

**BOOK REVIEW: CYBER LAWS, JUSTICE YATINDRA SINGH  
(UNIVERSAL LAW PUBLISHING CO., 2010)**

*Prof. Ashwani Kumar Bansal\**

The phenomenon of the internet has revolutionized the world – the way we communicate, do business, store information, run machines or even open river gates to control the production of electricity and maintain water levels in reservoirs. All of this happens at the mere click of a mouse while sitting at distant places through signals sent via satellites and novel devices based on digital technologies. The internet is largely a network of computers spread all across the world and connected to one another through hardware, routers and cables. There are numerous private or government agencies that keep our precious data in electronic form. Anyone who has a bank account is being served by networked or stand-alone computers. We use ATMs, debit cards and credit cards for shopping and use email, cell phones and SMS for communication. Thus, in the present digitized world, no one can really claim to be unaffected by cyber law altogether.

Cyber crimes such as online banking frauds, source code thefts, virus attacks, phishing attacks, email and website hacking, etc. have become common place. It is for these reasons that ‘cyber law’, that is, the legal aspects of the cyber world has become important. The cyber law of India is mostly found in the Information Technology Act of 2000.<sup>1</sup> Necessarily, all the good about technology can always be used in an adverse manner, and therefore, the role of the law is to maximize the good and minimize the adverse.

The book ‘Cyber Laws’, by Justice Yatindra Singh, a sitting judge of Allahabad High Court, has been published by Universal Law Publishing Co. and is now in its fourth edition. The book is a comprehensive guide to the various legal issues which have arisen as a result of the unprecedented growth of the internet. It covers both academic and practical information regarding technology-related issues and the underlying legal principles which have been applied in these areas. Part I of the book has 146 pages of commentary and Part II contains relevant Acts, rules, notifications,

---

\* Professor In-charge, Law Centre-I, Faculty of Law, University of Delhi.

<sup>1</sup> Information Technology Act, 2000, No. 21 of 2000 (hereinafter ‘IT Act’).

circulars, etc. in 276 pages. The book provides an overview of the cyber law scenario in India. The material is well researched and clearly described in thirteen concise chapters.

Justice Singh has included multi-faceted introductory material that also covers new developments in other jurisdictions. He simplistically guides the reader and provides suitable inputs at all times. He does not cling to a rigid structure and attempts to incorporate diverse information in the book on all relevant occasions. He has included pertinent case law and discussed the implications of the same for future legal developments. The author uses foreign case law to explain propositions in relation to the law in India. He explains the *Pettigrew* case<sup>2</sup> and the *Myers* case<sup>3</sup> so as to inform the reader about the acceptable level of amendment that can be brought about in the law of evidence in India through the IT Act.

The book not only explains the law as it is but also informs the reader about the practical aspects of using information technology. It is necessary for a reader to comprehend why Justice Singh is explaining things that appear un-connected at first glance. However, I am quite confident that at a subsequent time the reader will find out how these nuggets that amount to no more than two or four pages have helped clarify issues. It is this attention to detail that he has given that one may not find in other books on cyber law. The underlying logic appears to be that once a person knows something, only then he realizes how much he does not know and may crave for that knowledge. I must therefore congratulate Justice Singh for accomplishing this onerous task.

Justice Singh takes the reader to the UNCITRAL Model Law on E-commerce, the basis for the IT Bill of 1999 that resulted in the IT Act. The IT Act provides legal infrastructure for e-commerce transactions, recognises electronic documents as legal evidence, opens up business opportunities for digital certificate companies, paves the way for e-governance transactions, and creates specific provisions against cyber crimes. In 2002 itself, it was felt that the IT Act needed amendments to address current issues and challenges in the cyber world. The Inter-Ministerial Working Group on Cyber Law and Cyber Forensics was established in November 2002 in order to pursue this object. The present reviewer was appointed as the Member-Secretary of this group and on the basis of the deliberations in this group and other related groups, an expert committee was later constituted to suggest amendments to the IT Act. The amendments suggested were introduced in Parliament as the IT (Amendment) Bill of 2006 which was modified and passed by Parliament on 23 December,

---

<sup>2</sup> R v. Pettigrew, (1980) 71 Crim. App. 39 (C.A.) (U.K.).

<sup>3</sup> Myers v. DPP, [1965] A.C. 1001 (C.A.) (U.K.).

2008. IT (Amendment) Act of 2008 received the assent of the President of India in February 2009 and then was brought into force on 27 October, 2009. The book covers all the important changes introduced by the IT (Amendment Act) of 2008. The book also incorporates several important provisions of the Communication Convergence Bill of 2001.

The book is divided into two Parts. Part I deals with different aspects of cyber laws with discussions on various topics, controversies and possible solutions. The book discusses several foreign statutes and provides citations using online sources in order to enable easier access. Chapter I deals with the historical background of the IT Act and in 10 sections refers to the different provisions of the IT Act. It also includes a brief section on Electronic Funds Transfer. Chapter II introduces the basic concepts of Intellectual Property Rights and also discusses issues in relation to international organisations and important treaties. In Chapters III and IV, the author discusses computer software and copyright in an interesting fashion and introduces the idea of 'Copyleft.' He analyses the existing controversies in relation to computer software and patents and includes a concise discussion on the idea of 'Invention.' He also introduces the reader to the new field of business method patents. Chapter V discusses the system of protection in relation to trade secrets and reverse engineering and talks about the important issue of disassembling copyrighted software. Chapter VI may be an eye opener to those who have not come across the terms 'open source code' and 'proprietary code' and the myriad issues relating to the open document format. Chapter VII deals with font licenses and Justice Singh suggests that the Government of India should release fonts on a copyleft basis and grant the permission to use and modify the same through an open source code. Chapter VIII deals with IPR in cyber space and the legal problems faced by websites hosting illegal content and internet service providers. Chapter IX deals with the protection of semiconductor topography as per the Semiconductor Integrated Circuit Layout-Design Act of 2000 and details the different advantages and disadvantages of the protection afforded under the Act. Chapter X deals with e-commerce and taxation in a nutshell. Chapter XI discusses the grey areas of privacy and 'cyberslackers.' Chapter XII deals with how information technology can help in case management, court management and self improvement and bring about major changes in the legal system. The conclusion of the entire discussion is stated in brief at the end.

Part II provides useful and important legal instruments including Acts, rules, regulations, treaties, notifications, policies, guidelines, etc. These instruments are updated and so provide an invaluable resource for further research.

In sum, the book aptly discusses how some persons have been misusing the phenomenon of the internet to proliferate criminal activities in cyber space, how such activities can be curbed through suitable law, and how a pressing challenge faces the cyber law regime in India. The book provides concrete suggestions regarding the manner in which the flaws, loopholes and ambiguities observed in certain provisions of cyber law can be tackled and encourages the reader to engage with the length and breadth of the entire subject.