CHAPTER ONE

RESEARCH DESIGN

1.1 Introduction
1.2 Need and importance of the study
1.3 Significance of the study
1.4 Scope of the study
1.5 Statement of the problem
1.6 Objectives of the study
1.7 Hypothesis of the study
1.8 Methodology of the study
1.9 Sample design
1.10 Source of data collection
1.11 Limitations of the study


1.1 INTRODUCTION

Cyber space is the new concept evolved since 1997. This has created new opportunities to the business like E-Commerce. Due to cyber space some new crimes have been identified. These crimes are totally new. The Indian Penal Code is not able to punish the offender in a direct manner, who has committed an offence which is related to cyber space. By considering this inability, the Indian Government has passed “The Information Technology Act 2000”. The Information Technology Act has been passed by the Indian Parliament with an object to facilitate e-commerce, e-governance and to prevent Cyber Crimes. The crimes like Hacking, Publishing information which is obscene in electronic form, Breach of confidentiality & privacy, publishing false digital signature certificate, confiscation etc. is covered under this special Act, and the offender can be punished directly under sections of the IT Act 2000.

When we think about the E-Commerce, the three main parameters come in the picture, a) Computer b) Internet c) Authenticity of transaction. E-Commerce is a new emerging tool for the business. To spread your business in the whole world, E-Commerce is playing key role in this regard. The above mentioned three parameters need to be considered in detail.

E-Governance is supportive to E-Commerce, which includes legal recognition of electronic records as well as legal recognition of digital signature. These two recognitions are very important for doing business through E-Commerce. Authentication of document is the most important aspect in E-Commerce.
CHAPTER ONE RESEARCH DESIGN

1.2 NEED AND IMPORTANCE OF THE STUDY:

As IT Act 2000 has enacted for the purpose of increasing the E-commerce and to punish the offenders of the cyber crime, in this study researcher wants to see how IT Act 2000 is really playing the role in this regard. What are the opinions of the Judges, Police, Advocates, Business Persons and experts in this field? This study will help to see the parameters and the reasons why E-commerce is not being widely used instead of enactment of IT Act 2000? What are the parameters required to speed up the disposal of the matters registered under IT Act 2000? To find out the views of the people regarding IT Act 2000. To see what are the loop holes in the implementation of this well known Act, which might be very useful in the future? The above facts have thus lead to the importance of this study, in identifying the reasons why people of India hesitates to approach court of law for the Cases registered under IT Act 2000.

1.3 SIGNIFICANCE OF THE STUDY

The preamble of the Information Technology Act 2000 states .... “An Act to provide 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 involves the use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies.....” [1]

Hence, it would be important to look into the evolution of electronic data interchange as a proprietary business model and its subsequent transformation into Internet enabled ‘electronic data interchange’ called e-commerce.
Traditional communication channels like posts and telegraphs have played an important role in the spread of commerce all over the world. Use of telephones further fast-forwarded the whole process of business transactions. As the business became more and more complex it was realized that in order to remain competitive in the business world, one needed faster processing of business information.

The question was not only how to speed up the whole process of business transactions but also how to overcome the lack of standardization in the information format among the trading partners. For example, trading partners had been using different form of Purchase Orders, Invoices, Shipping Notices, Export / Import Information, carrier-to-carrier waybills, fund Transfers, etc.

The answer came in the form of development of a “Paperless” approach to various business processes such as inquiries, purchase orders, pricing, order status, scheduling, shipping, receiving, invoice payments, contracts, production data, marketing, sales etc. in the form of standards and protocols. This “Paperless” approach is often referred to as Electronic Data Interchange (EDI) – an application-to-application exchange of standard business documents in an electronic format between two or more entities through computers. Today, all above mentioned facilities as well as related laws (IT Act -2000) is in existence. Even though the implementation of the E-commerce with law is in question, by observation in and around the situation of E-commerce needs to be improved. Researcher intends to study & find, the parties in the contract are under fear that if other party breaks the contract then how the law system particularly cyber law will protect the interest of the party in the contract.

