International Journal of Academic Research
ISSN: 2348-7666; Vol.9, Issue-2(1), February, 2022
Impact Factor: 6.023; Email: drtvramana@yahoo.co.in

LEGAL PROTECTION OF TECHNOLOGY USERS WITH REFERENCE TO VICTIMS OF POTENTIAL CYBER CRIMES

D. Vasantha Kumari
Dr. B.R. Ambedkar College of Law
Andhra University, Visakhapatnam

We had been acquainted with the usage of Phones since the British regime, which was invented by **Graham Bell** in 1885. Subsequently with the technological innovation, mobile phones are playing a greater role and provided an easy access for all kinds of transactions.

The creativity and innovation of **Sir Martin Cooper** brought a drastic change and now the usage of the instrument mobile phone in the current generation had become a part and parcel of human life and its usage is unavoidable despite of its harmful affects of radiation.

With the emergence of the word 'Digital', man had been in search of a tool or device to compute his electronically driven work for sharing his views and work. Computer and Internet had been made an access for the same and as years passed the Smart Mobile Phone had made its entry making a man completely addicted to it having access to internet.

The possible involvement of the Technology after the digitalization having access to a variety of transactions which include the E-commerce, electronic banking and reached its peak even to the extent of cash transaction across the country and the globe.

In the days to come, no surprise, separate budget secession is required to make policy for online business. However, opportunity followed by Crime is true, and technological space is no exception. This chapter deals with crimes online.

With advances in computers and telecommunications most businesses and many individuals have become dependent on computers and networks to carry out every day activities. Cyber crime is an evil having its origin in the growing dependence on computers in modern life. As the society is advancing, criminal tendency and methods of committing crime are also changing substantially.

World is undergoing a second Industrial Revolution. Information Technology today touches every aspect of life, irrespective of location on the globe. Everyone's daily activities are affected in form, content and time by the computer. Business, Governments and individuals all receive the benefits of this information Revolution. While providing tangible benefits in time and money, the computer has also had an impact on everyday life, as computerized routines replace mundane of human tasks.

Against Individuals : Harassment via email, Cyberstalking, Pornography, Defamation, Unauthorized Control, Indecent Exposure, E-mail Spoofing, and Cheating & Fraud.

Against Individual Property : Transmitting Virus, Net Trespass, Unauthorized Access, IP Crimes and Time-Thefts
Against Organization : Unauthorized Control, Possession of Unauthorized Information, Cyber Terrorism, and Distribution of Pirated Software.
Against Society at Large : Pornography, Trafficking, Financial Crimes, Sale of Illegal Articles, Online Gambling and Forgery.

Cybercrime involves activities like credit card fraud, unauthorized aces to computer systems, child pornography software piracy and cyberstalking. Electronic commerce includes encryption and data security. Abuse of freedom of expression includes defamation, obscenity issue and censorship. Intellectual property rights cover copyright, software licensing and trademark protection.

Legal reforms necessitated in the respective areas for its integrity, authentication and proper regulation to prevent the potential threats like Cyber-Crimes and online frauds, are being continuously undertaken and it is obvious that one must be familiar with the laws relating to it.

Smart phone having replaced a personal Computer or a laptop carved a blooming path for the cyber criminals to tamper, invade, inflicting malware and taking unauthorized access, such as Ransomware, Vishing, Smishing, Lottery Scams, Blue Bugging, Blue Jacking, Blue Snarfing besides Stalking and Spam, and Hacking etc., and damaging the interest of the common man, companies and any organization.

Cybercrimes may be territorial or international by its very nature. Users of Smart Mobile Phones must be aware of the attacks and protect themselves by adopting proper security tools to minimize threat.

Despite several security measures having been undertaken by the competent authorities to prevent the Cyber Crimes, the security survey reveals that the cybercrimes are increasing rapidly. Basic factors rejuvenating Cyber Crimes favorable to the offenders in accomplishing their task are :

i) Jurisdiction
ii) Jurisprudence
iii) Lack of investigating tools in tune with existing technology crimes.
iv) Volatile Evidence

i) JURISDICTION wherein Space transformed into Place
Dependence on internet has transformed the notion of space into place. The technological innovations have gradually merged into our popular culture and intertwined inextricably with our day-to-day lives.

The basics issues is that the notion of space is also related to the ideas of ‘presence’ or ‘being’ and how technologies can transform the feeling of identifying oneself in the cyberspace. If technology can transform our feelings of being presenting a separate space, then perhaps one can accept the existence of ‘cyberspace', which is incidentally said to have emerged out of the use of Information Technology.

The basic features that could be attributed to the cyberspace are place without boundaries, the relative study of borders of real world and cyber world,

notice, transborder data flow, regulating professional conduct on net etc. These basic features could be considered as characteristics of cyberspace.

a. Place without a Location[1]

Global computer-based communications move across the globe cutting down the distances and lifting the barriers.

b. Notice

Physical boundaries are appropriate for the delineation of law in the physical world because rules change when the boundaries are changed / crossed. Proper boundaries have signposts that provide warning that will be required, after crossing, to abide by different rules, and physical boundaries are generally well-equipped to serve this signpost function.

c. Trans Border Data Flow[2]

The concern of the governments to regulate Data Flow, crossing their territorial borders has increased. All countries are striving to curb, cabining, or confine data flow.

d. Regulating Professional Conduct on the Net[3]

Almost everything involving the transfer of information can be done online like, education, health care, banking, the provision of intangible services, all forms of publishing, and the practice of law. The laws regulating many of these activities have developed as being distinctly local and territorial. In other words, authorities certify the individuals to take up a particular profession. But on the net any service could be rendered to any body without any kind of regulation or vigilance.

ii) JURISPRUDENCE

Jurisprudence[4] in proper perspective is meant to inquire into the fundamentals of law, aimed at conceptualizing every branch of law, focused on precision, needed to balance between changes in the society and expected changes in law and meant to unravel the confusion surrounding the concept of law.

