Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/17801
DOI URL: http://dx.doi.org/10.21474/IJAR01/17801

RESEARCH ARTICLE

IN DEFENSE OF A SPECIAL CYBER LAW FOR INDIA

Dr. Sapam Dilipkumar Singh
Assistant Professor, Department of Law, Manipur University, Chanchipur.

Manuscript Info

Manuscript History
Received: 05 September 2023
Final Accepted: 09 October 2023
Published: November 2023

Key words:-
Cyberspace, Crime, Conventions, Cybercrime, Terrorism, Combate, Resolution

Abstract

Attempt to unfold the secrets of nature marks the progress of human civilization. With the extreme advancement of science and technology particularly in the field of information science, man can communicate and act in the virtual space. In the 21st century, it is almost impossible to live in this world without depending on cyber space as most of human activities are going to carry out in such space. The flip side of this advancement is the misuse of cyberspace for various purposes in the contemporary world. Cybercrime, different from traditional crime, is a new form of crime committed in cyberspace having swept and widespread impact on human society. Since cybercrime knows no national boundary, all out effort of nation states is required to combat the menace of cyber crime. However, the international community could not able to negotiate and adopt internationally binding legal instrument for preventing and combating cybercrime. On the other hand, nation states including India meet the challenges posed by cyber criminals, which necessitates to enact specific law for preventing and combating cybercrime. The paper attempts to explore national and soft international law that prevents and combats the menace of cybercrime.

Introduction:-

Emergence of state system in human society has brought a radical change in all spheres of human activities. The state owes its obligation to protect the life, liberty and property of each and every subject of the state as the authority and power of the state actually derive people. The administration of criminal justice constitutes one of the primary functions of the state, which is indispensable for maintenance of peace and tranquility in a politically organized society and it also refers to using the force of the state to maintain law and order in such politically organized society for which it circumscribes to enact of laws and establish courts and other law enforcement agencies as well. Force is necessary to coerce the recalcitrant minority and prevent them from gaining and unfare advantage over the law abiding majority of the state.[1]

Crime is as old as human society. It is an act prohibited by law which is the expression of the will of the state. With the help of law, every human society has been endeavouring to prevent and reduce the occurrence of crimes in society. Even though crime is contextual, some crimes are universal in their nature and character in the sense that such acts are obviously disapproved or prohibited by laws as well as the conscience of the people.

[1] P.J. Fitzgerald, *Salmond on Jurisprudence*, p.89, Sweet & Maxwell,London,1966

Corresponding Author:- Dr. Sapam Dilipkumar Singh
Address:- Assistant Professor Department of Law, Manipur University, Chanchipur.

Considering that law changes according to the need of the society, many acts which were treated as crimes in the past are no longer crimes in the present; however, new acts are required to be declared as crimes according to the changes of human society. It was seen in the history that industrial revolution has brought drastic change in the body of rules across the world that has led to codification of many laws for the protection of worker's rights. In the same way, with the advancement of science and technology, particularly, the evolution of information and technology in the present century has necessitated nation states to enact laws to cope with the emerging set of acts which are extremely needed to regulate and control, because of their devastating effect in all respects in any given society. Cyber crimes are the emerging flip side of the revolution of information technology.

An Overview of Cyber Crimes

The advancement of science and technology has brought a drastic change in the landscape of criminal jurisprudence creating new space for combating and preventing crimes which were unknown to criminal jurisprudence of the past. The special feature of cybercrime is that it is committed in cyberspace which is manmade space. Cyberspace is nothing but innumerable computers connected together, sharing data, and information and have become the fastest mode of communication. … Though it may not seen and felt, it is the space where serious business takes place and the happenings result in real consequences.[2] Cyberspace can be defined as a conceptual world of information and electronic networks accessible via the internet and can be rightly called space without frontiers, whose boundaries seems limitless.[3] The internet evolution not only connects people across the world but also plays a significant role in all activities of life. However, the virtual space has been misused by cybercriminals and took shelter in this space as this space knows no national boundary. Cybercrime is the most dangerous of all crimes because of the magnitude of the loss it is causing today and its potential, the ease with which it is committed; its invisibility and the disregard for geographical boundaries; the difficulty in investigation, the collection of evidence and the successful prosecution of the cyber criminal; and the costs of dealing with cybercrime by law enforcement and protective technology.[4] It is reported that in 2011, at least 2.3 billion of people got the access to the internet for various reasons. Over 60 per cent of all the internet users are in developing countries and 45 per cent of all the internet users are those persons who are below the age of 25 years. It is also estimated that mobile broadband subscription will approach 70 per cent of the world's total population by the year 2017. By the year 2020, the number of network devices will outnumber people by six to one, transforming current conceptions of the internet. In the hyper-connected world of tomorrow, it will become hard to imagine a computer crime, and perhaps any crime, that does not involve electronic evidence linked with internet protocol connectivity.[5]