The present research study is conducted to emphasize on how cyber law will help any party in the contract for E-commerce as well as how the citizen will get fast relief in the court of law if he is aggrieved by any offence which is punishable under IT Act 2000.
The projected value of the market over the years and projected for the upcoming years are:

<table>
<thead>
<tr>
<th>Year</th>
<th>Projected Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>$2.8 billion</td>
</tr>
<tr>
<td>2010</td>
<td>$4.1 billion</td>
</tr>
<tr>
<td>2011</td>
<td>$5.6 billion</td>
</tr>
</tbody>
</table>

*Source: Compiled from techcrunchies.com [4], Web sites accessed on 13th Oct 2008*

The recent survey conducted by Nielsen, India has emerged as the 3rd biggest nation when it comes to online shopping and using a credit card online. Drawn by the facilities offered by the Web and the diversity of products available on it, Indian netizens have emerged as the third biggest credit card users globally for online purchasing, next only to the Turkey and Ireland.

The survey shows more than 85 per cent of Internet users in the world are purchasing goods or services online, with credit cards as the most used method of payment [5].
### Table No. 1.2
Cyber Crimes/Cases Registered and Persons Arrested under IT Act 2003-2006

<table>
<thead>
<tr>
<th>SL NO.</th>
<th>Crime Heads</th>
<th>Case Registered</th>
<th>Person Arrested</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tampering computer source department</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Hacking Computer Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i) Loss/damage to computer resource/utility</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i) Hacking</td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>Obscene publication/transmission in electronic form</td>
<td>20</td>
<td>34</td>
</tr>
<tr>
<td>4</td>
<td>Failure</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>i) Of compliance/orders of certifying Authority</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ii) To assist to decoy or the information in interception by Govt Agency</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Un-authorised access/attempt to access of protected computer system</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>Obtaining Licence or digital signature by misrepresentation/suppression of fact</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Publication false digital signature certificate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>Fraud digital/signature</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>Breach of confidentiality/privacy</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>Other</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>Total</td>
<td>60</td>
<td>68</td>
</tr>
</tbody>
</table>

Source: Compiled from National Records Crime Bureau [2], Web sites accessed on 26th Oct 2008
Before amendment in IPC it was difficult to cope-up with Cyber Crimes. The Criminals are doing crime with the help of latest technology. The concept of time theft is not there in the IPC. Now a day, Internet time can be stolen by the offenders. Money can be transferred electronically with the help of computers and internet. So, to cope-up for Cyber crime the IT Act is there, it has been enacted in 2000. With the help of this study it is possible to understand the problems faced by the people of India with different point of views namely Jurisdiction, which section will be applied, which court needs to be approached, what precautions need to be taken etc. Therefore this study is of immense significance to understand the problems of the Cyber Crimes how to handle it and we can find out some probable solutions in the form of suggestions.

1.4 SCOPE OF THE STUDY:

IT Act 2000 came into force on 17th October 2000. After that too many cases were registered under IT Act 2000. There is some areas which needs to be studied so that the weak area can be pointed out. Some steps needs to be taken so that the effectiveness at the IT Act 2000 increases. Hence, the present study has been undertaken to examine the problems being faced by the citizen of India for getting early justice for the matters registered under IT Act 2000. This study is useful in identifying problems and their causes and provides probable solutions to increase the usage of E-commerce in day to day business.

1.5 STATEMENT OF THE PROBLEM:

The use of Cyber Space has been increased and widely spreading day by day. Due to increase in Cyber Space there has been number of complaint reports in area of Cyber Crime in the age of Information Technology. To control the Cyber Crime, it is a very urgent need to do some research in this direction. So the researcher has chosen the topic “IMPLICATIONS
CHAPTER ONE RESEARCH DESIGN

OF CYBER LAW IN THE AREA OF CYBER CRIME” for detail study.

1.6 OBJECTIVES OF THE STUDY:

The present research work was undertaken with the prime objective of identifying the various reasons and the problems of people in the world facing to approach the court at law.

The main objectives of the study are as follows:
1) To study the reasons why people hesitate to approach court of law in the dispute regarding cyber crime.
2) To study the average time to decide any matter registered under the IT Act 2000.
3) To find out the reasons for E-commerce not being widely used instead of enactment of IT Act 2000.
4) To compare any general matter with matter registered under the IT Act 2000.
5) To suggest parameters for speedy disposal of the matters registered under the IT Act 2000.

1.7 HYPOTHESIS OF THE STUDY:

With the above stated objectives in mind, the following hypothesis was formed for the present study by the researcher.

