IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

Impact Factor: 7.301

Volume 3, Issue 3, December 2023

Effect of Cyber Crimes in Education: Need for Specific Legal Framework

Sushma Narsinha Prasad Subedar

Research Scholar, Department of Post Graduate Studies in Law,
Shri JJT University, Jhunjhunu, Rajasthan

Abstract*: Of all the significant advances made by mankind, probably the most important is the development of internet. The real power of today's internet is that it is available to anyone with a computer, mobile phone, etc. Initially when internet was developed, the founding fathers hardly had any inclination that it could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are a number of crimes committed in cyberspace due to the anonymous nature of the internet. Hence, the need for stringent cyber laws.*

Keywords: cyber laws

I. INTRODUCTION

It has been precisely said, he modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb". At present, the transition from paper to paperless transactions has been made possible through technological developments. Computers are extensively used in the storage of confidential data of political, social and economic or personal nature which are of immense benefit to the society. The use of computers and mobile phones in India and Iraq is increasingly spreading, and more and more users are connecting to the internet. Internet is a source for almost anybody to access, manipulate and destroy other's information.

The rapid development of the internet and computer technology globally has also led to the growth of new forms of trans-national crimes especially those which are internet related. These criminal activities directly relate to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored data, or sabotage of systems and data. These crimes have virtually no boundaries and may affect any country across the globe within a fraction of a second The ways of tackling cyber crimes through legislation may vary from one country to another, especially when cyber crimes are committed within a specific national jurisdiction with different definition and socio-political environment, i. India. Cyber crimes likewise pose the biggest challenge for the police, prosecutors and legislators. Crimes of this nature are usually indulged in by young teens, recreational computer programmers and persons having vested interest. Unlike conventional crimes, there is no policeman patrolling the information superhighway, leaving it open to everything from trojan horses and viruses to cyber stalking, trademark counterfeiting and cyber terrorism.

The question that arises is what constitutes a computer crime and how can it be distinguished from other routine crimes? The query has no legal answer because no Indian legislation gives any precise or concise definition for the same. However, some recent changes in the Indian Penal Code provide punishments to certain acts without making any specific reference to computers. This creates a lot of imbroglio in the minds of cyber users because of the confusion arising out of how any rule or doctrine should be made applicable in case of infringements or violations made by parties within the country and outside.

Another critical issue in the cyber era relates to the jurisdiction of a Court to hear and determine a dispute within their respective sovereign territories. Because the legal establishment of e-commerce has no geographical boundaries, it establishes immediate long-distance communications with anyone who has access to internet. For e.g., engaging in e-commerce on the internet may expose the company to the risk of being sued
in any State or foreign country where an internet user can establish a legal claim.

In consideration of the above issues under the scope of cyber-crimes and their impact on global socio- economy and education, it is therefore appropriate that stringent legislative measures should be taken India before it is too late.

Effect of Cyber Crimes in Education:

In every nation is concerned of the growing trend of cyber crimes in education sector. For instance, the Human Resource Development Ministry in India had warned in June 2010 all Central Educational Institutions and regulatory bodies to beef up cyber security measures to prevent their websites from being misused b frauds to mislead students. The move had followed the hacking of the website of the National Assessment and Accreditation Council, the country's largest higher education rating agency. The hacking set off alarm bell within the Ministry because it represented the second major attempt by little-known and unrecognized education groups to use popular websites to mislead students.

After the attack on the National Assessment and Accreditation Council, the All India Council f Technical Education, the apex technical education regulator, became the second victim of a "cyber raid". The original All India Council for Technical Education at the time had a website address, aicte.ernet.in, and the unrecognized body, which claimed to offer myriad courses in computer engineering across the country, started a website with the address aicte.ac.in. The success of the fraud was gauged from the fact that aicte.ac.in received significantly higher Google hits than the website of the genuine All India Council for Technical Education. The genuine All India Council for Technical Education eventually created a new website, aicte- india.org. Many students were fooled by the fake All India Council for Technical Education website.

It is therefore incumbent that programmers recognized internationally to deal with cyber crimes in education sector should be adopted at the earliest. Such programmers should as well be designed to be accessible to members of law enforcement on an international basis.

II. CONCLUSION

Internet has over the years grown in a completely unplanned and unregulated manner. Even the inventors of Internet could not have really anticipated the scope and far reaching consequences of cyberspace. With the spontaneous and almost phenomenal growth of cyberspace, new and ticklish issues relating to various legal aspects of cyberspace have begun cropping up. It may be noted that a wide variety of statutory provisions, administrative regulations and codes of practices are in place to contain cyber crimes in India. However, the existing legal measures i.e., the Indian Information Technology Act, 2000, are inadequate to deal with the emerging intricate cyber crimes.. In response to such issues cyber law or the law of internet is now inevitable.