PREVENTION AND CONTROL OF CYBER CRIMES IN INDIA: PROBLEMS, ISSUES AND STRATEGIES

(ABSTRACT)

A. INTRODUCTION

As a saying in criminology goes – “a crime will happen where and only when the opportunity avails itself.” Until recently, we were aware of only traditional types of crimes like murder, rape, theft, extortion, robbery, dacoity etc. But now with the development and advancement of science and technology there came into existence machines like computers and facilities like internet. The internet has opened up a whole new virtual heaven for the people both good and bad, clever and naive to enter and interact with lot of diverse cultures and sub-cultures, geography and demographics being no bar. The very same virtues of internet when gone in wrong hands or when exploited by people with dirty minds and malicious intentions, make it a virtual hell. Stories of copyright theft, hacking and cracking, virus attacks and plain hoaxes etc. have mounted up in the last few years. As a result of the rapid adoption of the internet globally, computer crimes are multiplying like mushrooms. The law enforcement officials have been frustrated by the inability of the legislators to keep cyber crime legislation ahead of the fast moving technological curve. At the same time, the legislators face the need to balance the competing interests between individual rights such as privacy and free speech, and the need to protect the integrity of the world’s public and private networks.

B. OBJECTIVES OF THE STUDY

The objectives of this research work are to touch all the important facets of the cyber crimes in a comprehensive way and to achieve new insights into it. The main objectives of the present study are as under:

1. To understand the basic concepts of the cyber world.
2. To trace the origin and development of the cyber crimes.
3. To examine critically the position of intellectual property rights in cyber space.
4. To analyze the principles of jurisdiction in cyber offences.
5. To discuss comprehensively the concept of electronic evidence.
6. To decipher as to how the issue of cyber crimes has been dealt with in the Indian scenario.
7. To find out the international initiatives to curb cyber menace.
8. To point out the possible defects in the existing laws relating to cyber crimes.
9. To suggest the reforms and remedial measures for the prevention and control of cyber crimes.

C. SCHEME OF CHAPTERS

The present research work has been divided into nine chapters.

Chapter I – ‘Introductory’
Chapter II – Basic Concepts of the Cyber World: An Overview’
Chapter III – Cyber Crimes: Meaning, Definition, Nature, Scope, Elements, Characteristics and Classification
Chapter IV – ‘Intellectual Property Rights in the Cyber Space’
Chapter V – Jurisdiction and the Internet: A Global Medium in a Territorial World
Chapter VI – Electronic Evidence: Tracking Digital Footprints’
Chapter VIII – ‘Global Perspective of Cyber Crimes and the related Laws’
Chapter IX – ‘Conclusions and Suggestions’

D. SUGGESTIONS

Based on the study following meaningful suggestions are recommended:
1. Net Security be tightened up
2. Use of Encryption Technology
3. Intrusion Management
4. False E-mail identity registration be treated as an offence
5. Self-regulation by Computer and Net Users
6. Liberalization of Law relating to Search and Seizure
7. Use of Voice-recognizer, Filter Software and Caller ID for Protection against Unauthorized Access
8. Development of Cyber Forensics and Biometric Techniques
10. Need for a Universal Legal Regulatory Mechanism
12. Need for Universalization of Cyber Law
13. Interpol and Emergency Response Computer Security Team
14. Combating the Menace of Cyber Terrorism
15. Special Cyber Crime Investigation Cell for Hi-Tech Crimes
16. E-Judiciary and Video-Conferencing for Speedy Justice
17. Need for Cyber Crime Reporter or Cyber Law Journal
18. The Information Technology (Amendment) Act, 2008 – A Step in the right direction
19. Digital Time Stamping System (DTS)
20. Extradition Treaty: Need of the Hour
21. Establishment of Special Cyber Courts to try Cyber Crimes
22. Diffusion of Internet Technology in India
23. Technical Means for Blocking of Errant Websites
24. Planting of Baits in Cyberspace for Worms and Viruses
25. Regulation of Social Networking Sites
26. Decentralization of the National Informatics Centre
27. Appointments under the IT Act, 2000: Fair, Transparent and Speedy
28. Need for Increased Awareness among Victims of Cyber Crimes
29. Need for Imparting Training to Officials to Investigate Cyber Crimes
30. Need for connecting Cyber Cafes with Police Control Rooms.