Dept of Computer Science, P B SIDDHARTHA COLLEGE OF ARTS & SCIENCE, VIJAYAWADA.
UGC SPONSORED NATIONAL SEMINAR ON "CYBER SECURITY WITH SPECIAL FOCUS ON CYBER CRIMES & CYBER LAWS (NSCS 2014)" on
15th & 16th November 2014-IJDCST SPECIAL ISSUE, PAPER –ID: IJDCST-17
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Review on emergence of cyber laws in India

G. Sahaya Baskaran[1*], S.A.B. Nehru[2], P. Maria Priya[3], S. Christopher[4*]

[1]Department of Physics, Andhra Loyola College, Vijayawada, A.P-520 008.

[2] Department of Computer Science, Andhra Loyola College, Vijayawada, A.P-520 008.

[3]St. Francis de sales college, Bangalore, Karnataka.

[4] II ECE, St. Joseph's College of Engineering, Chennai, Tamil Nadu.

Corresponding author email : sbalc@rediffmail.com

Abstract: Human race has progressed due to technology which is also paved a way for the act of crime in various forms. Legal provisions should provide assurance to general public, empowerment to law enforcement agencies and deterrence to criminals. The law is as stringent as its enforcement. Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies. The number of internet users is increasing exponentially. IT professionals need good definitions of cybercrime in order to know when (and what) to report to police, but law enforcement agencies must have statutory definitions of specific crimes in order to charge a criminal with an offense. In Indian law, cyber crime has to be voluntary and willful, an act or omission that adversely affects a person or property. The IT Act provides the backbone for e-commerce and India's approach has been to look at e-governance and e-commerce primarily from the promotional aspects looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. The Information Technology (IT) Act, 2000, specifies the acts which have been made punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain omissions and commissions of criminals while using computers have not been included. With the legal recognition of Electronic Records and the amendments made in the several sections of the IPC vide the IT Act, 2000, several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC

1. Introduction

The number of internet users is increasing exponentially. In 1990, less than 100,000 people were able to log on to the Internet worldwide. In 1995, it was less than 1%. The first billion of internet users was reached in 2005; the second billion in 2010 and the third billion in 2014. Around 40% of the world population has an internet connection today. Until recently, many information technology (IT) professionals lacked awareness of and interest in the cyber crime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn't

quite fit the crimes being committed, new laws hadn't quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. Furthermore, debates over privacy issues hampered the ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy—or at the least, distrust— between the two most important players in any effective fight against cyber crime: law enforcement agencies and computer professionals. Yet close cooperation between the two is crucial if we are to control the cyber crime problem and make the Internet a safe "place" for its users. Law enforcement personnel understand the criminal mindset and know the basics of gathering evidence and bringing offenders to justice.

2. Need of Cyber laws

IT personnel understand computers and networks, how they work, and how to track down information on them. Each has half of the key to defeating the cyber criminal. IT professionals need good definitions of cybercrime in order to know when (and what) to report to police, but law enforcement agencies must have statutory definitions of specific crimes in order to charge a criminal with an offense. The first step in specifically defining individual cybercrimes is to sort all the acts that can be considered cyber crimes into organized categories.

United Nations' Definition of Cybercrime Cybercrime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus: a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them; b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in another. There are more concrete examples, including unauthorized access, Damage to computer data or programs, Computer sabotage, Unauthorized interception of communications, Computer espionage. These definitions, although not completely definitive, do give us a good starting point—one that has some international recognition and agreement—for determining just what we mean by the term cybercrime.

3. Cyber Laws in India

In Indian law, cyber crime has to be voluntary and willful, an act or omission that adversely affects a person or property. The IT Act provides the backbone for e-commerce and

India's approach has been to look at e-governance and e-commerce primarily from the promotional aspects looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. There is the need to take in to consideration the security aspects. In the present global situation where cyber control mechanisms are important we need to push cyber laws. Cyber Crimes are a new class of crimes to India rapidly expanding due to extensive use of internet. Getting the right lead and making the right interpretation are very important in solving a cyber crime. The 7 stage continuum of a criminal case starts from perpetration to registration to reporting, investigation, prosecution, adjudication and execution. The system can not be stronger than the weakest link in the chain. In India, there are 30 million policemen to train apart from 12,000 strong Judiciary. Police in India are trying to become cyber crime savvy and hiring people who are trained in the area. Each police station in Delhi will have a computer soon which will be connected to the Head Quarter.. The pace of the investigations however can be faster; judicial sensitivity and knowledge need to improve. Focus needs to be on educating the police and district judiciary. IT Institutions can also play a role in this area.

Technology nuances are important in a spam infested environment where privacy can be compromised and individuals can be subjected to become a victim unsuspectingly. We need to sensitize our investigators and judges to the nuances of the system. Most cyber criminals have a counter part in the real world. If loss of property or persons is caused the criminal is punishable under the IPC also. Since the law enforcement agencies find it is easier to handle it under the IPC, IT Act cases are not getting reported and when reported are not necessarily dealt with under the IT Act. A lengthy and intensive process of learning is required. A whole series of initiatives of cyber forensics were undertaken and cyber law procedures resulted out of it. This is an area where learning takes place every day as we are all beginners in this area. We are looking for solutions faster than the problems can get invented. We need to move faster than the criminals. The real issue is how to prevent cyber crime. For this, there is need to raise the probability of apprehension and conviction. India has a law on evidence that considers admissibility, authenticity, accuracy, and completeness to convince the judiciary. The challenge in cyber crime cases includes getting evidence that will stand scrutiny in a foreign court.

