CHAPTER - 3

RESEARCH METHODOLOGY
CHAPTER-3

RESEARCH METHODOLOGY

3.1: INTRODUCTION

The success of any research depends upon the methodical and planned approach that has been undertaken by the researcher. The planning and research design is vital at every stage of the research. This chapter depicts the various aspects that have been considered in the planning stage, while designing the study. It contains the statement of the study, its aims and objectives, the hypothesis for the study undertaken, the field or the areas in which the investigations were undertaken, the tools and the techniques of the study, the modes of their usage and finally in the subsequent chapters, the analysis and conclusions drawn from it are the issues that have been explicitly brought in, in this chapter.

3.2: STATEMENT OF THE STUDY.

The title of the topic of the study is ‘A Criminological study on the Importance of the Information Technology Act 2000 with special reference to Cyber Crimes in Bangalore City”. The principle aim of selecting this topic of study is to assess the impact of law on crime. Cyber crime and the related laws are new, when compared to the traditional and other white collar crime. India has been one of the pioneering countries in implementing the cyber law, which was perhaps with intent to facilitate the e-commerce meaningfully in India. It also contained within it a penal component, under which the various criminal and malicious acts using the computers and the cyber space are addressed. Criminology studies crime, criminals and the law in relation to the society. It seeks explanation on where, when, why and how different types of
crimes occur. Criminologists seek the relationship between the laws, the persons violating it and the victim upon whom the crime is affected. Criminology also suggests the effective means of preventing these crimes. The significance of this study is that much has been said about the concept of cyber crime, however there are a very few criminological studies made in this area. It is aimed to create a base for further studies, especially in the Indian context.

This Chapter presents description of the methods, techniques and empirical measures employed to collect and analyze the data. The chapter has been organised and presented as following:

1. Aims and objectives of the study.
2. Hypothesis of the study.
3. Area of the study.
4. Sample of the study.
5. Research design.
6. Pilot survey.
7. Variables considered in the study.
10. Limitation of the study.

3.3: AIMS AND OBJECTIVES OF THE STUDY:

An adequate explanation of objectives is a crucial prerequisite for the successful completion of a research undertaking. The establishment of these proposals highlights the scope of the study. The use of computers has significantly increased in India. The penetration of computers as a tool in several spheres of commerce, trade and entertainment has risen all over the world. So have crimes using computers. Governments divide crimes into offences against persons, property, public order or morality. Crimes are also classified upon the intent of the offender. Cyber crimes
are some of these. Cyber crimes are on the increase due to a host of factors. Technology has enabled these, as much as any other factor. The lack of regulation or legislation in several countries was severely hampering the e-commerce. The Information Technology Act 2000 became necessary due to India becoming a signatory to the resolution of the General Assembly of the United Nations for the adaptation of the Model Law on Electronic Commerce adapted by the United Nations Commission on International Trade Law (UNCITRAL). While most of the recommendations emphasized the incorporation and recognition of electronic commerce within the framework of a law, the regulatory mechanisms for trade and commerce using the computers and the electronic media, information security, the offences arising from these, their descriptions, penal provisions and adjudication were vested with the member countries.

THE OBJECTIVES OF THE STUDY ARE THEREFORE, AS LISTED BELOW:

• The Information Technology Act 2000 has ambiguities which are not addressed, leading to an increase in cyber crimes.
• The loss, is monetary terms are greater in cyber crimes than conventional crimes in Bangalore City.
• An increase in the rate of cyber crimes is greater than conventional crimes in Bangalore City.
• Victims of cyber crimes are ignorant of their victimization; most victims do not know their offender, while a crime is being committed on them.

3.4: HYPOTHESES

FIRST HYPOTHESIS: Computer and cyber space are usually used to commit crimes on the premise that the incidents are rarely detected, due
to its anonymity and the fact that crimes may be committed in one country and its effects may be felt in another and the varied nature of the trans national laws, technologies to prevent and detect these crimes.

SECOND HYPOTHESIS: Cyber crimes are mainly committed for economic gain and defamation of the intended victim.

