/127517806/

https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf