Chapter 1

Introduction

1.1 Cyberspace

The Information and Communication Revolution (ICR) has overtaken the world, demolishing economic barriers and political boundaries and challenging the established laws of even the industrialised world\(^1\). ICR has brought its own set of laws regulating not only business and commercial activity but also the governance of postindustrial society. ICR has brought into existence a virtual space called as Cyberspace which is evolving rapidly into a highly dynamic space, one that is supportive of varied transactions and interactions. As the ICR affected only certain parts of the world, the legal systems of the so called developing countries could not, as yet, equip themselves to the challenges of ICR.\(^2\).

Nature and Salient feature of Cyberspace

The cyberspace has been described by The Supreme Court of United States of America (US) in a decided case which explains it as follows:\(^3\)

“Anyone with access to the internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorise precisely. But, as presently constituted, those most relevant to this case are electronic mail ("e-mail"), automatic mailing services ("mail explodes", some time referred to as ("list servs"), "newsgroups", "chat rooms", and the "world wide web". All these methods can be used to transmit text; most can transmit sound, pictures and moving

\(^3\) ACLU vs Reno,(1997) 521 US 844.
video images. Taken together, these tools constitute a unique medium known to users as, “cyberspace”-located in no particular geographical location but available to any one in the world, with access to the internet.”

Thus the salient features of cyberspace are:-

i) Any one in real world can have access to cyberspace through access to the internet.

ii) It consists of entire virtual world connected through e-mails, mailing list services, newsgroups using computer and internet.

iii) The speed is tremendous and reach is unlimited.

iv) The cost of communicating, storing, retrieving and processing data in cyberspace is very less. Fewer resources are needed in cyberspace.

v) It’s very easy to disguise one’s identity in cyberspace.

vi) It has no particular boundaries

vii) Cyberspace and real world impact each other.

viii) The cyberspace is expanding day by day.

**Cyberspace and the Indian Society**

Cyberspace being a social phenomenon is touching every arena of modern society. It is expanding throughout India and challenging established institutions and practices in a manner difficult even to comprehend. With rise in cyberspace usage, India has also witnessed a dramatic rise in the number of crimes in cyberspace. According to the report published by the globally reputed internet security company Symantec entitled, “Symantec Global Internet Security Threat Report Trends of 2009” India ranked the fifth highest world wide in 2009 for

---

malicious activity behind only US, China, Brazil and Germany. The annual reports of Computer Emergency Response Team (CERT) a security department under the Ministry of Communication and Information Technology, also reveals a dramatic increase in cyber crime in India\(^5\). Nevertheless, India is considered slow in developing corrective measures in the event of web attack and has failed to come up with an aggressive strategy to counter the attacks.

**Dilemma in regulation of Cyberspace**

The systems of socio-economic organization and political governance are undergoing unprecedented changes in cyberspace compelling Governments to review the laws relating to management of knowledge in society. Most developing countries of the world have to make a quantum jump in law-making if they want to develop capacities to protect national interests and to avoid exploitation by those who own technology—the limits of which are still unknown. This is the dilemma that India faces today by the advent of cyberspace, Information Highway and Cyberspace\(^6\). On one side are the cyberspace ‘unexceptionalists’ who argue in various contexts that the online medium did not significantly alter the legal framework to be applied. On the other hand cyberspace ‘exceptionalists’ argue that the medium itself created radically new problems requiring new analytical work to be done for its regulation\(^7\). Cyberspace is unconstrained by geographic boundaries, so like international trade, it cannot be effectively governed by geographically defined legal systems. Hence, there is a growing interest in the identification of potential solutions to the uncertainties that arise from online relationships and networks\(^8\).

\(^5\)A.Vishwanathan, Cyber Terrorism, Cyber Law, Indian and International Perspectives, 2-6 (2012).
1.2 Regulation of Cyberspace

The nature of the regulatory environment is such that regulation surrounds and controls our actions from the moment we are born to when we die. Some areas of our lives are clearly and noticeably regulated, often for our own protection or for the protection of others. All aspects of our everyday activities such as walking to work or shopping in a supermarket are equally closely regulated but in a less formal manner. Efforts are made to identify and evaluate macro-regulatory modalities which may be used by regulators to control patterns of behaviour within complex systems.

In Robert Baldwin and Martin Cave’s book *Understanding Regulation*, the authors outline eight (alternative) regulatory strategies: (1) command and control, (2) self-regulation, (3) incentives, (4) market-harnessing controls, (5) disclosure, (6) direct action, (7) rights and liabilities laws, and (8) public compensation. The authors describe these eight strategies as the application of the ‘basic capacities or resources that governments possess and which can be used to influence industrial, economic or social activity. Thus government may (a) use legal authority and the command of law to pursue policy objectives, or it may (b) deploy wealth through contracts, loans, grants, subsidies or other incentives to influence conduct, or (c) harness markets by channeling competitive forces to particular ends, or (d) deploy information strategically, or (e) act directly by taking physical action, or (f) confer protection to create incentives.

In attempting to provide a model which simplifies the variety of regulatory strategies Thatcher models suggests four families of regulatory interpretation: (1) classical economics, where regulation is an interference in the market that may be

---

10 Ibid
necessary, (2) political economy, where regulation is inherent to society, and is
used by the state to ensure that the market functions, (3) political science and law,
where regulation steers public activity and is concerned with controls over private
activity, and (4) sociological, where regulation is informational norms that guide
behaviour. An attempt to extend the traditional model of regulatory analysis into
Cyberspace was made by Lawrence Lessig in his extended essay Code and Other
Laws of Cyberspace. In this Lessig seeks to identify four ‘modalities of regulation’:
(1) law (2) market, 3) architecture and (4) norms which may be used individually
or collectively either directly or indirectly by regulators.\(^1\)

Cyberspace is a socially disruptive technology. Cyberspace, with its uniquely malleable environment and its stratified or layered structure is a particularly complex regulatory environment, meaning that mapping or forecasting regulatory settlements within Cyberspace is especially difficult. Any change at any point in the regulatory web can have immeasurable repercussions.\(^2\) Regulation within the complex, malleable, layered environment of Cyberspace is considerably more complex to model than regulation within physical space. India is amongst few of the countries in the world which have any legal framework for e-commerce and e-governance. Cyber law in India is incorporated in the form of Information Technology Act, 2000 (IT Act) and rules enacted under the Act.\(^3\) The IT Act, 2000 chiefly covers: E-commerce in India, (b) E-governance in India, (c) Cyber contraventions, (d) Cyber crimes, etc.

The IT Act is a comprehensive piece of legislation which aims at policing some of the activities over the Internet. However, the working and implementation of this law will depend greatly on the rules and regulations that will be formed by

---

\(^{1}\) Ibid.
\(^{2}\) Ibid.
\(^{3}\) The Information Technology Act, 2000 (21 of 2000).
the Government and other authorities constituted under the Act. The Act is only a skeletal figure, while it is the rules and regulations that will form the fleshy content. This Act is not the end but only a beginning to a plethora of legislation that still needs to be formed. At the same time, Indian law must be consonant with international standards that are prescribed and that may be prescribed in the future. This is essential for effective regulation of this boundless world.

Further to save ourselves from emerging problems of unregulated cyber space regulation only with the existing legal framework would not suffice. There is need to explore multifaceted approach involving architectural, social and legal measures for the regulation of cyberspace in India.

1.3 Research Hypothesis:

Unregulated cyber space is a major threat to national security and economy. It is heading the society towards a social damage. It is clear that existing control of cyber space does not sufficiently respond to the needs of society, legal professionals, and the nation at large. There is need to appreciate law as itself a discursive system that is both the product and producer of culture. Emphasis is to be placed on other forms of regulation such as social regulation and architectural governance that operate on the margins and boundaries of formal legal institutions.