THIRD HYPOTHESIS: Victims do not readily come forward to report cyber crime, especially, the corporate bodies, for the reason of loss of credibility and further businesses; futility of the whole process, as the crime has trans-national dimensions and there is no law to act beyond the sovereign boundaries.

FOURTH HYPOTHESIS: The Information Technology Act 2000 is casually enforced unlike other penal legislations; The Act requires amendments with the changes in the technology and types of usage of cyber space;

FIFTH HYPOTHESIS: The Cyber Crime Police Station, Bangalore though well equipped and staffed is unknown to the victims of Cyber Crime; Corporate Bodies have their own internal Cyber Security mechanisms to handle cyber crimes

SIXTH HYPOTHESIS: Cyber Crimes are preventable to a great extent by creation of awareness of it; involvement of experts in the field of Information Technology and by increasing the awareness levels of the users of the Cyberspace.
3.5: AREA OF THE STUDY:

The area of the study is Bangalore City. Bangalore is regarded as the Technology hub of not only India, but also the world, with its presence clearly seen in the global scenario. It stands out in the spheres of Software Development, Information Technology Enabled Services (I.T.E.S.), Business Process Outsourcing (B.P.O.) and Knowledge Process Outsourcing (K.P.O.).

Geography

Bangalore lies in the southeast of the South Indian state of Karnataka. It is in the heart of the Mysore Plateau (a region of the larger Precambrian Deccan Plateau) at an average elevation of 920 m (3,018 ft). It is positioned at 12°58'79"N 77°34'34"E12.97°N 77.56°E and covers an area of 741 km² (286 mi²). The majority of Bangalore City lies in the Bangalore Urban district.

Climate

Due to its high elevation, Bangalore usually enjoys salubrious climate throughout the year, although freak heat waves can make things very uncomfortable in the summer. The coolest month is January with an average low temperature of 15.1 °C and the hottest month is April with an average high temperature of 33.6 °C. The highest temperature ever recorded in Bangalore is 38.9 °C and the lowest ever is 7.8 °C (on January 1884). Winter temperatures rarely drop below 12 °C (54 °F), and summer temperatures seldom exceed 36-37 °C (100 °F). Bangalore receives rainfall from both the northeast and the southwest monsoons and the wettest months are September, October and August, in that order. The summer heat is moderated by fairly frequent thunderstorms, hence it has acquired the sobriquet as the ‘Air Conditioned City’.
Bangalore is known as the "Garden City of India" because of its greenery and the presence of many public parks, including the Lal Bagh and Cubbon Park.

**History**

The name Bangalore is an anglicised version of the city's name in the Kannada language, *Bengaluru*. The earliest reference to the name "Bengaluru" was found in a ninth century Western Ganga Dynasty stone inscription on a "vira gallu" (literally, "hero stone"), a rock edict extolling

---

30 http://www.mapsofindia.com
the virtues of a warrior). In this inscription found in Begur, "Bengaluru" is referred to as a place in which a battle was fought in 890 AD. It states that the place was part of the Ganga Kingdom until 1004 and was known as "Bengaval-uru", the "City of Guards" in Halegannada.

Map 2. Showing the Districts of Karnataka State
An apocryphal, though popular, anecdote recounts that the 11th-century Hoysala king Veera Ballala II, while on a hunting expedition, lost his way in the forest. Tired and hungry, he came across a poor old woman who served him boiled beans. The grateful king named the place "benda-kaaluru" (Kannada: ಬೆಂಡಾಕಾಲುರು) (literally, "town of boiled beans"), which eventually evolved into "Bengaluru".

After centuries of the rule of the Western Gangas, Bengaluru was captured by the Cholas in 1024 CE which later passed on to the Chalukya-cholas in 1070. In 1116 the Hoysala Empire, overthrew the Cholas and extended its rule over Bangalore. Modern Bangalore was founded by a vassal of the
Vijayanagara Empire, Kempe Gowda I, who built a mud-brick fort and a Nandi Temple in the proximity of modern Bangalore in 1537. Kempe Gowda referred to the new town as his "gandubhūmi" or "Land of Heroes".

