EAS Journal of Humanities and Cultural Studies
Abbreviated Key Title: EAS J Humanit Cult Stud
ISSN: 2663-0958 (Print) & ISSN: 2663-6743 (Online)
Published By East African Scholars Publisher, Kenya

OPEN ACCESS

Volume-1 | Issue-6| Nov-Dec-2019 | DOI :10.36349/EASJHCS.2019.v01i06.015

Review Article

Comparative Perspective of Cyber Terrorism in India

Surendra Singh Baghel[1*] and Dr. D.C Upadhay[1]

[1]Barkatullah University, Bhopal (M.P.) - India

*Corresponding Author
Surendra Singh Baghel

Abstract: Almost all countries now enjoy internet access, and there are approximately more than twenty million internet hosts worldwide. E-commerce has a tremendous impact on copyright and other intellectual property rights (IPRs). The issues related to copyrights on digital content also lie unaddressed. From one perspective, the internet has been described as "the world's biggest copy machine." Generally, a trade mark can be owned by an individual, a company, or any sort of legal entity. When someone else tries to use that trademark without authorization, it could be considered an illegal dilution of the distinctive trademark. If someone uses a trademark in such a way as to dilute the distinctive quality of the mark or trade on the owner's reputation, the trademark owner may seek damages. In the cyberspace, domain name infringements are rampant. At times, people forget or ignore the legal and ethical values of their actions. Consequently, cyber wrongs in different forms are increasing day by day: cracking/hacking, e-mail spoofing, spamming/Denial of Services (DOS attacks), carding (making false ATM Debit and Credit cards), cheating and fraud, assault by threat, impersonation, intellectual property rights (IPR) infringements (software piracy, infringement of copyright, trademark, patents, domain names, designs and service mark violation, theft of computer source code, etc.), online gambling and other financial crimes including the use of networking sites and phone networking to attack the victim by sending bogus mails or messages through internet, forgery, URL hijacking or squatting (using the domain name of another person in bad faith), cyber vandalism (destroying or damaging the data when a network service is stopped or disrupted), virus transmission, internet time thefts, pornography, cyber terrorism etc-the list is endless. In traditional and online trading environments, consumers are entitled to have their privacy respected. While shopping on the internet; most people typically do not think about what is happening in the background. Customer information has to pass through several hands; and the safety and security of a customer's personal information lies within the hands of the business. Therefore, security and privacy of the information are a major concern. The present study primarily intends to address the pitfalls in the present legal system and to evolve a strategy to regulate cyber crimes in India.

Keywords: Cyber space, Cyber Crimes, internet, piracy.

INTRODUCTION

The growth of the e-commerce is indicative of the increasing receptiveness of the public but has also brought the issues that the legal system of the country has been faced with. Now internet has become a basic necessity for every household in most cities, the e-commerce industry has come a long way. The legal system has constantly tried to catch up especially with the enactment of the various rules under the IT Act to deal with a host of issues emerging from the use of internet. Moreover, the IPR issues in e-commerce transactions have taken a new form with users finding ways not only easily to duplicate material but also mislead other users. Though India has started dealing with it by enacting IT Act, 2000 but, it still lacks a lot as no specific legislation governs online transactions and IPR issues in India. The Information Technology Act, 2000 provides for the admissibility of electronic records and sets out offences and penalties for cybercrimes, etc. But, this is just an enabling statute to facilitate online transactions and thus has to be read in conjunction with the Contract Act in order to determine whether an online transaction constitutes a valid contract or not.

At times, people forget or do not consider the legal and ethical values of their actions. Consequently, cyber wrongs in different forms are increasing day by day: cracking/hacking, e- mail spoofing, spamming/Denial of Services (DOS attacks), carding

Quick Response Code

Journal homepage:
http://www.easpublisher.com/easjhcs/

Article History
Received: 05.12.2019
Accepted: 13.12.2019
Published: 27.12.2019

(making false ATM Debit and Credit cards), cheating and fraud, assault by threat, impersonation, intellectual property rights (IPR) infringements (software piracy, infringement of copyright, trademark, patents, domain names, designs and service mark violation, theft of computer source code, etc.), online gambling and other financial crimes including the use of networking sites and phone networking to attack the victim by sending bogus mails or messages through internet, forgery, URL hijacking or squatting (using the domain name of another person in bad faith), cyber vandalism (destroying or damaging the data when a network service is stopped or disrupted), virus transmission, internet time thefts, pornography, cyber terrorism etc- the list is endless. However, the issue of law on the internet is a complex one. Between the two all-or-nothing extremes lies a broad spectrum of possibilities (Abel, S. M. 1998).

