LEGAL DIMENSIONS OF CYBER CRIMES AND PREVENTIVE LAWS WITH SPECIAL REFERENCE TO INDIA(2010). By Vishwanath Paranjape. Central law Agency, Allahabad. Pp. .xxxi+356. Price Rs.350/-.

THE TECHNOLOGICAL changes are boon for mankind and the Internet has changed the life of people altogether. One can communicate across the world through e-mail. The data can be downloaded or sent anywhere in no time. The social networking sites have facilitated contacts with near and dear ones. Businesses are being conducted on-line. Almost everyone is accustomed to the virtual world and accesses the same. However just like the real world the virtual world is not free from crimes. The persons committing the crimes are technological savvy. The kinds of crimes that can be committed are social crimes e.g. cyber stalking; financial crimes like credit card frauds, intellectual property crimes; crimes against state e.g. cyber terrorism *etc.*. The crimes may specifically target the computer system or the computer may be used as a medium to commit crimes. In such a situation it was not possible to leave the cyberspace in uncontrolled situation. This had led to passing of the Information Technology Act, 2000. The Act, initially covered fewer cyber crimes but was amended in 2008 to include some more crimes. It gives legal recognition to electronic evidence and has amended the Indian Evidence Act, 1872. The Act has also amended the Indian Penal Code, 1860, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934. The evidence available in electronic form requires an expert knowledge to interpret it and hence this led to the development of field of cyber forensics. The police have challenging task of enforcement of the legislation as they have to depend on modern tools and techniques to investigate cyber crime. Often the cyber criminal remains unpunished because the crime can be committed sitting anywhere in the world and thus creating the problem of exercising jurisdiction over the accused person. To prosecute the accused the country requires extradition treaties with other states. The extradition will not be possible if the act committed by accused is not a crime in that country. At present very few countries have legislation on cyber crimes.

This necessitates some literary work in the area of cyber crimes and such efforts have been made in the book under review. The author has based this book on his Ph.D. thesis with modifications. The book consists of eight chapters and five appendices. Chapter I of the book is an introductory chapter and has covered history of computer and Internet. It consists of definitions of cyberspace and cyber crime, the scope and characteristics of cyber crime and reasons of cyber crime. Some of the reasons given are huge data storage capacity, wider access to information, negligence of network users, non availability or loss of evidence *etc.* It has dealt with

the kind of persons, like children, professional hackers, disgruntled employees, who may indulge in such kind of criminal activities. It has further discussed about the cyber law and its importance.

Chapter II is on various cyber crimes and their classification. The author has dealt with the unique features or peculiar characteristics of cyber crime like no territorial barriers, evidence in digital format, perpetrators being high tech persons, anonymity of the perpetrator. The author before classifying the crimes has dealt with forms of computer attacks that help to gain unauthorized access to the network. He has further discussed about the various cyber crimes. Under the heading "General Classification" he has divided the cyber crimes into three heads *i.e.*. against 1) individuals 2) property and 3) State. He has dealt with crimes like harassment through e-mails, cyber stalking, pornography, unauthorized access/hacking, defamation and e-mail related crimes like spoofing, spamming, bombing *etc.* In unauthorized access the techniques used by hackers like Packet sniffing, Password cracking, Buffer overflow and web jacking has been discussed. The crimes against property included are computer vandalism, intellectual property crimes, data and internet time theft *etc.* There is discussion on computer P.C. virus *viz.* file infectors, boot sector viruses, macro viruses other multi-partite viruses under computer vandalism. Further certain major virus incidents like Melissa, Trojans, worms and logic bombs have been dealt in the chapter. Finally there is discussion in the chapter on various crimes against state or society in general *viz.* cyber terrorism, trafficking, financial crimes *etc.*

Chapter III is on modes and techniques of cyber crime which deals with the tools and techniques used by perpetrators to commit cyber crime by using computer, computer system or computer network. The author has briefly explained the terms like computer hardware, software, computer memory, RAM and ROM. There is discussion on unauthorized access as a mode. Further the author discusses the preventive measures to deal with flaws in computer security system. While dealing with unauthorized access modes some of the terms which were already explained in chapter II have been repeated like password cracking, buffer overflow, phishing and web jacking. The author could have made reference of chapter II instead of being repetitive.

Chapter IV deals with intellectual property crimes. There is a general discussion on kinds of intellectual property rights, patenting in software in the US and India, copyright protection on internet. It further discusses the *Eastern Book Company* and *Daljeet Titus* cases. These were civil suits filed for copyright infringement and had sought civil remedies. The author has made a detailed discussion on copyright protection of software programs and discussed foreign cases on copyrightability of computer programs, statutory protection of computer programs in India, and how copyright in computer programmes can be infringed through internet. The author then turns the discussion on version recordings under Copyright Act and then once

again moves on the aspects of computer programmes like reverse engineering, open source software, measures to prevent software piracy, and brief discussion on international efforts to protect computer piracy through TRIPs agreement, WIPO Internet Treaties, DMCA , 1998 *etc.* Further there is discussion relating to domain name disputes and numbers of cases have been discussed relating to passing off (a remedy under law of torts) by using domain names deceptively similar to already existing trade marks. Further the legal issue of cyber squatting has been discussed. The chapter ends with a brief and general discussion on geographical indications, lay out designs and integrated circuits and other intellectual property rights. As the book relates to cyber crimes, it was expected from the author that he will concentrate on the piracy in musical works, sound recordings, films through use of new technologies, the statistics relating to that, criminal cases decided on these specific areas and also the efforts of IMI, NASSCOM and other organizations to combat piracy. The chapter is not as per expectations of readers who specifically would want to gain knowledge about the criminal aspects of intellectual property.

