

## Cyber Crimes in India – A Closer look

CMA. CS. DR.V.N. PARTHIBAN, PHD., FCMA, FCS, CPA, CA(I), LLM, ASM, AMT, MSW, FIII, FIIMM, M.L., MBA, MHRM, MBL, M.COM, M.PHIL, MS,\*

Email: vnparthiban@yahoo.co.in

### Introduction

The more modern scientific inventions are used for the benefit of the people, the more crimes are committed. Generally, the crimes of any sort are committed by the poor, the needy, greedy, educated unemployed etc. but the cyber-crimes are committed by the most intelligent, courageous, cunning intellectuals. From this explanation we can understand the types of the crimes committed by this section of the people. Computer is the machine, a product and brain child of scientific thinking person. Machine is incapable of committing blunders but it becomes a good material for bad people. A cybercrimes is the topic discussed time and again by the law makers of any country and police officers including CBI (Central Bureau of Investigation) and Cyber Crime Investigation Cell. They have mainly identified forgery, hacking, cyber stalking, cyber pornography phishing, carding, cracking, child pornography, e-mail bombing, tampering with computer source documents, transmitting virus, online gambling, e-mail spoofing, phreaking bypassing computer system and finally credit card frauds. Apart from these, stopping the functioning or introducing viruses or espionage are the other cyber-crimes. It has been observed that these crimes are committed not from the outside of the corporates but also for the insider who uses the information. The theft of source code, exchange of business secrets or

misusing the office computers for personal business are the other crimes that not considered by the law makers in the field of Information Technology.

Today, the computers are used worldwide and naturally there would be cyber criminals in every country. The Law maker of each country might make laws to protect the people from these criminals. But these laws are not always uniform. For example, the pornography is a crime in India according to cyber law but it is not a crime in USA. In most of the western countries cyber pornography is not at all a crime. So criminal law of one country does not attract the penal action in another country. The culture of the country frames the laws of the country but the misuse of the computers should properly be defined so that there should be universal uniformity in the definition of the crime and applicability of law for such crimes. The crimes are the product of greedy, unnatural, negative persons. They cannot be stopped from committing the crime. In certain cases, these criminals can never be identified also. That is the reason it is suggested that the laws governing the cyber criminals should be strengthened to include even the minor crimes into the framework of cyber laws. These cyber offenders can go to any extent from innocuously commit mistakes to deliberately

frighten innocent. The punishment should be commensurate with the crime and unless the crimes are properly defined with minor and major details the criminals cannot be punished. This is needed because the criminals appears to be most intelligent than law makers. The law makers should anticipate the varieties of crimes, crime within crime, crime with motivation and motiveless criminalities.

The recent technological advancements in the field of computer, communication and cyber world have brought many revolutionary changes in the world. Cyber Crimes is not a national problem but it is a problem found all over the world. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes which comes within the ambit of cyber crime. The impact of cyber-crime is not limited to any particular region or any particular target group. Any internet user may become the victim of cyber-crimes. Cyber-crimes affect every walk of society and it does not discriminate between people of different society and country.

### **Review of Literature**

Cyber Crime may be defined as the "act of creating, distributing, altering, stealing, misusing, and destroying information through the computer manipulation of cyber space; without the use of physical force and against the will or the interests of the victim"<sup>1</sup>

The encyclopedia Britannica defines 'cybercrime' as any crime that is committed by

means of special knowledge or expert use of computer technology.

Cyber Crime, in a general sense, is an act that covers the entire range of crimes which involves computer, computer network, cell phones etc.<sup>2</sup>

Cyber Crime refers to all the activities done with criminal intent in cyberspace. Cyber Crime is any unlawful act where computer is either a tool or target or both. However, any activities which basically offend human sensibilities, can also be included in its ambit. (eg.) Child Pornography on the Internet constitutes one serious Cyber Crime. Another name of cyber crimes is computer crimes.

Cyber Crime is any crime that involves computer or computer system either as a target or as a medium. Cyber Crime includes those 'Conventional crimes' in which the criminal has found a new way to launch their wrong-doing, by way of computer network or otherwise being facilitated by information technologies. The legal role of addressing and curbing cybercrime can therefore be attributed to the conventional law of crime.

Cyber Crime can generally defined as a criminal activity in which information technology systems are the means used for the commission of the crime. Basically cybercrimes are aimed at stealing the computer, damaging information, or stealing information, whereas conventional crime is not necessarily technical in origin.

Cyber Crime can be basically divided into 3 major categories being Cyber Crimes against person,

property and Government, whereas in conventional crimes there are various kinds \_\_\_\_\_

<sup>1</sup> Joga Rao, S.V., Law of Cyber Crimes, 2004, p.70

<sup>2</sup> Singh, P.K., Laws on Cyber Crimes, 2007, p.6

namely; crimes against property, crimes against person, crimes against society, crimes against Government or State etc. The following are major types of cybercrimes namely Hacking, Cyber Stalking, Spamming, Cyber Pornography, Identity Theft, Malicious Software, Child Soliciting and Abuse, Phishing, Software Piracy, Corporate, Money Laundering, Embezzlement, Password Sniffers, Spoofing, Web Jacking, Credit Card Fraud, Cyber Terrorism etc.