In traditional and online trading environments, consumers are entitled to have their privacy respected. While shopping on the Internet; most people typically do not think about what is happening in the background. Customer information has to pass through several hands; and the safety and security of a customer's personal information lies within the hands of the business. Therefore, security and privacy of the information are a major concern. E-commerce has a tremendous impact on copyright and other intellectual property rights (IPRs) (Mitra, A. 2013). The issues related to copyrights on digital content also lie unaddressed. From one perspective, the Internet has been described as "the world's biggest copy machine (Singh, A. D. 2008)." Generally, a trademark can be owned by an individual, a company, or any sort of legal entity. When someone else tries to use that trademark without authorization, it could be considered an illegal dilution of the distinctive trademark. If someone uses a trademark in such a way as to dilute the distinctive quality of the mark or trade on the owner's reputation, the trademark owner may seek damages. In the cyberspace, domain name infringements are rampant.

In the international level, the UNCITRAL Model Law on Electronic Commerce (1996) was the first legislative attempt by the United Nations Commission on International Trade Law (Bains, M. S. 2003). The Model Law purports to enable and facilitate commerce conducted using electronic means by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce. In particular, it is intended to overcome obstacles arising from statutory provisions that may not be varied contractually by providing equal treatment to paper-based and electronic information. Such equal treatment is essential for enabling the use of paperless communication, thus fostering efficiency in international trade. The power of the Web to reach the world carries with it a variety of legal issues, often related to intellectual property concerns, privacy, decency, etc. Authorities seeking to apply their laws in traditional ways or to expand legal control over international links face many challenges due to the global nature of the Internet. Therefore, there is an urgent need for a comprehensive policy and an effective legal frame work to regulate cyber crimes. The present study primarily intends to address the pitfalls in the present legal system and to evolve a strategy to regulate cybercrimes in India.

Michael A Sinks argues that, (Barr, D. D. 2000) in land, sea, and air battles, military combatants can see the enemy coming, whether it's the whites of their eyes or a blip on a screen. International boundaries easily define when an aggressor threatens the sovereignty of a nation, giving the victim nation the right of jurisdiction, and there are specific international laws that address military operations in space. In addition, the international community has defined when an adversary's use of force threatens a nation's territorial integrity and political independence. However, the global nature of cyberspace and the speed of which victims can experience cyber attacks force nations to deal with the legal challenges associated with over-the-horizon military operations.

Cybercrime is the deadliest epidemic confronting our planet in this millennium. A cyber criminal can destroy websites and portals by hacking and planting viruses, carry out online frauds by transferring funds from one corner of the globe to another, gain access to highly confidential and sensitive information cause harassment by e-mail threats or obscene material, play tax frauds, indulge in cyber pornography involving children and commit innumerable other crimes on the internet. It is said that none is secure in the cyber world. People with intelligence have been grossly misusing this aspect of internet to perpetuate illegal acts in cyber space. The field of cyber crime is just emerging and new forms of criminal activities in cyber space are coming to the forefront with the passing of each new day. Cyber crimes may range from 'the merely annoying' to 'the catastrophic.' Gurmanpreet Kaur, Anand Pawar and Simranpreet Kaur conclude that the only possible step to make people aware of their rights and duties is to make the laws more stringent to keep a check on crimes (Moses, L. B. 2003).

Cyber crime, today, have increasingly emerged as major challenges for nations across the world. The fact that Internet has made geographical history has further facilitated cyber criminals to perpetuate their criminal designs and activities across networks. The transnational nature of cybercrimes has further complicated the challenges for national governments to regulate cyber criminal activities. As such, national governments are adopting their national legislations for regulating cyber crimes. India has come up with its own regulatory regime with aimed at cyber fraud and

cybercrimes. Pavan Duggal‟s book *Cyber Frauds, Cybercrimes & Law in India (*Ont: Captus Press. 2010*)* looks at the way of how Indian cyber law addresses cyber fraud and the various cybercrimes and quantum of punishments for it. The book and further looks at what are the challenges being faced by the Indian legal regime while regulating cybercrimes; and the deficiencies of the Indian approach in dealing with cybercrimes.