In chapter V author has discussed certain judicial decisions on cybercrimes. Under the topic "Cyber Jurisdiction" the author has covered some of the US cases relating to cyber jurisdiction. In *United States* v. *Thomas* a complaint was filed under the US law of obscenity. The court assumed jurisdiction on the basis of distributing and downloading of obscene material in the forum state. The Indian cases which the author has mentioned on cyber jurisdiction are relating to civil jurisdiction and not the criminal jurisdiction. The *P R Transport Agency* v. *Union of India* referred by the author, was on the issue of civil jurisdiction of court in a suit relating to performance of contract made through e-mail. The chapter further deals with judicial recognition of electronic evidence and many US and Indian cases have been discussed on electronic evidence. The case of *SBI* v. *Rizvi Exports Ltd.* deals with section 65B of the Indian Evidence Act where the court admitted the computer print outs, CD Rom *etc.* as evidence, with the authenticated certificate. In the other case mentioned as the *Parliament Attack* case, the court relied on digital evidence in the laptop and smart media storage disks and devices recovered from the truck intercepted at Srinagar. Further the Australian, US and Indian cases on unauthorized access to protected system have been discussed. The Indian cases referred on cyber pornography are *Suhas Kutti* case, *Avinash Bajaj* case commonly known as *Baazi.com* case, *Fatima Rizwana* case, *Air Force Bal Bharti* case *etc.* Here the prosecution was done under section 67 of the Information Technology Act, 2000. The *Soni Smabandh* case *and Pune Citibank bank* cases that discussed were concerned with credit card fraud. In the intellectual property related crimes the author has discussed the cases relating to civil disputes and none of the criminal cases have been mentioned. The *Nasscom* case has been discussed on phishing, in which the Delhi High Court has ruled that phishing is illegal. The *Mount Everest Mineral Water* case is inappropriately

put under the heading phishing as the case is on use of deceptively similar trade marks. Further the author has dealt with judicial approach to cyber forensics which includes cyber evidence. The author could have made a detailed discussion of cyber forensics, laws relating to that and the judicial approach in a separate chapter in order to give a better understanding of the subject to the reader.

Chapter VI is on global perspective of cyber crimes where the author has discussed what efforts have been made internationally to combat cyber crimes. The chapter includes the text of European Convention on Cyber Crime, 2001, apart from the discussion on various conferences or summits held for the purpose like G7 Summit, OECD, ICC *etc.* The text on cyber crime convention could have been given in the appendix and only the important provisions could have been analysed by the author in the chapter. There is also brief discussion of laws on cyber crimes incorporated in their legal system by some countries like the United States, United Kingdom, Australia, Japan *etc.*

Chapter VII deals with legal provisions relating to cyber crimes under Information Technology Act, 2000 and the amendments to Indian Penal Code briefly, without any analysis of those provisions. The author has also dealt with provisions on interception, National Nodal Agency. Further in legal issues relating to investigation of cyber crimes, the author discusses the problems involved in investigation and the provisions of the Information Technology Act which confer power for investigation. The author could have discussed the investigation aspect along with cyber forensics as the evidence is collected at the stage of investigation. This would have facilitated the readers interested in gaining knowledge about cyber forensics, otherwise the readers will have to go through all pages to get the clear understanding of the subject. Further the author has given statistics of cases registered under cyber crimes in India from 2005-2009. On that basis author has suggested that preventive strategies should be evolved to deal with constant increase in crimes and focus should be on crime prone regions. Lastly in this chapter the author has discussed the preventive strategies like electronic surveillance, intrusion management, data protection *etc.*

In Chapter VIII, the author concludes that not many countries have enacted cyber crime legislation and this is used as a loophole to escape punishment by cyber criminals. There is lack of adequate cyber forensic technology to deal with cyber crimes which is a hurdle in cyber crime investigation. The problem of exercising jurisdiction in case of cross country disputes needs to be resolved. Finally the author suggests the ways to tackle cyber crime by tightening net security, use of encryption technology, use of preventive strategies, development of cyber forensics, and universal legal regulatory mechanism *etc.*

The five appendices in the book include 1) the Information Technology Act, 2000, 2) the Information Technology (Amendment) Act, 2008, 3) the rules relating

to safeguards for interception and monitoring, and decryption, 4) the rules for monitoring and collecting traffic data, and, 5) the cyber regulations and appellate tribunal procedure rules. Out of the 356 pages of the book, 88 pages have been used for Appendices and Index.

There is dearth of literary work on the above subject and the author has to be complimented as he has tried to cover all aspects related to cyber crimes. It will be of immense use to the reader who wants to gain knowledge on the kinds of cyber crimes, how cyber crimes are committed, what are the legal provisions relating to cyber crimes and the recent judicial precedents on the subject. By removing the shortcomings as suggested above, the book can become a excellent piece of work on the subject. The book is fairly priced and will attract wide readership by those interested in the area of cyber crimes.

Poonam Dass[*]

[*] Assistant Professor, Faculty of Law, University of Delhi.