Book Review: Cyber Crime in India – A Comparative Study by Dr. M. Dasgupta

Ranit Kumar Bose[*]

Abstract: This article is a review of "Cyber Crime in India – A Comparative Study" by Dr. M. Dasgupta and the book is a worthy addition to the existing research works on Cyber Crime and Criminals. Though the title of the book is named as "Cyber Crime in India", it also consists galore of international perspectives, incidents, and case judgments. The book was written and published in 2009 but the visualization of the author of the book on the various aspects of cyber-crime and its impacts on society is really praiseworthy and still applicable in present days. Moreover, how the issue relating to cybercrime can be probably remedied is very lucidly explained. The book is précised, comprehensive, and reader-friendly establishing its value as elaborative and illustrative research work on cybercrime in India. The article is mainly segmented into three parts excluding the introductory part, such as: General Review, Criticisms, and Concluding Remarks.

Keywords: *Cyber Crime, Internet.*

1. Introduction

> *"I know I will have to go, yet as long as I live, I shall stake my life to clear the world's refuse,*
> *I shall make this world habitable for the child, to the newborn, this is my firm promise."*

The main part of the book is concluded with this poem of Late Sukanta Bhattacharya intending to draw the honest purpose and commitment to combat terrorism and other cybercrimes.

No doubt the internet is a boon for this era but with the prospective emergence internet system, cyber-related crimes and criminals have become a materializing threat to society. In the broad sense, cybercrime is a criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity that mainly consists of unauthorized access to computer systems data alteration, data destruction, and theft of

[*] LL.M. Candidate, Department of Law, University of Calcutta

intellectual property. Moreover, in the context of national security, it may involve terrorist activism, traditional espionage, information warfare, and other related activities.[12]

The book “Cyber Crime in India: A Comparative Study” is mainly a compact analysis of multifarious perspectives of cybercrime and elaborative research work on the effect and role of the Information Technology Act 2000 in purposive to regulate and prevent cyber-related offenses in India. Moreover, the book covers a major portion of international aspects of cybercrime along with an elaborative historical background. The book also provides a plethora of international and Indian judgments on various incidents of cyber-related crime both at the national and international levels. However, the author has given her priority to researching international judgments and incidents mainly in the American and European countries which may be reasoned as the book was written in 2009 and the nation did not immensely experience cybercrime.

Significantly, the author has also briefly described the theories of criminal behavior from criminological and penological perspectives and beautifully drawn the relation with a crime in cyberspace. Thus, the book is a very reader-friendly and handy guide and contained a plethora of unknown information and innovative scientific research works which are very helpful for the students, advocates, judges, researchers, and teachers. This book review has been segmented into three major parts excluding this introductory segment such as: general review where a general review of the book along with characterization has been tried to put down, criticisms where some portion of the book has been critiqued and it has been attempted to provide critical analysis of the literature, and at the penultimate part, it is the conclusion where the final remarks and sum up of the book are drawn.

2. General Review

No doubt, in these present days, cybercrime is the greatest concern for individuals, various bodies, and the government too. Innovation of new technologies and phenomenal growth and rapid adaptation of the internet though make daily life easier, but it also enhances the opportunities for cybercrime. Moreover, the pattern of crime is changing due to the worldwide dimensions and limitless nature and new, mutable and innovative responses to

[12] V. Karamchand Gandhi, ‘An Overview Study on Cyber Crimes in Internet’ (2012) 2(1) Journal of Information Engineering and Applications 1

the cyber world.[13] Thus, it is a challenging procedure to accrue all the data and analysis in one research or book. Moreover, the flexible and transformational social change and behavioral approach are also a great concern and challenge for the legal researcher not only in the arena of cyber law but also in every field of law. Thus, the contribution of the author of the book is deserved the best compliment and will be helpful in litigation and the progression of academic research.

The book is mainly divided into parts such as firstly, the main part and secondly appendices. The main part is characterized by six chapters such as:

- Cyber Crime – A General Perspective
- History of Cyber Crime
- Cyber Hacking
- Cyber Fraud
- Cyber Pornography
- Cyber Terrorism

The first chapter mainly caters to the introduction of cybercrime where the author observed the distinction between traditional laws and cyber laws as traditional laws are not adequate in cyberspace always. Thus it needs separate laws along from the traditional cyber world. The major challenges faced in the contemporary legal system are that the cyberspace or cyber world does not have any specific limitations or boundaries and individuals have the absolute freedom to access this world.[14] Moreover, the online transmission of e-data, e-commencing, mobile communication, and e-governance has become so popular not only among educated individuals but also among every section of society. Thus, sans having due preventive measures, the high demand for technology and internet facilities in using amounts to the various e-crimes or cyber-crimes like software piracy, pornography, hacking, fraud, etc. which are sinking gradually around the world.[15] In this connection, the author put her view on the reason behind to control cyber-crime why so difficult such as – the victim's vulnerability and unawareness, lack of adequate legislation, lack of