In his work (Chaudhury, A., & Kuilboer, J. P. 2001) of felt need round the globe- *Cyber Crime in India-A Comparative Study*, the experienced author has discussed the intricate problems that are being faced by the international community every moment and also their probable solutions. With advancement of technology the cyber criminals very often trespass, destroy or alter computer, computer system, computer programme, software, network and related devices. While dealing with this emerging subject the author has taken adequate care to incorporate the issues like classification, nature and elements of cyber crime, activities of the cyber hackers, cyber frauds, cyber pornography, online child pornography, cyber terrorism and so on.

Police Investigation Powers, Tactics and Techniques (Chitrangda. 2014)

Is a benchmark and best-practice model and regarded as the „Bible‟ for professional investigation in India. Anchoring himself firmly on the ever-contested space of Indian law and legal processes, and drawing substantive support from his rich and varied experience as a law enforcement officer in the police department, the author, has sought to fulfill the legitimate requirements of police officers, advocates, judicial officers, social activists, NGOs, gender activists and the general public. The author's utopian ideal that no innocent person should be punished and no offender should go unpunished is the dominant message of the book. The citation of more than 800 landmark judgments of various High Courts and the Supreme Court for the period 1965-2016 in the appropriate chapters is another outstanding feature of the book.

Cyber Crimes against Women in India10 reveals loopholes in the present laws and policies of the Indian legal system and what can be done to ensure safety in cyberspace. The book is a significant contribution to socio-legal research on online crimes targeting teenage girls and women. It shows how they become soft targets of trolling, online grooming, privacy infringement, bullying, pornography, sexual defamation, morphing and so on. The authors address various raging debates in the country such as how women can be protected from cybercrimes; what steps can be taken as prevention and as recourse to legal aid and how useful and accessible cyber laws are.

Banks are offering many services of which, the electronic mode is becoming popular amongst Banks and their customers. Presently, these are in the form of ATMs, credit & debit cards, online transactions, net banking, mobile banking, e-commerce, new payment systems etc. As more and more services of banks are offered in electronic mode, they must be aware of the risks due to possible misuses of new technology based services and various online channels. It has became important that the bankers, particularly who are dealing with I.T. and online channels, would be well versed with the various cyber crimes and frauds which may occur in offering these services. To safeguard the interest of the banks and their clients, a banker who is dealing in such services should have thorough knowledge and understanding about cyber crimes and how to mitigate a fraud and prevent eventualities in future. The book; *Cyber Crimes and Fraud Management* provide an overview of various types of cybercrimes and how to alleviate such crimes (Debarati, H., & Jaishankar. 2017).

Computer Internet and New Technology Laws (Goldsmith, E., & McGregor, S. L. 2000)

Is a comprehensive work that aptly highlights new laws, policies, cases, concepts, events and studies that have evolved cyber laws in the national and international spheres. It specially focuses on the development of laws in India including new bills and guidelines that were passed such as Electronic Delivery of Service Bill, 2013, the cabinet approval of the New Consumer Protection Bill 2015 and the new guidelines for the introduction of e-authentication technique using Aadhar-eKYC services. It also discusses land mark cases, including *Shreya Singhal v. UOI*, which struck down Section 66A of the IT Act, 2000 as unconstitutional and *Anwar v. P.K Basheer* which clarified the law on appreciation of electronic evidence in India. The book critically examines the emerging crimes such as trolling, sexting and revenge porn and new developments such as Net Neutrality that have impacted the cyber world. The work cover recent amendments and new Rules related to Protection of Children from Sexual Offences Act 2012, National Cyber Security Policy 2013, IPR policy, Guidelines for Foreign Direct Investment in India, Directives on Consumer Rights, Regulation on Data Protection Rules within European Union and more.

John Dickie outlines and analyses the legislative activity of the European Union in an area which is currently experiencing exponential growth in terms of both commercial activity and legal significance (Gurmanpreet, K. *et al*., 2012). He has taken great pain in incorporating the current, pending and proposed Internet-related law on contracts, copyright, data protection, commercial communications, financial services, electronic cash and electronic signatures; and submits that the European Union is in the process of displacing Member State autonomy in the regulation of the Internet. Within that frame, it is argued that there is a

lack of focus on the individual in the electronic marketplace and a lack of co-ordination between relevant legislative instruments.

Electronic Commerce:

The only casebook dealing with e-commerce, Electronic Commerce**, (**Dickie, J. 1999**)** utilizes problems to expound a transactional approach to electronic commerce. Ronald J. Mann attempts a hypothetical representation of a technology company. The work provides a detailed discussion on click-through contracts, cyber- squatting, web site development, software licensing and electronic payments.