Within Bangalore Fort, the town was divided into smaller divisions – each called a "pete". The town had two main streets – Chikkapete Street, which ran east-west, and Doddapete Street, which ran north-south. Their intersection formed the Doddapete Square — the heart of Bangalore. Kempe Gowda's successor, Kempe Gowda II, built four famous towers that marked Bangalore's boundary. During the Vijayanagara rule, Bangalore was also referred to as "Devarāyanagara" and "Kalyānapura" ("Auspicious City"). After the fall of the Vijayanagara Empire, Bangalore's rule changed hands several times. In 1638, a large Bijapur army led by Ranadulla Khan and accompanied by Shahji Bhonsle defeated Kempe Gowda III and Bangalore was given to Shahaji as a jagir. In 1687, the Mughal general Kasim Khan defeated Ekoji I/Venkoji, son of Shahaji, and then sold Bangalore to Chikkadevaraja Wodeyar (1673–1704) of Mysore for 300,000 rupees. After the death of Krishnaraja Wodeyar II in 1759, Hyder Ali, Commander-in-Chief of the Mysore Army, proclaimed himself the de facto ruler of Mysore. The kingdom later passed to Hyder Ali's son Tippu Sultan, known as the Tiger of Mysore. Bangalore was eventually incorporated into the British Indian Empire after Tippu Sultan was defeated and killed in the Fourth Anglo-Mysore War (1799). The British returned administrative control of the Bangalore "pētē" to the Maharaja of Mysore, choosing only to retain the Cantonment under their jurisdiction. The 'Residency' of Mysore State was first established at Mysore in 1799 and later shifted to Bangalore in the year 1804. It was abolished in the year 1843 only to be revived in 1881 at Bangalore and to be closed down permanently in 1947, with Indian independence. The British, found it easier to recruit employees in the Madras Presidency and
relocate them to cantonment area during this period. The Kingdom of Mysore relocated its capital from Mysore city to Bangalore in 1831. Two important developments during this period contributed to the rapid growth of the city: the introduction of telegraph connections and a rail connection to Madras in 1864.

In the 19th century, Bangalore essentially became a twin city, with the "pête", whose residents were predominantly Kannadigas, and the "cantonment" created by the British, whose residents were predominantly Tamils. Bangalore was hit by a plague epidemic in 1898 that dramatically reduced its population. New extensions in Malleshwara and Basavanagudi were developed in the north and south of the pête. Telephone lines were laid to help co-ordinate anti-plague operations, and a health officer was appointed to the city in 1898. In 1906, Bangalore became the first city in India to have electricity, powered by the hydroelectric plant situated in Shivanasamudra. Bangalore's reputation as the Garden City of India began in 1927 with the Silver Jubilee celebrations of the rule of Krishnaraja Wodeyar IV. Several projects such as the construction of parks, public buildings and hospitals were instituted to beautify the city. After Indian independence in August 1947, Bangalore remained in the new Mysore State of which the Maharaja of Mysore was the Rajapramukh. Public sector employment and education provided opportunities for Kannadigas from the rest of the state to migrate to the city. Bangalore experienced rapid growth in the decades 1941–51 and 1971–81, which saw the arrival of many immigrants from northern Karnataka. By 1961, Bangalore had become the sixth largest city in India, with a population of 1,207,000. The population as per the Census of 2001 stands at 5,101,000, and is estimated approximately to be 5,300,000 in 2009.
Economic Development.

In the decades that followed, Bangalore's manufacturing base continued to expand with the establishment of private companies such as Motor Industries Company (MICO; a subsidiary of Robert Bosch GmbH), which set up its manufacturing plant in the city. Bangalore experienced a growth in its real estate market in the 1980s and 1990s, spurred by capital investors from other parts of the country who converted Bangalore's large plots and colonial bungalows into multi-storied apartments. In 1985, Texas Instruments became the first multinational to set up base in Bangalore. Other Information Technology companies followed suit and by the end of the 20th century.