1. There would be no difference in the time of disposal of general matter and the matter registered under the IT Act 2000.
2. There are no parameters for speedy disposal of the matter registered under the IT Act 2000.
3. People hesitate to file a criminal case under IT Act 2000.
4. There are some reasons for E-commerce for not being widely used instead of enactment of the IT Act 2000.
1.8 METHODOLOGY OF THE STUDY

Keeping in the mind the aforesaid objectives, the methodology chosen for the present study is elaborated as under-

1. Survey Method: In order to elicit relevant information pertaining to the problems of Cyber Crimes a survey method was adopted. At the outset, a pilot survey was conducted to clarify and finalize the key issues. After the pilot survey, the cyber crime cells at Mumbai and Pune visited and the responses were collected. In order to collect responses, a comprehensive questionnaire was administered in person by visiting the selected persons.

2. Observation Method: To have a microscopic view of the cyber cell, the researcher adopted an observation method too. The objective of this method is to cross examine the various responses received from the respondents regarding the problems faced. With this view, the researcher collected the responses regarding the cyber law.

1.9 SAMPLE DESIGN:

To choose required sample non probability sampling method has been utilized. Under this, purposive sampling method is used to select different categories of respondents. These respondents are as indicated in Table No. 1.1. The Sample has been chosen with reference to Krejcie and Morgan Model.
### Table No-1.3
**Research Sample**

<table>
<thead>
<tr>
<th>Category (Occupation)</th>
<th>Count</th>
<th>Category Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Judiciary</td>
<td>1</td>
<td>.3%</td>
</tr>
<tr>
<td>Police</td>
<td>25</td>
<td>7.7%</td>
</tr>
<tr>
<td>Advocate</td>
<td>122</td>
<td>37.8%</td>
</tr>
<tr>
<td>Business Person</td>
<td>29</td>
<td>9.0%</td>
</tr>
<tr>
<td>Experts</td>
<td>146</td>
<td>45.2%</td>
</tr>
<tr>
<td>Total</td>
<td>323</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

(Source: Primary Data, Count: No. of Respondents)
MAP NO. 1.1
MAP, SHOWING STUDY AREA IN MAHARASHTRA

The oval indicates the Sample areas Pune, Satara, Kolhapur, Sangali and Mumbai
1.10 SOURCES OF THE DATA COLLECTION

1. Primary data: The primary data has been collected from the respondents like Judges and Advocates at District Court. The data has been collected from the businessmen and Cyber experts. Considering geographical limitations and personal visits, the data has been collected from Pune, Satara, Kolhapur, Sangali and Mumbai. The data has been collected from Cyber Cell of Police Commissioner’s Office at Pune and Mumbai also. The primary data, tools like structured questionnaire, Interview and Observations has been considered.

a) Questionnaire: A detailed and comprehensive questionnaire was prepared in consultation with many experts in this field and the same was pre-tested and then suitably amended. Then, the questionnaire was administered to the concerned persons in the selected cyber related cell by personally visiting them. While preparing the questionnaire, care was taken to put only objective questions because the objectivity of the responses was important. To achieve the given objectives, only one set of questionnaire was administered to the entire cell. The questions were set in such a manner that they were applicable to all cyber crimes. The detail questionnaire has been attached in Annexure-I format in the last part of the thesis.

b) Informal Discussions, Structured and Unstructured Interviews: After the administration of questionnaire, it was necessary to have detailed investigation for certain issues which could not be adequately covered through the questionnaire. The questionnaire which is open in nature or area in which a further investigation was required was taken up and information was
elicited through informal discussions or through structured and unstructured interviews.

c) Observations: During the visit, the researcher observed the infrastructure, layout and the activities carried out at Cyber Cell at Police Commissioner’s Offices at different places. The researcher also observed the activities carried out at the JMFC Courts.

2. Secondary data: Statistical data has been collected from CID (Crime Investigation Department) [2], Pune for Maharashtra State and NCRB (National Records Crime Bureau) [3] for India. As well as data is collected from Internet, Computer books and documentation. In addition to this, the information related to Cyber Crime, Cyber Law and E-commerce has been collected from various journals, books, Manuals and web sites.

1.11 LIMITATIONS OF THE STUDY:

As Law is applicable to all over the territory of nation, IT Act 2000 is also applicable to all over the territory of India. As our country is so big in size, it is not feasible to take the respondents from all over the country. Hence the Researcher has taken five districts in which the majority of the crimes took place.

REFERENCES

Books:

Websites:

2. www.mahacid.com, Maharashtra Crime Investigation Department website, chapter 18 Cyber Crime

3. www.ncrb.nic.in, National Records Crime Bureau, chapter 18, Cyber Crime