With the increase of offshoots of law, the legal studies have gained unprecedented importance; many branches which were never considered as part of legal studies have gained immense importance in the present scenario. The reason is, instead of considering rules of law as simply something to be accepted as part of natural order or sovereign power, the subjects of law started questioning the rationality of rules, bylaws, orders and ordinances passed by appropriate authorities, on the premise of every aspect of legal system like legislation, judicial process, the working of legal profession, bench and bar relation, etc, which in turn have become legitimate fields of legal study. Understanding law needs interdisciplinary approach of social studies, political science, psychology, anthropology and different religious, customary practices.

iii) LACK OF INVESTIGATING TOOLS IN TUNE WITH EXISTING TECHNOLOGY CRIMES :.

The growth and utilization of the Internet for communication as well for commerce has been surpassed in modern history. One of the foremost challenges being the utmost need of the hour is to track down sophisticated users of technology to commit unlawful acts on the Internet by hiding their identities by upraising the need for close coordination among law enforcement agencies and the requirement for well-trained and equipped personnel to gather evidence, investigate, and prosecute the related cases. FBI had already placed a high priority on investigating cyber crime matters. Various types of important tools used for preventing unlawful actions are

Kali Linux, Ophcrack, EnCase, SafeBack, Data Dumber and Md5sum[5]. In Bharat the institution "Indian Computing Emergency Response Team(CERT In)" being declared as nodal agency in Bharat under Section 70B of IT Act, 2000 but investigating agencies are yet to be well trained to combat crimes at the basic level of our Country.

iv) VOLATILE EVIDENCE :

Evidence being essential for combating crimes and it's assessment had ever been a challenging question before Judiciary for combating Cyber crimes. The most important factor enabling the cyber criminals to escape their liability is volatile evidence which could otherwise be effectively collected using live forensic methods existing in system's RAM(Random Access Memory) being available in a Computer memory. It is indeed difficult to ensure the availability of tools to make copies of RAM and hard drives on running Systems and line-of-business servers will not shut down ensuring those copies to be forensically sound.

It has been observed that "cyberspace' is no more a fantasy, but is more pragmatic, serious and alarming space/place/zone demanding urgent attention of the whole technical and juridical problems complex, which connected with absence of:

1. Legislation
2. Specially trained staffs
3. Necessary technical measures.

The legislative effort to mitigate cybercrime, at global level, at present is not up to the mark. Indian Parliament passed Information Technology Act, 2000 in the year 2000 and then subsequent substantial amendments carried into it in the year 2008 since then till date no single amendment has been made or no new law has been passed. This inactiveness of legislators made Information technology Act 2000 toothless. This insensitive approach made cyber space vulnerable to cyber crimes. It is not out of place also to observe that, howsoever disheartening to say so, neither the judicial officers nor the investigating and enforcing agencies are meekly versed on the technical aspects of IT laws.

Techno-legal safeguards sought to be provided by the state through successive legislations on the other, apparently stand to serve little or no purpose unless there is an issue based amendment from time to time. To overcome at least some problems, the following measures to be taken for combating ecommerce crimes:

1. Harmonizing laws and procedures globally,
2. Improving the technical capabilities of investigators, and
3. Sharing information between public and private sector investigators and
4. Enhancing international cooperation.

A strong education system should be followed in the society to deliver education at every stage of the society with a special stress on Information Technology which should be secure and free from cyber crime and in reach to a common man apart from educating and involving the media professionals, netizen and then encourage them to increase public awareness.

The next mandatory factor to combat Cyber crimes is that the law enforcement personnel must be trained and equipped to tackle high-tech crimes. In furtherance the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime should be permitted by legal systems.

Last but not the least is that practise of continuing effort to enforce regulations could reduce criminality to a minimum.

---

[1]Law And Borders-The Rise of Law in Cyberspace by ©1996 David G. Post & David R. Johnson;48 Stanford Law Review 1367 (1996)- © 1996 David G. Post & David R. Johnson. Permission granted to redistribute freely, in whole or in part, with this notice attached.

[2]"Trans border Data Flow Debate" by B.M.GUPTA & S.P.GUPTA Annals of Library Science and Documentation Vol 29(2), June 1982 page 51-63.

[3]"Prescription Drug Fraud and Misuse" by Julie Wartell and Nancy G. La Vign; 2nd Edition (2012 available at http://www.popcenter.org/problems/prescription_fraud/print/.

[4]Dias 'Jurisprudence' Fifth Edition Aditya Books, Butter Worths.

[5]What is Cybercrime? Types, Tools, Examples by Lawrence Williams – https://www.guru99.com.