Bangalore is called the Silicon Valley of India because of the large number of information technology companies located in the city which contributed 33% of India's Rs. 144,214 crore (US$ 31 billion) IT exports in 2006-07. Bangalore's IT industry is divided into three main clusters — Software Technology Parks of India (STPI); International Tech Park, Bangalore (ITPB); and Electronics City. UB City, the headquarters of the United Breweries Group, is a high-end commercial zone. Infosys and Wipro, India's second and third largest software companies are headquartered in Bangalore, as are many of the global SEI-CMM Level 5 Companies.

Bangalore is the undisputed IT Capital of India. Apart from leading Indian IT companies like Infosys, Wipro, Tata Consultancy Services, the world's leading IT companies like GE, Texas Instruments, CISCO, Digital, IBM, HP, Digital/Compaq, Sun Micro Systems, Motorola, Microsoft, Lucent Technologies, S A P, Oracle, Novell, Intel, Network Associates, Sasken, Nokia, A D C, Sasken, Sony, Nortell, A M D Satyam, (now Satyam Mahindra) Tech Mahindra, Siemens, Synopsys, Philips, Analog Devices, National Semiconductors, Freescale Semiconductors, Broadcom, etc. have establishments in Bangalore. As per the NASSCON- McKinsey Report
2008, Bangalore city has 664 Multi National Companies, out of 87 SEI CMM Level-% IT companies in the world, 63 are in India. Out of these 32 are in Bangalore. Totally there are 1999 Information Technology Companies, which employs 5,50,000 IT professionals, which is approximately 1/3 rd of the total IT professionals in the country. This is the reason why Bangalore is also known as THE IT CAPITAL OF INDIA.

Bangalore is also the Fourth largest Technology Cluster in the World, after Silicon Valley (California, U S A), Boston and London.

More than 40% of Bangalore's software exports are in the high technology areas-IT access networks, optical networks, video broadcasting, Bluetooth, WAP, 3G Wireless Applications etc.

The first internet service provider in Bangalore was STPI, Bangalore which started offering internet services in early 1990s. This internet service was however restricted to corporate establishments, until VSNL started offering dial-up internet services to the general public at the end of 1995. Currently, Bangalore has the largest number of broadband internet connections in India.  

The 2004 National Crime Records Bureau statistics indicate that Bangalore accounts for 9.2% of the total crimes reported from 35 major cities in India. Delhi and Mumbai accounted for 15.7% and 9.5% respectively.  

3.6: CYBER CRIME POLICE STATION, BANGALORE:

Establishment, Organisation Structure, brief Overview of the Functions and related Equipment

Table 3.1: Indicating the Staffing pattern of Cyber Crime Police Station, Bangalore.

<table>
<thead>
<tr>
<th>Allocation Particular</th>
<th>DY.S.P</th>
<th>P.I</th>
<th>PSI</th>
<th>HC/PC</th>
<th>APS</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sanctioned Strength</td>
<td>04</td>
<td>04</td>
<td>10</td>
<td>05</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>Actual Strength</td>
<td>09</td>
<td>03</td>
<td>02</td>
<td>07</td>
<td>03</td>
<td>24</td>
</tr>
<tr>
<td>Vacancy</td>
<td>NIL</td>
<td>01</td>
<td>-----</td>
<td>04</td>
<td>02</td>
<td>07</td>
</tr>
</tbody>
</table>

This Police Station has one legal advisor of the rank of public prosecutor.

Technical assistance:

Investigation officer are provided with the service of IT experts on hired.

Training: The officers are trained by the following agencies:

- CBI Academy, GHAZIABAD
- Office of the controlled for certified authorities, NEW DELHI.
- Asian school of cyber laws, PUNE.
Roman Technology SSI Wipro, ECT based in Bangalore.

Local highly qualified computer impact continuous training of Cyber Crime Police Station.

The Cyber Crime Police Station is equipped with cyber-forensic equipment and has other infrastructure. The cyber Forensic Lab is equipped with the following Hardware and software for the purpose of investigation.