In India, the National Crimes Records Bureau (NCRB) has also started documentation of the incidence of cyber crimes as separate genre of crimes in India in view of the increasing trend of cyber crimes. The NCRB reported that a total of 9,622 cases were registered under the cyber crimes in 2014 as compared to 5,693 cases registered during the previous year which shows an increase of 69% over the previous year. These cases were registered under the Information Technology Act, 2000, related sections of IPC and Special and Local Laws. Maharashtra has reported the highest number of such crimes by registering 1,879 cases accounting for 19.5% of total cyber crimes followed by Uttar Pradesh by registering 1,737 cases accounting for 18.1% and Karnataka by registering 1,020 cases accounting for 10.6%.[6] Altogether 5,752 persons were arrested under cybercrime in the year 2014. Among the North Eastern States of India, Assam is on the top by arresting 351 persons for committing cybercrimes. The age-wise profile of persons arrested in cyber crime cases were in the age group 30 - 45 years.[7] In Rajya Sabha, the minister of state in the ministry of Home Affairs, Shri G. Kishan Reddy stated that as per data maintained by the National Crime Records Bureau, a total of 9622, 11592 and 12317 cybercrime were registered during the year 2014,2015,and 2016 respectively. He further stated that the Ministry has rolled out a scheme for establishment of Indian Cyber Crime Coordination Centre (I4C) for 2018-20. The main objective of the I4C Scheme is to set up a national cybercrime coordination center for law enforcement agencies of States/UTs as an effective apparatus to handle issues related to cyber crime in the country. The I4C scheme has a component namely National Cybercrime

[2] Dr. Amita Verma, *Cyber Crimes & Laws*, Central Law Publications, Allahabad, Reprint, 2012 p.2
[3] Ibid, p.31
[4] Ibid,p.42
[5] *Comprehensive Study on Cybercrime(Draft) February, 2013*, p.xvii, United Nations, New York,
[6] Crimes *in India, Compendium,2014*,p.161, National Crimes Records Bureau, Ministry of Home Affairs, Government of India
[7] Ibid. p 161-167

Reporting Portal to enable public to report all types of cyber crime complaints.[8] His statement made on the floor the Rajya Sabha, based on NCB record, indicates that cybercrime has been increasing in India which requires extra effort to combat it.

Global Measures

The unique characteristic of cyber crime is that it has no national boundary. Such crimes may be committed from any country targeting to a country. Almost all nation states have been facing challenges of cybercrime and cyber terrorism. It has been common concern of all nations, large and small, rich or poor, to create a secure cyberspace which is possible only when there is co- operation among the nations. Acknowledging such widespread effect of cyber crime, the United Nations General Assembly has adopted dozens of resolutions, such as Resolution No. 55/63 for combating the criminal misuse of information technology in 2000. The Resolution provides inter alia the following measures to combat and prevent criminal misuse of information technologies:

1. *State should ensure that their laws and practice eliminate safe heavens for those who criminally misuse information technologies;*
2. *Law enforcement co operation in the investigation and prosecution of international cases of criminal misuse of information technologies should be co-ordinated among all concern states;*
3. *Information should be exchanged between states regarding the problems that they face in combating the criminal misuse of information technologies;*
4. *Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;*
5. *Legal system should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is panalised;*
6. *Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;*
7. *Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and timely gathering and exchange of evidence in such cases;*
8. *The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;*
9. *To the extent practicable, information technologies should be designated to help to prevent and detect criminal misuse, trace criminals and collect evidence;*
10. *The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of the government to fight such criminal misuse;*[9]