Cybercrime has nowhere been defined in any statute/Act passed or enacted by the Indian Parliament. The concept of cybercrime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state.

Further, there is apparently no distinction between cybercrime and conventional crime. However on a deep introspection we may say that there exists a fine line of demarcation between them. The demarcation lies in the involvement of the medium in cases of cybercrime. The sine qua non for cybercrime is that there should be an involvement, at any stage, of the virtual cyber medium. In Cyber Crime the criminals use computer, computer resources and computer networks and communication

devices as the weapon for committing their crimes, whereas conventional criminals use arms and ammunition, knives and other deadly weapons for committing the crimes. In case of cybercrimes, it is very difficult for law enforcement agencies to prosecute the criminals unlike the conventional crimes.

Cyber Crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel.<sup>3</sup> Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime.<sup>4</sup>

---

<sup>3</sup> Dr. B. Muthukumaran, Cybercrime scenario in India, Criminal Investigation Department Review, January 2 (MIS) p.17

<sup>4</sup> Pawan Duggal, *Cyber Law- The Indian Perspectives*, Saakhar Publications, New Delhi.

Computer crime as (i) any illegal action in which a computer is a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the purpose of the computer (ii) any incident associated with computer technology in which a perpetrator by intention made or

could have made a gain and (iii) computer abuse is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and transmission of data.<sup>5</sup>

### **Existing laws in India to prevent cyber crimes**

1. The Information Technology Act, 2000 (Central Act 21 of 2000)
2. Common Law (governed by general principles of law)
3. The Indian Penal Code, 1860
4. The Indian Evidence Act, 1872
5. The Bankers' Book Evidence Act, 1891
6. The Reserve Bank of India Act, 1934
7. The Information Technology (Amendment) Act, 2008 and 2009
8. Criminal Procedure Code
9. The Information Technology (Removal of difficulties) Order, 2002
10. The Information Technology (Certifying Authorities) Rules, 2000
11. The Information Technology (Certifying Authorities) Regulations, 2001
12. The Information Technology (Securities Procedure) Rules, 2004
13. Various laws relating to IPRs .

---

<sup>5</sup> Suresh T Viswanathan, *The Indian Cyberlaw*, Bharat Law House, New Delhi, (2000) p.13.

### **Conclusion**

There is an urgent need for preparing a universal code of cyber laws. These should be applicable to all the cyber-crimes of all the countries. In this context, we should understand and accept the fact that the development in the information technology must go side by side with the framing of cyber laws and cyber investigation. In most of the cases, the investigation of cyber-crimes has been handicapped by the ignorance of the system of computers. The criminals come to know before the police and law maker could do. It may not be surprising that in the days to come the cyber criminals themselves may be able to suggest to the law makers to frame ideal cyber laws. It is high time that people from information technology world investigating agency, lawyers practicing criminal side, administrators, business community to come together and discuss the nature of the crimes that might be committed in the future along with the advancement of information technology. It is an undeniable fact that without the criminals there cannot be crimes. There cannot be laws without criminalities. Let us anticipate through deep thinking, the possibilities and probabilities in the art of cybercrimes. The cyber criminals are great thinkers, fast movers and fit for any emergency situations. Their mind is more scientific minded than that the inventor of the system. The criminal activities cannot be stopped and in the same way the institution of cyber laws should not be stopped. The

law makers should imagine themselves to be criminals just as the cyber criminals are thinking themselves to be cyber law maker. I request that I should not be mistaken for the cyber criminals just because I thought deeply about the ineffective laws and very effect cyber criminals.

### References

1. Nandan Kamath, “Law Relating to Computers, Internet and E-commerce”, New Delhi, Universal Law Publishing Co. Ltd, 2000.
2. Rahul Matthan, “The Law Relating to Computer and internet”, New Delhi, 2000.
3. The day of the Cyber Pirates, Handbook of Cyber Law, Macmillan India Ltd., 2000
4. Amita Verma, Dr. “Cyber Crimes in India”, Central Law Publications, Allahabad, 2012.
5. Manish Kumar Chaubey, “Cyber Crimes and legal measures”, Regal Publications, New Delhi, 2013.
6. Mishra.J.P., “Introduction to Cyber Laws”, Central Law Publications, Allahabad, 2012.
7. Singh, P.K., “Laws on Cyber Crimes”, Book Enclave, Jaipur, 2007.

**About Authors:** \*Associate Professor and HOD, Department of Commerce, RKM Vivekananda College (Govt. aided)(Autonomous), Mylapore, Chennai-600 004. Email: [vnparthiban@yahoo.co.in](mailto:vnparthiban@yahoo.co.in) (Cell No.9884723138)

\*\* Paper presented at UGC Sponsored National Seminar on “Cyber Security with Special Focus to cybercrimes and cyber laws” organized by Departments of Computer Science, P.B.Siddhartha College of Arts and Science, Vijayawada-10.