HARDWARE
- DRAC 2000 WORKSTATION
- DRAC 2000 PORTABLE
- CYBER IMAGE BACK UP SYSTEM
- WINDOW 2000 SERVER WITH 2 NODES
- SUN SOLARIS SERVER WITH 2 NODES
- LINEX SERVER WITH 2 NODES

SOFTWARE
- ENCASE
- WINHEX
- ADVANCED PASSWORD RECOVERY TOOL
- FILE AND PHOTO RECOVERY TOOL
- E MAIL EXAMINER
- PDA EXAMINER
Photograph 1: Showing the research Scholar and the Guide interacting with a C.O.D Officer.

Functions:

The Government of Karnataka has passed rules u/s 90 of IT Act 2000 for regulation of cyber cafes on 5th August 2004. The Cyber Crime Police Station has been declared as cyber authority to enforce the rule and it is being implemented.

The officers of Cyber Crime Police Station are imparting training to the Judges of Judicial Academy, on the aspects related to computer, computer forensics and digital evidence.

Table No.3.2: Abstract of Criminal Cases as On 31.12.2007.

<table>
<thead>
<tr>
<th>Years</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported</td>
<td>04</td>
<td>16</td>
<td>08</td>
<td>14</td>
<td>42</td>
<td>27</td>
<td>41</td>
</tr>
<tr>
<td>Charge Sheeted</td>
<td>01</td>
<td>07</td>
<td>01</td>
<td>01</td>
<td>08</td>
<td>04</td>
<td>03</td>
</tr>
<tr>
<td>Un/Reported To the Court</td>
<td>01</td>
<td>03</td>
<td>04</td>
<td>06</td>
<td>09</td>
<td>02</td>
<td>01</td>
</tr>
<tr>
<td></td>
<td>01</td>
<td>04</td>
<td>01</td>
<td>04</td>
<td>11</td>
<td>01</td>
<td>01</td>
</tr>
<tr>
<td>Other Wise Disposed/(High Court Quashed)</td>
<td>01</td>
<td>NIL</td>
<td>NIL</td>
<td>01</td>
<td>NIL</td>
<td>NIL</td>
<td>NIL</td>
</tr>
<tr>
<td>Acquittal</td>
<td>NIL</td>
<td>02</td>
<td>01</td>
<td>NIL</td>
<td>NIL</td>
<td>NIL</td>
<td>NIL</td>
</tr>
<tr>
<td>Case Transferred To Other Police Station</td>
<td>NIL</td>
<td>NIL</td>
<td>NIL</td>
<td>NIL</td>
<td>05</td>
<td>03</td>
<td>02</td>
</tr>
<tr>
<td>U.I</td>
<td>NIL</td>
<td>NIL</td>
<td>01</td>
<td>02</td>
<td>09</td>
<td>17</td>
<td>34</td>
</tr>
<tr>
<td>Total</td>
<td>08</td>
<td>32</td>
<td>16</td>
<td>28</td>
<td>84</td>
<td>54</td>
<td>82</td>
</tr>
</tbody>
</table>

The above table indicates the abstract of the crime particulars from its inception till the end of 2007.
ENQIRIES:

The IT Act of 2000 permits the complainant to submit his/her information about a Cyber Crime and to be treated as a Non-Cognizable Crime. Such cases are called as enquiries, where it may lead to warning of the offender, or be compoundable by payment of fine or penalty or even compensation. This is so because there is a tort element in the functionality of the IT Act.

Table 3.3: Showing the number of enquiries regarding the offences.

<table>
<thead>
<tr>
<th>Year</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received</td>
<td>13</td>
<td>39</td>
<td>59</td>
<td>93</td>
<td>123</td>
<td>188</td>
<td>103</td>
</tr>
<tr>
<td>Enquiry Completed</td>
<td>13</td>
<td>39</td>
<td>59</td>
<td>93</td>
<td>123</td>
<td>185</td>
<td>71</td>
</tr>
<tr>
<td>Pending Enquiry</td>
<td>nil</td>
<td>nil</td>
<td>nil</td>
<td>nil</td>
<td>nil</td>
<td>03</td>
<td>32</td>
</tr>
</tbody>
</table>

This table shows the abstract of Enquiries reported at Cyber Crime Police Station. The table indicates that all the Enquiries from 2001 to 2005 have been completed. There are 03 enquiries pending in 2006 and 32 pending in 2007.
### Table 3.4: Classes of Criminal Cases Registered at Cyber Crime Police Station From 2001 To 31-12-2007