Law is a tool for social engineering and social control, it should be studied in the social context. This means integrating law subjects with social and behavioral sciences. This would enable the lawyer to solve problems in socially acceptable ways and assist in developing public policies appropriate to social needs. In short, when it is the issue of controlling cyber space, modern law has to play a balancing role between stability and change, human rights and public interest.
Chapter 1

Introduction

To formulate the agenda for reforming law relating to control cyber space, it is crucial to identify its objectives in the context of needs and aspirations in general, and in terms of the expectations of society in particular. With these in mind, the present work was proposed to examine the nature and scope of social, architectural and legal regulation of cyber space and identify its strengths, weaknesses, and areas in need of reform. In addressing the reform needs, several options were explored given the context and constraints in the country. These and related issues were the concerns of this project.

1.4 Research Methodology:

The cyber space has provided tools to steal with impunity, control and manipulate the thoughts and movement of millions, holding an entire society hostage. It is cutting across all barrier of region, religion, caste, social & financial status. The vulnerability of Indian society in view of unregulated cyber space is still not sufficiently realized. Need was felt to consider the response of law and society and to draw conclusions as to consistency of approach towards regulation of cyberspace.

The present research work required both theoretical and empirical study. The theoretical work dealt with the literature survey relating to cyber regulation. A comprehensive literature search about the research topic was carried out. For this purpose databases, and other reference sources like bibliographies, online information resources, conference proceedings, library journals, newspapers, etc. were scanned to collect relevant literature. The empirical work comprised of the questionnaires, data collection in order to bring out the actual factors and forces regulating cyber space.
Chapter 1

Introduction

Universe of Study:

The empirical study was conducted in Chandigarh as it is a leading centre of cyber and legal activities. Chandigarh has been adjudged as a leader in the latest report on e-Readiness of the States and UTs in India. This report was recently released by the Department of Information Technology, Government of India, after conducting a survey in association with the National Council of Applied Economic Research (NCAER). It has been ranked fifth in the latest e-readiness rankings after Karnataka, Tamil Nadu, Andhra Pradesh and Maharashtra. The e-Readiness index of an Indian state/UT reflects its capacity to participate in the global networked economy. Chandigarh is the only Union Territory (UT) amongst the “leaders” and only sole representative of the Northern states in the “leaders” category. Its performance has been considered outstanding in the Environment sub-index, which measures the degree of conduciveness of the environment, that a state /UT provides for the deployment an use of Information and Communication Technology (ICT). Similarly, the Chandigarh has been ranked as a leader in the usage sub-index that measures the degree of utilization of ICT by individuals, businesses and the Government.\(^{14}\)

Thus the Chandigarh represents a true picture of evolving Information and Communication Revolution in Indian society. Being capital of two states and having Punjab and Haryana High Court it is a leading centre of legal activities. It represents a true picture of evolving Indian society, having a no. of educational institutions it is a hub of IT professionals, social and legal experts, thus providing varied factors leading to a common end.

\(^{14}\)Hindustan Times, March 03, 2007.
1.5 Plan of Study:

The study has been planned and conducted as discussed and described in following chapters as enumerated below:-

Chapter 1 – Introduction

Chapter 2 – Cyber space and its implications

Chapter 3 – Policing Cyber space

Chapter 4 – Architectural measures to regulate Cyber space

Chapter 5 – Social measures to regulate Cyber space

Chapter 6 – Legal measures to regulate Cyber space

Chapter 7 – Cyber law in India

Chapter 8 - Empirical Study

Chapter 9 – Conclusion and Suggestions

1.6 Cyber space and its implications

The World Wide Web and the Internet are rapidly expanding spaces, of great economic and social significance, which offer an opportunity to study many phenomena, often previously inaccessible, on an unprecedented scale and resolution with relative ease. It has been and continues to be a powerful engine for economic and social development. It provides tools that accelerate growth and enhance productivity. The Cyberspace can be harnessed to improve living standards worldwide and for achieving poverty eradication. Therefore the Chapter 1 explored the definition of term cyberspace and its implications in the field of Information, communication, Commerce, Education, Health, Social Implications, governance, etc.