[13] Neelesh Jain & Vibhash Shrivastava, 'Cyber Crime Changing Everything – An Empirical Study' (2014) 1(4) IJCA

[14] M. Dasgupta, *Cyber Crime in India: A Comparative Study* (1st ed., Eastern Law House 2009) 1

[15] *Ibid*

knowledge about cybercrime, lack of expert law enforcement agencies with infrastructural support, lack of expert adjudicating system, etc.[16]

The author briefly discusses the initiative taken by the European Community as being a signatory to the WTO agreement on telecommunication and the view of the United Nation by adopting the Model Law on e-Commerce (the General Assembly of UN by Resolution A/RES/51/162). Moreover, UN Model (UNCITRAL) Law accorded that there must be an equal legal treatment for users of electronic communication and paper-based manual communication. India also adopted this Model Law and enacted the Information Technology Act in the year 2000 within a very short time to fill the certain lacuna. The Act was amended twice in the year 2005 and 2006 but not enforced (finally in the year 2008 it was enacted). In this context, the author observed that:

> "*In a developing country like India, communication and Information Technologies are the keystone for development and progress. In the recent past, the concept was that government should stay away from electronic governance. But gradually internet has become mainstream and previous concepts have become inadequate in this dynamic society. Some of the problems are very complex such as jurisdiction over Internet regulation to prevent and control hacking, cyber fraud, cyber theft, unauthorized access, mischievous activities in cyberspace and flowing worm, viruses etc.*"[17]

Moreover, the author has discussed various conferences on Computer Freedom and Privacy held in several countries regarding encryption policy, censorship, privacy, online democracy, commercialization of cyberspace, IP law and other related laws. Moreover, the author also mentioned the science fiction author W. Gibson's novel 'Nuromancer'[18] in the year 1982 where the term 'Cyberspace' was coined and described as an environment where computer hackers operate, the activity of hacking securing unauthorized access to the computer and computer system.**[19]**

Significantly, the author has described the nature of crime propounded by several jurists like Blackstone, Huda, Sutherland, Austin etc and bridged the connection with cybercrime. To define the nature of cybercrime author put the opinion of Prof. S.T Viswanathan on three definitions of cybercrime such as:

[16] *Ibid* at 2

[17] Dasgupta (n 3)

[18] William Gibson, *Nuromancer* (Ace 1984)

[19] Dasgupta (n 3)

Any illegal activity in which a computer is the tool or object of the crime that is a crime, the means or purpose of which is to influence the function of a computer.

Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain.

Computer abuse is considered any illegal, unethical or unauthorized behaviour relating to the automatic processing and transmission of data.**[20]**

Moreover, to describe the elements of cybercrime and criminal liability author has very beautifully evaluated and explained the maxim '*actus non facit reum nisi mens sit rea*' and successfully proved that in the case of cybercrime, '*actus reus*' and '*mens rea*' are the essential elements. Significantly, the author put the examples too for a better understanding of how they are established as the essential elements and co-related in the commission of cybercrime[21] and the author classifies cybercrimes into eight categories, those are:

- Unauthorized access
- Cyber fraud
- Cracking
- Hacking
- Cybertheft
- Flowing of viruses
- Cyber Pornography
- Cyber terrorism

Remarkably, the author has laid down the theories of criminal behavior in cyberspace from the criminal perspective where she has put down the criminological and penological perspectives and most significantly, analysis the Differential Association theory by Sutherland in contemporary hi-tech society. She also mentioned Blackburn's theory of peer pressure and peer attitudes and Hollin's theory of Psychology and Crime. Moreover, she also discusses the Differential Reinforcement theory and Social Learning theory briefly in this context.[22]

[20] *Ibid*; *See also*, S.T. Viswanathan, *The Indian Cyber Laws with Cyber Glossary* (Bharat Law House 2001) 81

[21] Dasgupta (n 3) at 10

[22] *Ibid* at 20-21

The second chapter deals with the 'History of Cyber Crime' where the author has very elaborately explained the evaluation of computers, evaluation of cybercrime before the 1960s (first phase), in the 1960s (second phase), in the 1970s (third phase), in 1980s (fourth phase) and 1990s (fifth phase). Moreover, the author has explained various foreign case judgments such as the Boxes Whistle case (1970), Thompson case (1984), Gold case (1988), Czubinski case (1997), etc. Besides these, evaluation of cyber pornography, computer intrusion, virus, etc. has elaborately been discussed. Moreover, cybercrime in the year 2000 has also been mentioned where various international and Indian incidents of crimes are discussed including cricketer Hansie Cronje case (2000), Claude R. Carpenter Case (2001), etc.[23]

The third chapter of the book enumerates cyber hacking where the author provides various definitions of Cyber hacking along with the nature and culture of hacking. Significantly, the author has laid down the possible ways of hacking such as impersonation, cracking passwords, reinstallation of the system, damaging the security, etc. Moreover, the hacker's culture and behavior have also been briefly discussed.