At a time when there are still a number of voices calling for the Internet to remain a law-free zone, a whole bundle of conflicts have already emerged, many of which have found their way to lawyers and the courts in a substantial number of different jurisdictions. It surely now cannot be doubted that the Internet, like any other place in the world where people come together and follow their own interests, needs rules to be developed for the handling of such conflicts. Lawyers have already reacted and have created a new area of law--commonly called "law of the internet" or "cyber law." This area, however, is still far from being strictly defined. It touches on many existing areas of law, but at the same time it deals with a wholly new medium-- cyberspace--which itself is subject to constant change and development. Under these circumstances, it is not surprising that in a number of cases the predictions as to how this law will look at some selected moment in the future are vague and uncertain (Karnika, S. 2016).

In order to provide an overview of the most important legal issues of E-Commerce Gerald and **Borner (**Kenneth, C. *et al*., 1999**)** describe the regulatory framework in nine European countries (Belgium, France, Germany, Great Britain, Italy, Norway, Spain, Switzerland and Nether lands) and the United States of America. The country-specific contributions present an overview of the main questions and trends in E-Commerce Law, in particular with regard to the adoption of several EU Directives. An Indian author, (Lessig, L. 1999) in his work discusses various legal issues in electronic commerce and states how legislation in other countries has sought to solve them. It also discusses the beginning made by Information Technology Act, 2000 in India. There are many important issues which are critical for the success of e-commerce that have not been covered or properly addressed by IT Act. Dr Sumanjeet reveals that the present IT Act is weak on various fronts and in the absence of sound legal framework e-commerce cannot create a success story in India (Maher, D. W. 1997). Indian Government must appreciate that for safe and secure business environment on cyberspace, a sound legal framework is needed. His paper suggests that there is strong need to introduce separate laws for e-commerce in India. After having critically examined the Indian IT Act 2000 and IT (Amendment) Act 2008 in the light of e-commerce perspective to identify the present status of e-commerce laws in India, the author identifies various loopholes in the existing e-commerce laws in India; and suggests measures to protect the interests of Indian software industries, BPO sector and other stakeholders.

Information Technology Law and Practice- Cyber Laws

Laws Relating to E- Commerce (Michael, A.S. 2012) *captures* the essence of the Information Technology Act, 2000; discusses and analyses in great detail different aspects related to the subject and the challenges posed by information technology. Issues related to cyber-crime, virtual currency (bit-coin), Internet blocking, sexting, child pornography, surveillance, cyber terrorism, encryption, digital India, social media, cyber security have been discussed in the legal context. Further, considering the nature of the subject and the international perspective, it provides a comparative analysis of corresponding provisions in other jurisdictions. Hundreds of judgments, including that of Shreya Singhal, Aadhaar, Bazee, etc. have been interwoven seamlessly to underline the way judges have been weaving technology with judicial wisdom and coming out with judicial interpretation of various facets of technology.

BIBLIOGRAPHY

1. Abel, S. M. (1998). Trademark issues in cyberspace: The brave new frontier. *Mich. Telecomm. & Tech. L. Rev.*, *5*, 91.
2. Mitra, A. (2013). E-commerce in India-A Review. *International Journal of Marketing, Financial Services & Management Research*, *2*(2), 126-132.
3. Singh, A. D. (2008). *E-commerce in India: Assessments and Strategies for the Developing World*. LexisNexis Butterworths India.
4. Bains, M. S. (2003). Software, Sovereignty and the Internet: Circumventing Chaos Through TRIPs. *The Columbia Science and Technology Law Review*, *4*, 2.
5. Barr, D. D. (2000). The Need of a Broad Standard in Global E-Commerce. *The Internet Law Journal*, *28*.
6. Moses, L. B. (2003). Adapting the law to technological change: a comparison of common law and legislation. *UNSWLJ*, *26*, 394.
7. Ont: Captus Press. (20^{10}). Campbell, Legal Issues in Electronic Commerce (3rd edn. Concord,) Chatterjee Bivas, Cyber Contract (Legal Analysis) (Asia Law House, 2015).
8. Chaudhury, A., & Kuilboer, J. P. (2001). *E-business and E-commerce Infrastructure:*