<table>
<thead>
<tr>
<th>Offences</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tampering</td>
<td>-----</td>
<td>01</td>
<td>01</td>
<td>02</td>
<td>04</td>
<td>03</td>
<td>03</td>
<td>14</td>
</tr>
<tr>
<td>source code</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacking</td>
<td>04</td>
<td>09</td>
<td>05</td>
<td>06</td>
<td>24</td>
<td>20</td>
<td>31</td>
<td>99</td>
</tr>
<tr>
<td>Electronically obscene e-mails</td>
<td>-----</td>
<td>05</td>
<td>01</td>
<td>06</td>
<td>10</td>
<td>04</td>
<td>11</td>
<td>37</td>
</tr>
<tr>
<td>Copyright Act 1957</td>
<td>-----</td>
<td>01</td>
<td>01</td>
<td>-----</td>
<td>02</td>
<td>-----</td>
<td>-----</td>
<td>04</td>
</tr>
<tr>
<td>Trademark Act</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>01</td>
<td>-----</td>
<td>-----</td>
<td>01</td>
</tr>
<tr>
<td>Others</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>01</td>
<td>-----</td>
<td>02</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>04</td>
<td>16</td>
<td>08</td>
<td>14</td>
<td>42</td>
<td>27</td>
<td>41</td>
<td>152</td>
</tr>
</tbody>
</table>

This table indicates the classes of cases that were registered by the Cyber Crime Police Station. The first three categories i.e, Tampering source code, Hacking and Electronically obscene e-mails fall under the Information Technology Act, 2000.

The Copyright Act 1957 and the Trademark Act are not within it. Cases pertaining to it were registered only till the year 2005 only. They were transferred since then to the relevant police station, mainly due to the ambiguity of scope of the Information Technology Act-2000.
3.7: SAMPLE FOR THE STUDY:

The sample for the study was chosen on the basis of Stratified Random Sampling Method. The researcher has understood the strata of the respondents to be employed directly in the areas of Software Development, Information Technology Enabled Services (I.T.E.S.), Business Process Outsourcing (B.P.O.) and Knowledge Process Outsourcing (K.P.O.), who are into the field of information technology. This stratum was chosen by the researcher due to the fact that they are the most exposed to the field of Information Technology and the Cyber medium, wherein most of the Cyber Crimes are said to occur. Due to the vastness of the field, three hundred respondents were chosen for the current study, mainly due to the constraints of time and availability of the respondents. Amongst these, one hundred and fifty respondents were male and one hundred and fifty female. Thus there were equal numbers of gender wise representation. All the respondents were employed in Bangalore City and employed in the Information Technology field during the period of this study.

3.8: METHODOLOGY:

Survey method has been used for the current study, as this design of study is the most appropriate one. Criminologists in the past three decades have found favour with this method (Neuman and Wiegand; 2000). It has been attributed to factors such as computerization of large quantities of data and feasibility of its analysis; the emergence of several survey agencies with a high level of expertise; data storage capacity of

---

computers, and, the availability of the internet as a communicating device for distribution and receiving of information.

3.9: DATA COLLECTION:

For the present study, a Questionnaire schedule was prepared. The questionnaire was distributed to the respondents by e-mail, using friends and other sources known to the researcher. They were mailed to the researcher in after being filled at his e-mail address (profaravind@gmail.com). After receiving the mails, the researcher has taken a print out of the mail and used the responses for the compilation of the data.

3.10: ABOUT THE QUESTIONNAIRE:

The questionnaire was prepared with the help of existing literature, articles and present trends, which can help to fulfill the objectives and support the hypotheses. The questionnaire contained both open ended and close-ended questions. There were blend of bi-polar and multi-polar questions. It also contained information about the respondents and information relevant to the study.

3.11: VARIABLES CONSIDERED FOR THE STUDY:

In consideration with the objectives framed for this study, the following are the Dependent Variables and independent variables.