Thereafter, the international initiatives (including the European Union and the Global Internet Liberty Campaign) to prevent and control have been enumerated, and cyber hacking in the UK, USA, and India with their legislative, judicial approach, and socio-legal impact have been lucidly observed. Significantly, the chapter culminated with a conclusion and suggestive measures where the author laid down her suggestion in purposive to prevent hacking which is helpful for future research work.[24]

Chapter four caters to cyber fraud also the possible mode of cyber fraud such as, victim's excitement, false representation, mistakes under urgency, lottery fraud, email fraud, etc. have been enumerated and Cyber hacking, the international perspective to combat cyber fraud (including the role of EU and UN), cyber fraud in the UK, USA, and India have been observed with a plethora of incidents and case judgment which are impressive and praiseworthy. Significantly, the concluding remarks and suggestions evaluate the expertise of the author in legal research.[25]

[23] *Ibid* at 27-50

[24] Dasgupta (n 3) at 51-99

[25] Dasgupta (n 3) at 100-133

Chapter five speaks about cyber pornography, where the author briefly discusses Brian Tod Schellenberg's case from an international perspective and analysis the role of UNESCO in preventing and controlling computer-related crime. Moreover, cyber pornography in the UK, and the USA has been observed with the legislative and judicial approaches. To discuss the Indian scenario, the author took the help Constitution of India, where Article 19(2) provides that in the interest of decency or morality, reasonable restrictions may be imposed by law upon freedom. Moreover, Article 21, 19(1)(a) has also been discussed with a remedial approach under articles 32 and 226 of the Constitution.

Besides this to discuss the legislative approach the author briefly discusses the various provision of the Indian Penal Code and Information Technology Act beautifully. Moreover, the author also mentions various judicial cases like Shaw v. Director of Public Prosecutor[26], Sukanto Halder v. State of WB[27], K.A. Abbas v. Union of India[28] to explain the judicial response before the Information Technology Act 2000 in India. In the end, it ends with a conclusion and suggestion where the author demands more teeth to the law to cope with this issue.[29]

Chapter six deals with cyber terrorism which includes national security, modes of cyber terrorism, evaluation, international perspectives, US and UK initiatives to prevent cyber terrorism, and finally the preventive measures are taken by India to control cyber terrorism. On the brink, the author has viewed her opinion in concluding remarks and suggestions to strengthen the national and world security standards.[30]

On the verge, the book ends with appendices such as:

- The Information Technology Act, 2000
- The Information Technology (Amendment) Act, 2008
- The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000
- The Information Technology (Certifying Authorities) Rules, 2000
- The Information Technology (Certifying Authorities) (Amendment) Rules, 2003
- The Computer Fraud and Abuse Act, 1986 (US)

[26] *Shaw v Director of Public Prosecutor* [1961] 2 All ER 44 B
[27] *Sukanto Halder v State of WB* AIR 1952 Cal 214
[28] *K.A. Abbas v Union of India* (1970), AIR 481
[29] Dasgupta (n 3) 134-186
[30] *Ibid* at 187-226

- The Computer Misuse Act, 1990 (c. 18)
- European Committee on Crime Problems (CDPC)

3. Criticisms

No doubt, the book is a valuable addition for academic research and litigation purpose but still the book could have been improved. In the first chapter though the author has provided briefly the theories of criminal behavior in a cybercrime perspective, it requires more elaborative discussion thus the academician can better co-relate the cybercrime and criminal behavioral approach. Moreover, the history of cybercrimes (chapter two) is silent about the Indian perspectives of origin and evaluation of cybercrime.

Significantly, the book is unmentioned the Yahoo v. Akash Arora[31] case which was considered the first landmark case on cybersquatting in India decided by the Delhi High Court in the year 1999.[32]

Moreover, the book is unresponsive to the recent and updated judgments of the Supreme Court and other High Courts in India and that may be reasoned as the book was written and published in 2009 and that was the *ab ovo* scenario of cybercrime in India. Moreover, the legislative and judicial approaches were not very strong at that time. Thus, the book requires and it is the high demand for publishing a second updated edition with new and innovative research work by the author.

4. Conclusion

From the above analysis, it is clear that the book is no doubt very helpful both for academic and litigation purposes. The book is so informative and rendezvous of vast research work. The suggestion drawn by the author at the end of every chapter is practical and appreciable and helpful for future research and significantly in determining rules and regulations for preventive purposes. Moreover, the international perspective of every crime and initiative to prevent these crimes is very educative and the Indian perspective along with the socio-legal impact of cybercrime also very helpful to understand the Indian scenario. Due to the

[31] *Yahoo v Akash Arora* (1999) IIAD Delhi 229

[32] Varsha, 'An Analysis on Cyber Crime in India' (*Legal Service India*) <https://www.legalserviceindia.com/legal/article-797-an-analysis-on-cyber-crime-in-india.html#:~:text=In%201992%2C%20the%20first%20cyber,Akash%20Arora> accessed 23 March 2022

lack of updated case laws and incidents, the book is highly required in its second edition. On the verge, it prospects that every reader who goes through Dr. M. Dasgupta will beprospered with knowledge and be inspired by her research work.