Chapter 1

Introduction

1.7 Policing Cyber space

The cyberspace is a double edge sword, which can be used for destructive as well as constructive work. Although cyberspace has enhanced the efficiency, it has also brought about new vulnerabilities and challenges, thus necessitating its need for policing\(^{16}\). Thus this chapter describes about the characteristics which necessitate its policing in the field of Information, Data, Communication, Commerce, Education, Healthcare, Social problems, Crime. Further few case laws were described which gives a glimpse of need for policing cyberspace in India.

1.8 Architectural measures to regulate Cyber space

For cyberspace to serve as an engine for development, it is absolutely critical that an effective regulatory framework is in place; such a framework will enable an economy to fully capture the benefits of the cyberspace. Cyberspace is architecture first. Cyberspace encompasses today a large number of architectures and applications. From the architecture point of view, it contains small PCs and large mainframes or local networks and long-haul networks. It is a platform that gets designed. It is constituted by a set of code – by software and hardware that make cyberspace as it is. This code imbeds certain values; it enables certain practices; it sets the terms on which life in cyberspace is lived, as crucially as the laws of nature set the terms on which life in real space is lived. Developments in the architecture of the internet are spurring changes that make the cyberspace easier to control. Some architectures of cyberspace are more regulable than others; some architectures enable better control than others. Therefore, whether a part of cyberspace—or the Internet generally—can be regulated turns on the nature of its code. Its architecture will affect whether behavior can be controlled. The networks

\(^{16}\text{Ibid.}\)
thus differ in the extent to which they make behavior within each network regulable\textsuperscript{17}. Thus this chapter explored many branches of architectural regulation of cyberspace based on the secondary data search.

1.9 Social measures to regulate Cyber space

As in all other modes of social interaction, conduct can be regulated by social norms and conventions in significant ways. While certain activities or kinds of conduct online may not be specifically prohibited by the code architecture of the internet, or expressly prohibited by applicable law, nevertheless these activities or conduct will be invisibly regulated by the inherent standards of the community, in this case the internet users. And just as certain patterns of conduct will cause an individual to be ostracized from our real world society, so too certain actions will be censored or self-regulated by the norms of whatever community one chooses to associate with on the internet. Rules can be thought of as behavioral patterns that individuals expect each other to follow. The rules one individual is expected to follow influence the choices made by other individuals: like prices, rules coordinate and motivate interdependent behavior. A subset of rules, generally do not require explicit codification or backing by coercive threats to induce recognition, because they are widely “shared values” (voluntary adopted by individuals in their interactions with an identifiable (but perhaps changing) group of other individuals. As such interactions evolve and change, these “norms” or “customs” also spontaneously evolve\textsuperscript{18}.

Therefore this chapter explained various modes of social regulation such as by means of Education, by dissemination of adequate information, by means of

\textsuperscript{17}Ibid.
\textsuperscript{18}Ibid.
Introduction

Ethics, by peer groups, by Alternative dispute resolution, by Public, by Dissemination of Good Practice, by self-determination and self-regulation, by Co-regulation, by religion through Cameralism, through taskforce and also describes international perspectives in this regard.

1.10 Legal measures to regulate Cyber space

Cyberspace comes within the ambit of Cyber law. Cyber law is a generic term which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Cyber law encompasses a wide variety of legal issues related to use of communications technology. This chapter provides details regarding national as well as international measures available for the regulation of underlying issues in legal regulation of cyberspace.

1.11 Cyber law in India

India is amongst few of the countries in the world which have any legal framework for e-commerce and e-governance. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

The Preamble to the Act states that it aims at providing legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information and aims at facilitating electronic filing of documents with the Government agencies.

The IT Act is a comprehensive piece of legislation which aims at policing some of the activities in the cyberspace. The fundamental approach of the Act is
towards validating and legalizing electronic and on-line transactions so as to reduce cost and increase transaction volumes. However there is need to expunge the inadequacies in the existing laws. With the enactment of the IT Act, in India law has taken a quantum jump to include even the intangibles under its purview\textsuperscript{19}. This chapter will describe cyber law in India, its advantages and pitfalls.