For this India needs total international cooperation with specialised agencies of different countries. Police has to ensure that they have seized exactly what was there at the scene of crime, is the same that has been analysed and the report presented in court is based on this evidence. It has to maintain the chain of custody. The threat is not from the intelligence of criminals but from our ignorance and the will to fight it. The law is stricter now on producing evidence especially where electronic documents are concerned. The computer is the target and the

tool for the perpetration of crime. It is used for the communication of the criminal activity such as the injection of a virus/worm which can crash entire networks. The Information Technology (IT) Act, 2000, specifies the acts which have been made punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain omissions and commissions of criminals while using computers have not been included. With the legal recognition of Electronic Records and the amendments made in the several sections of the IPC vide the IT Act, 2000, several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC .

During the year 2003, 60 cases were registered under IT Act as compared to 70 cases during the previous year thereby reporting a decline of 14.3 % in 2003 over 2002. Of the total 60 cases registered under IT Act 2000, around 33 % (20 cases) relate to Obscene Publication / Transmission in electronic form, normally known as cases of cyber pornography. 17 persons were arrested for committing such offences during 2003. There were 21 cases of Hacking of computer systems wherein 18 persons were arrested in 2003. Of the total (21) Hacking cases, the cases relating to Loss/Damage of computer resource/utility under Sec 66(1) of the IT Act were to the tune of 62 % (13 cases) and that related to Hacking under Section 66(2) of IT Act were 38 % (8cases). During 2003, a total of 411 cases were registered under IPC Sections as compared to 738 such cases during 2002 thereby reporting a significant decline of 44 % in 2003 over 2002. Andhra Pradesh reported more than half of such cases (218 out of 411) (53 %).

Of the 411 cases registered under IPC, majority of the crimes fall under 3 categories viz. Criminal Breach of Trust or Fraud (269), Forgery (89) and Counterfeiting (53). Though, these offences fall under the traditional IPC crimes, the cases had the cyber tones wherein computer, Internet or its related aspects were present in the crime and hence they were categorised as Cyber Crimes under IPC. During 2003, number of cases under Cyber Crimes relating to Counterfeiting of currency/Stamps stood at 53 wherein 118 persons were arrested during 2003. Of the 47,478 cases reported under Cheating, the Cyber Forgery (89) accounted for 0.2 per cent. Of the total Criminal Breach of Trust cases (13,432), the Cyber frauds (269) accounted for 2%. Of the Counterfeiting offences (2,055), Cyber Counterfeiting (53) offences accounted for 2.6 %.

A total of 475 persons were arrested in the country for Cyber Crimes under IPC during 2003. Of these, 53.6 % offenders (255) were taken into custody for offences under Criminal Breach of Trust/Fraud (Cyber) and 21.4 % (102) for offences under 'Cyber Forgery'. The age-wise profile of the arrested persons showed that 45 % were in the age-group of 30-45 years, 28.5 % of the offenders were in the age-group of 45-60 years and 11 offenders were aged 60 years and above. Gujarat reported 2 offenders who were below 18 years of age. Fraud/Illegal gain

(120) accounted for 60 % of the total Cyber Crime motives reported in the country. Greed/Money (15 cases) accounted for 7.5 % of the Cyber Crimes reported. Eve-teasing and Harassment (8 cases) accounted for around 4 per cent. Cyber suspects include Neighbours / Friends / Relatives (91), Disgrunted employees (11), Business Competitors (9), Crackers Students / Professional learners (3). Cybercrime is not on the decline. The latest statistics show that cybercrime is actually on the rise. However, it is true that in India, cybercrime is not reported too much about. Consequently there is a false sense of complacency that cybercrime does not exist and that society is safe from cybercrime. This is not the correct picture. The fact is that people in our country do not report cybercrimes for many reasons. Many do not want to face harassment by the police.

A recent survey indicates that for every 500 cybercrime incidents that take place, only 50 are reported to the police and out of that only one is actually registered. These figures indicate how difficult it is to convince the police to register a cybercrime. The establishment of cybercrime cells in different parts of the country was expected to boost cybercrime reporting and prosecution. However, these cells haven't quite kept up with expectations.

Netizens should not be under the impression that cybercrime is vanishing and they must realize that with each passing day, cyberspace becomes a more dangerous place to be in, where criminals roam freely to execute their criminals intentions encouraged by the so called anonymity that internet provides. The absolutely poor rate of cybercrime conviction in the country has also not helped the cause of regulating cyber crime. There has only been few cyber crime convictions in the whole country, which can be counted on fingers. We need to ensure that we have specialized procedures for prosecution of cybercrime cases so as to tackle them on a priority basis. This is necessary so as to win the faith of the people in the ability of the system to tackle cybercrime. We must ensure that our system provides for stringent punishment of cybercrimes and cyber criminals so that the same acts as a deterrent for others.

4. Conclusion

Computer related crime is a real, expanding phenomenon. Furthermore, a steady increase in number of such crimes in this area is expected which demands for greater attention of lawmakers. The law of the Internet has already emerged, and various governance issues cannot be resolved overnight. We will need to redefine Cyber Legal processes in this new dynamic context and should not be the same law as that applicable to physical, geographically defined territories.

REFERENCES

1. Blythe, Stephen E. (2007). China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce, Chicago-Kent Journal of Intellectual Property 7, 1.

2. Blythe, Stephen E. European Journal of Law and Economics 26:1, 75-103.

3. K. C. and Traver, C. G., 2010, "e-commerce", Prentice Hall, NJ

4. Cyber Law & Its implication By J. Sruis

5. Cyber law : The Law of Internet by J. Rosenoer

6. Blythe, Stephen E. (May, 2008). Armenia's Electronic Document and Electronic Signature Law: Promotion of Growth in E-Commerce via Greater Cyber-Security, Armenian Law Review

7. Cyber Law : Legal Principles of Emerging Technologies By Jeffrey A Helewitz.