In the similar way, the Economic and Social Council has also adopted resolution no. 211/ 33 for the prevention, protection and international co-operation against the use of new information technology to abuse and/or exploit children in 2011.The 12th United Nations Congress on Crime Prevention and Criminal Justice was held in Salvador, Brazil in 2010 with a view to take more effective and concerted action and to prevent, prosecute and punish crime and seek justice.[10] The Declaration recommends the United Nations Office on Drugs and Crime be requested to provide, in co operation with Member states, relevant international organizations and the private sector, technical assistance and training to states to improve national legislation and build the capacity of national authorities, in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all forms, and to enhance the security of computer networks[11].The 13th United Nations Congress on Crime Prevention and Criminal Justice was held in Doha in 2015 with the objective to reaffirm the shared commitment to uphold the rule of law and to prevent and counter crimes in all forms and manifestations at domestic and international level, among others[12]. The United Nations promises to endeavour ensure that the benefits of economic, social and technological advancements becomes a positive force to enhance its efforts in preventing and countering emerging

[8] Rajya Sabha, Unstarred Question No. 3534, to be answered on the 24th July, 2019/ Shravana 2, 1941(SAKA)
[9] Resolution, A/RES/55/63, 2000
[10] Preamble to Salvador Declaration for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, 2010.
[11] ibid, declaration no. 41
[12] Preamble to Draft Doha Declaration, 2015; A/CONF.222/L.6

forms of crime. It also recognizes to adequately respond to emerging and evolving threat posed by such crimes.[13] In this regard, the UN pledges to strive to:

1. *to explore specific measures designed to create a secure and resilient cyber environment;*
2. *to prevent and counter criminal activities carried over the internet;*
3. *to strengthen law enforcement co-operation at the national and international levels;*
4. *to enhance the security of computer networks and protect the integrity of relevant infrastructure;*
5. *to endeavour to provide long- term technical assistance and capacity building;*
6. *to strengthen the ability of national authorities to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crimes in all its forms.*[14]

However, the UN has not been able to negotiate and adopt a specific global treaty for the prevention and combating cyber crime as done in the case of promotion and protection of human rights, other than the adoption of the UN Convention against Transnational Organized Crime. Nonetheless, the UN resolutions are recognized as subsidiary sources of international law under Article 38 of the Statute of International Court of Justice, to which nation states ought to abide by. However, the regional legal instruments, such as the Council of Europe Convention on Cybercrime, 2001 and its Additional Protocol, 2003, the League of Arab States Convention on Combating Information Technology Offences, 2010 the Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information, 2001 and the Shanghai Cooperation Organization Agreement, 2009, African Union Convention on Cyber Security and Personal Data Protection, 2014 among others were adopted for combating cyber crimes. Regional organizations could adopt regional legal documents for preventing and combating misuse of information technology including cyber crime.

National Measures

Threat and its consequent necessity of combating cyber crime is not an exception to Indian society. The country has also been striving to bring about a digital revolution in governance.The parliament has enacted the Information Technology Act.2000 and also brought major amendments to the Indian criminal laws, viz; the Indian Evidence Act and the Indian Penal Code so as to cover and deal with emerging threat of cyber crimes. The Information Technology Act (IT Act), 2000 remained as the principal legislation for combating cybercrime in India. The uniqueness of the IT Act is that it has extra- territorial jurisdiction and applies to any offence or contravention committed outside India by any person.[15] The legislative intention of the enactment, as laid down in the preamble of the Act, is to provide legal recognition for e- commerce, to facilitate e- filing of documents with government agencies and to amend IPC, 1860, the Indian Evidence Act, 1872, the Banker's Books Evidence Act,1891 and the Reserved Bank of India Act,1934.The Act is divided into XIII Chapters consisting of 90 (ninety) sections. Chapter XI of the Act deals with cyber offences and their punishments. The Act prohibits and spells out punishment for sending offensive messages through communication service, receiving stolen computer resource or communication device, publishing or transmitting obscene material in electronic form, publishing or transmitting of material containing sexually explicit act in electronic form, publishing or transmitting of material depicting children in sexually explicit act, in electronic form, among others[16]. The Act also criminalizes the act of identity theft, cheating by personation by using computer resource and violation of privacy[17]. It is quite interesting that most of the penal provisions of the Act have been incorporated in by the Information Technology (Amendment) Act, 2008. It implies that the Act was not enacted with the sole objective of preventing and combating the menace of cybercrime in India. Considering the cyclonic wave of information revolution in the world and impact of cyber crime in India, the country requires a special legislation for meeting challenges of crimes committed in cyberspace.

