Name of the Scholar : Nishesh Sharma

Name of the Supervisor : Dr. S.Z. Amani

Name of the Faculty : Faculty of Law, Jamia Millia Islamia, New Delhi

Title of the Ph.D. : ***Cyber Forensics In India : A Legal Perspective***

Abstract

Legal perspective of cyber forensics in India invariably comes across multiples of case laws, statutes, and constitutional provisions on cyber crimes and cyber forensic procedures, all compendiously known as cyber law required to detect such cyber crimes which occur almost daily on the social electronic media, and which affect the computer devices and computer networks as well as the people and organizations in our society using such devices and computer network, all compendiously known as cyberspace. It also encounters with cyber terrorism, and jurisdiction issues regarding online disputes and the admissibility of cyber forensic evidence in the court of law, including foreign courts. Today various measures are adopted which are called Cyber Forensic techniques to identify, detect, collect and analyze electronic evidence admissible in the court of law to deal with the ugly situations arising from the incidence of cyber crimes.

India is facing a number of problems from various kinds of cyber crimes for example, fraud schemes, phishing scams, data mining and cyber obscenity etc. As a response to the increasing cyber crime and cyber terrorism in particular, the field of cyber forensics has emerged. “Cyber Forensics In India : A Legal Perspective” is a study of the laws dealing with cyber crimes in India at present. These laws have their basis in the precepts of the statute i.e. Information Technology Act, 2000 enacted by the legislature, and the procedures and practices developed by various government agencies such as National Cyber Security Coordinator (MCSC), Research and Analysis Wing (RAW), Computer Emergency Response Team (CERT-In) etc, having the responsibility of following the cyber forensic investigation procedures, electronic intelligence gathering operations, counter-surveillance operations, and of administering the cyber laws. It is also a study of the government policies with regard to cyber crimes and the steps taken by various authorities to implement those policies to counter cyber crimes.

Cyber crimes are punishable under various statutes besides IT Act, 2000. For example under Sections 22, 23, 33, 44, 96, 97, 268, 378, 425 of Indian Penal Code, 1860. Besides, Cyber crimes are punishable under National Investigation Agency Act, 2008, and also punishable under Section 15 of Unlawful Activities (Prevention) Amendment Act, 2008 etc. Different law enforcement agencies work in cooperation and coordination with each other to stop cyber crimes and to implement the Information Technology Act. What the Police, Cyber Crime Cells, Intelligence Bureau, Research and Analysis Wing, and National Technical Research Organization etc do is linked to the Courts through the analysis of the gathered electronic evidence based cyber forensics.

The significance of the study is to understand such conditions in society in which there are strong cyber laws, and there is protection to the online rights of the individuals in order to give sustenance to the Rule of Law

and a meaning and significance to the idea of Justice. The backbone of the research study is the Information Technology Act, 2000 along with other relevant legal enactments and judicial verdicts governing the cyber forensic issues. Information Technology Act, 2000 is one of the important statutes in India to tackle cyber crime having a bearing on cyber forensic matters and issues. Obviously to everybody understanding it has its basis in the Constitution and therefore reflects the idea which the people of India have with regard to their life, liberty, equality, privacy, religion and property in relation to each other and in relation to the State. Online hate speeches, state sponsored surveillance of individuals, violations of right to privacy and freedom of speech, etc need to be curbed but any improper method adopted to curb cyber crime would not only be violative of the principles of the Constitution but would shake up the very foundation of the system of justice. During the course of study the hypothesis i.e. Law and policies relating to the cyber forensics in India are inadequate to control the cyber crimes, was positively proved.

The study expounded the concept of cyber forensics investigations and examinations and underlined the basic features of the analysis and collection of electronic evidence in India. The Research is useful to the professionals who have the responsibility of dealing with cyber crime cases in the courts and other institutions. The study discusses the cyber forensics, social cyber media and cyber crimes and also endeavors to discuss the governance aspects such as guidelines and framework of cyber forensics. An empirical study of the threat of cyberterrorism presents the possible threats brought about by cyberterrorism. The study also highlights the importance of the jurisdictional aspects of cyber forensics to make the cyber forensic evidence admissible by analyzing the United States, European, Australian and Indian approaches to cross-border cyber crime cases to be dealt under the territorial jurisdiction of the country.

The study concludes that over the years social electronic media websites have become a powerful instrument in ensuring democratic process by increasing transparency in the conduct, access to information, and for facilitating active citizen participation in building democratic Societies. But at the same time cyber crimes have increased on the social networking sites, hence the role of Cyber Forensics to identify, detect and adduce evidence in the cases of fraud, misinformation, and cyber crimes on social networking sites.

In the study, certain suggestions have been incorporated such as there is a need for consistent, coherent definition of social media and also to bring in data protection laws in relation to social media applications. Also certain contents which can be termed to be unacceptable need to be censored. Besides, the social networking site should be brought within the umbrella of Indian legislations and there server installation in India is needed. There must be international coordination and cooperation in fighting crimes over social media as well as training of the investigation agency and the judicial members is much required.