Technologies Supporting the E-business Initiative. McGraw-Hill Higher Education.
9. Chitrangda. (2014). "E-commerce-Business & Legal Ethics," 2 International Journal of Scientific Research & Management, 565-572.
10. Dasgupta. (2009). Cyber Crime in India-A Comparative Study.
11. Debarati, H., & Jaishankar. (2017). Cyber Crimes against Women in India (Sage Publications, 2016) Prevention of Cyber Crimes and Fraud Management (*Macmillan Publishers India Private Limited; Second edition,)*
12. Goldsmith, E., & McGregor, S. L. (2000). E-commerce: consumer protection issues and implications for research and education. *Journal of Consumer Studies & Home Economics*, *24*(2), 124-127.
13. Gurmanpreet, K., Anand, P., & Simranpreet, K. (2012). Cyber Terrorism and Law (LAP Lambert Academic Publishing)
14. Dickie, J. (1999). *Internet and electronic commerce law in the European Union*. Bloomsbury Publishing.
15. Karnika, S. (2016). Computers, Internet and New Technology Laws-A Comprehensive Reference Work with Special Focus on Developments in India (Lexis Nexis; First edition)
16. Kenneth, C., Laudon, C., Guercio, T. (1999). E-commerce (Business Technology Society, 2014) Kostyu, Jennifer L, "Copyright Infringement on the Internet: *Determining the Liability of Internet Service Providers, 48 Catholic University Law Review.*
17. Lessig, L. (1999). The law of the horse: What cyber law might teach. *Harv. L. Rev.*, *113*, 501.
18. Maher, D. W. (1997). Trademark Law on the Internet-Will it Scale-The Challenge to Develop International Trademark Law. *J. Marshall J. Computer & Info. L.*, *16*, 3.
19. Michael, A.S. (2012). Cyber Warfare and International Law (Biblioscholar)
20. Miller, R. (2002). The Legal and E-Commerce Environment Today, (Thomson Learning)
21. Mik. (2011). the Unimportance of Being Electronic or - Popular Misconceptions about "Internet Contracting"" *19 Int J Law Info Tech 324*.
22. Mort, S.A. (1997). "The WTO, WIPO & the Internet: Confounding the Borders Copy Right Infringements in Cyberspace: The Need to Nurture International Legal Principles" *14 International Journal of the Computer, the Internet and Management.*
23. Pavan, D. (2013). Cyber Frauds, Cybercrimes & Law in India.
24. Ramappa, T. (2003). *Legal Issues in Electronic Commerce*. Macmillan India.
25. Ronald, J.M. (2011). Electronic Commerce (*Columbia University*)
26. Shoniregun, C.A., "Intellectual Property Rights of Multimedia".
27. Enriched Websites. (2002). " Communication of the ACM: *Ubiquity, 3(37), Oct 29.*
28. Jitender, K.M., & Sanjaya, C. (2019). CYBER SPACE- EVOLUTION & GROWTH. East African Scholars Journal of education, *Humanities and Literature, 2 (3), 2019, 170-190.*
29. Jitender, K.M., & Sanjaya, C. (2019). A BRIEF REVIEW ON CYBER CRIME -GROWTH AND EVOLUTION. *Pramana Research Journal, 9(3), 242.*
30. Jitender, K.M., & Sanjaya, C. (2018). POLICY CONSIDERATIONS IN INDIA AGAINST CYBER CRIME. *International Journal of Recent Scientific Research, 9(12)(A), December, 29811-29814.*
31. Jitender, K.M., & Sanjaya, C. (2018). THE CRIMINALS IN A CYBER ENVIRONMENT USING COMPUTER NETWORKS. *International Journal Of Current Innovation Research, 4(12) (A) , Dec, 1416-1422.*
32. Jitender, K.M., & Sanjaya, C. (2018). CYBER CRIMES- POLICY IN INDIA, *International Research Journal of Human Resources and Social Sciences, 5(4), April, 554-565.*
33. Spindler. (2002). Gerald and Börner, Fritjof, E-Commerce Law in Europe and the USA (Springer,)
34. Sumanjeet. (2010). "The State of E-commerce Laws in India: A Review of Information Technology Act," *52 International Journal of Law and Management 265-282*.
35. Toshiyuki, K., Christoph, G.P., & Harry, R. (2002). Selected Legal Issues of E-commerce (Kluwer Law International)
36. Vakul, S. (2016). Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce (*Universal Law Publishing, Fifth edition*)
37. Wigand. (2014). "Electronic Commerce: Definition, Theory, and Context" *9 International Journal of Electronic Commerce.*
38. WIPO. (2002). Intellectual Property on the Internet: A Survey of Issues (*Geneva: World Intellectual Property Organization)*
39. Yogendra, N.M. (2006). Internet Taxation and E-Retailing Law in the Global Context (2018) Zittrain, „The Generative Internet" *119 Harv L Rev 1974.*