The real meaning of law lies in its effective implementation. Understanding of law in letter and spirit by the law enforcement agencies of the state is the imperative and people are also required to make known the implications of those enacted and enforced laws for the realization of the objectives laid down in the constitution of India. Law relating to cyber crime still remains novel to the law enforcement agencies since such crimes are of recent origin. The key agencies for the enforcement of criminal laws, such as police and other investigating agencies have to be trained effectively with cyber laws and equipped with the skill to combat cybercrimes. Lack of knowledge of the fast

[13] ibid pp.9 and 10
[14] ibid p. 10
[15] Section 1(2) and Section 75 of the IT Act,2000
[16] Sections 66A, 66B,67,67A and 67B of the IT Act,2000
[17] Sections 66C,66D and66E of the IT Act,2000

changing nature of cyber laws and cybercrimes is the main stumbling block in combating cybercrimes in the North East India in particular and India in general. In this context, it is pertinent to refer the incident of arresting 11 (eleven) persons including one Sub-Inspector of Police and one Jamandar of 1st Battalion Manipur Rifles for uploading nude picture of a married women in social media site in Manipur[18]. It can safely deduce from the said episode that even law enforcement agencies are not well aware of cyber crime and trained to combat such crimes committed in the virtual space.

In India, the National Cyber Security Policy was adopted in 2013 with the vision and mission to build a secure and resilient cyberspace for citizens, businesses and Government, and to protect information and information infrastructure in cyberspace, to build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incedents through a combination of institutional structures, people, processes, technology and co-operation. The policy spelled out 14 (fourteen) objectives which includes creating a secure cyber ecosystem in the country and strengthening the Regulatory framework for ensuring a secured cyberspace ecosystem. The government of India has established Computer Emergency Response Team (CERT-In) to function as a Nodal Agency. Indian Computer Emergency Response Team (CERT-In), reported that a total no. of 44679, 49455, 50362 and 27482 cyber security incidents were observed during the year 2014, 2015, 2016 and 2017 (till June) respectively. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, ransomware, Denial of Service attacks,etc.[19] Counter Terrorism and Counter Radicalization and cyber and information security divisions were also established under the Ministry of Home with a view to prevent and combat misuse of cyberspace.

Conclusion:-

Crimes grew along with the millennia old human society. The mechanism for preventing crime has also developed from within the society itself. With the emergence of new concept of state the measures for prevention of crimes and punishment of offenders have been carried out with a system of uniformly enacted criminal laws. Efforts have also been constantly made for maintaining order in the society both at the national and international level to meet the challenges of new *genre* of crime commonly known as cyber crime. The government of India has also enacted and enforced various criminal laws to prevent and combat cyber crimes; however, there is no specific law for combating the menance of cyber crime. Moreover, mere enactment of criminal law alone cannot prevent and combat cyber crime unless those laws are enforced effectively. Such crimes are new and committed in manmade space which affects both educated and uneducated people. Therefore, the people would be made aware of the nature and effects of cyber laws and crimes. It is a universal phenomenon that such cyclonic wave of cyber space often lead to a serious flaws in the society, more particularly in the North East states where people still live in the most traditional as well as conventional socio, economic and cultural pattern of society. Ultimately, it may be submitted that the government of India ought to introduce a special bill in the parliament to counter the menace of cyber. Such measure would enable the country to prevent cybercrime and to punish those who evolved in commission of cybercrime.

[18] *The Sangai Express*, 15th August, 2015

[19] Lok Sabha Unstarred Question No.673, Answered on 19/7/2017, Ministry of Electronics and Information Technology, Government of India.