1.12 Empirical Study

However, purely theoretical study based on secondary data cannot be relied upon until its findings are supported by primary data generated by an empirical study. Therefore inferences of secondary data search were tested using primary source of data generation i.e. an empirical study.

The empirical study was conducted in The Deptt. of Law and University Institute of Legal studies (UILS) at Panjab University, Chandigarh. Both are renowned for legal education. The Department of Laws, originally established at Lahore in 1889, was re-established at Shimla in 1948, shifted to Jalandhar in 1950 and finally re-located at the University Campus at Chandigarh in 1959. Its Alumni include eminent jurists, Judges of the Supreme Court and High Courts, Union Cabinet Ministers, State Chief Ministers, Cabinet Ministers, Ambassadors, Senior Bureaucrats, Police Officers and other legal luminaries. UILS was established as constituent department of Panjab University, in the academic session 2004-05. During a short span of time, it has emerged as one of the premier legal Institute with a unique blend of tradition and modernity. It is catering to the needs of Punjab, Haryana, Himachal Pradesh and Uttarakhand.

\textsuperscript{19}V. Sharma, Information Technology: Law and Practice, 352 (2012).
Open ended and close ended questions were framed for elaborate data collection. Since no previously validated questionnaire to assess law students’ attitudes towards socio-legal regulation of cyberspace was available, therefore items from published literature review were used to develop the attitudes section items. Draft questionnaire was designed based on discussions with study guide, professional colleagues, other researchers in the field and also related research studies. The questionnaire was pretested using a small population of Law students from Panjab University to find out the limitations in the design of questionnaire and to improve it in order to achieve the objectives formulated. The purpose of the pilot test was to evaluate the face validity of the questionnaire by soliciting comments on the clarity, relevance, and wording of the items and inclusion of any additional items or identification of any redundant items, if any. As the subject participants were reluctant to give their financial details like monthly income or annual income, so the details regarding income were removed from the questionnaire after the pilot study. Further some questions were restructured to bring clarity. The data obtained from pilot study was not included in final analysis. However, the basic use of the pilot study was to improve the quality of the date to be generated in the main study. The questionnaire was revised taking into consideration the respondents’ comments and suggestions. The modified questionnaire was used for the final survey conducted in both the university departments covered under the study.

For each question the multiple choice answers were given so that the respondents can record their opinion in form of yes/no/ no response. Also for the needful 5 point Likert type scale was framed. For each choice of answer was assigned points from 1 to 5 wherein point 1 corresponds to Strongly Disagree and point 5 corresponds to Strongly Agree. Point 3 point was assigned for the answer
wherever the respondent seemed to be Undecided. Study participants were asked to mark their responses on a 5-point Likert type scale on which 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree were assigned. The Chapter 8 will provide result of the empirical study in form of tables and graphs.

1.13 Conclusion and Suggestions

The role of the law has vastly changed with a variety of public interest functions directing the course of development locally, nationally, and internationally. These challenges have translated into multiple demands from actors in the legal and judicial system—civil servants, police, prosecutors, judges, legal advisors, and advocates—to be a social scientist, a policy planner, an administrator, a social reformer, and a conventional legal practitioner all at the same time.

Unfortunately, the legal system lags behind and remains far removed from the development needs and democratic aspirations of the people. The legal system is still a remnant of the system during colonial rule, resulting in a great disparity between constitutional aspirations for the legal system and the educational system’s performance. Clearly, there is an imminent need to reform legal system for it to be relevant and achieve its purpose. There is urgent need of comprehensive and harmonized laws in this domain. The ultimate solution is to analyse the laws of the country and make cyber laws compatible and commonly acceptable. Finally in Chapter 9 the conclusions from this work are presented. Suggestions and study limitations are also discussed.

This research work was designed to get a broad overview of this important field of interdisciplinary inquiry. It is a small step in understanding of how legal
Chapter 1

Introduction

institutions work in and through social and architectural arrangements. The data published in this context in the leading journals of law and society were also collected in addition to primary data collection in empirical study. Taken together, this research work involved an in depth inquiry into architectural-socio-legal regulation of cyberspace.