**Dependent Variables:**

A. Knowledge of the respondent of the existence of The Information Technology Act-2000;

B. Penal provisions in the Act;
C. Respondents reaction to Cyber Crime, when encountered and the organisational protocol towards it;

D. Opinion about the extension of the Act towards the areas of Intellectual property Rights;

E. The vulnerability of persons to Cyber Crimes;

F. Given the trans-national character, whether Cyber Crimes should have an Internationally governable law;

G. Opinion as to how well equipped are the Cyber Crime Police in Bangalore City to investigate, detect and prosecute cyber crime and criminals, and;

H. The common loss due to Cyber Crimes.

**Independent Variables:**

1. Age.
2. Gender.
3. Educational Qualifications.

**3.12: PILOT STUDY:**

A Pilot Study was undertaken in Mysore City, which has a reasonably large population and Information Technology Penetration. This study was made during the Third Term of the Scholar's study. Information so accumulated had a very salutary effect in executing research task. In the light of experience gained, the schedule was revised. During this phase attempt was made to assess the objectives already
determined in order to ascertain whether the research action envisaged and interest as found to be quite compatible.

3.13: PERIOD OF THE STUDY:

The study titled ‘A Criminological study on the Importance of the Information Technology Act 2000 with special reference to Cyber Crimes in Bangalore City” was conducted during the period of February 2005 to January 2009.

3.14: LIMITATIONS OF THE STUDY:

This study has the following limitations:

a. Since Cyber crime is a ‘Virtual’ crime, the victims are largely under the impression that the whole incident is a prank or something is wrong with their computer system. Hence, many do not know whether to react to it by going to the police or ignore it.

b. Most of the respondents declined to give their names in the questionnaire.

c. A few of the respondents did not wish to reveal the name of the organisation which they served; this is because of the reason that their opinion may be misconstrued as the organisational opinion.

d. A few of the respondents have opined that they are unable to respond to questions on the efficiency of the Police in the Cyber Crime Police Station, Bangalore, as they are unaware of the types of training received and the software used and as well as the industrial intervention in combating cyber crimes.

e. Another major limitation is the proposed amendment of the Information Technology Act-2000. The proposal, which was passed by the Parliament, is yet to be given the date of implementation.

THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 of 2000)

[9th June, 2000]

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 involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.


and whereas the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information;
and whereas it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

Be it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:—

CHAPTER I

Preliminary

S.1. Short title, extent, commencement and application

S.2. Definitions

(1) In this Act, unless the context otherwise requires, —

(a) "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

(b) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(c) "adjudicating officer" means an adjudicating officer appointed under subsection (1) of section 46;

(d) "affixing digital signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

(e) "appropriate Government" means as respects any matter,—
(i) Enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution,

the State Government and in any other case, the Central Government;

(f) "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(g) "Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24;

(h) "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

(i) "computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

(j) "computer network" means the interconnection of one or more computers through—

(i) The use of satellite, microwave, terrestrial line or other communication media; and
(ii) Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(k) "Computer resource" means computer, computer system, computer network, data, computer data base or software;

(l) "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (1) of section 17;

(n) "Cyber Appellate Tribunal" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;

(o) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

(p) "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

(q) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) of section 35;
(r) "electronic form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(s) "Electronic Gazette" means the Official Gazette published in the electronic form;

(t) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(u) "Function", in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(v) "Information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

(w) "Intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

(x) "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

(y) "Law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the
Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder;

(z) "Licence" means a licence granted to a Certifying Authority under section 24;

(za) "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(zb) "Prescribed" means prescribed by rules made under this Act;

(zc) "Private key" means the key of a key pair used to create a digital signature;

(zd) "Public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(ze) "Secure system" means computer hardware, software, and procedure that—

(a) Are reasonably secure from unauthorised access and misuse;

(b) Provide a reasonable level of reliability and correct operation;

(c) Are reasonably suited to performing the intended functions; and

(d) Adhere to generally accepted security procedures;

(zf) "Security procedure" means the security procedure prescribed under section 16 by the Central Government;

(zg) "Subscriber" means a person in whose name the Digital Signature Certificate is issued;
"Verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—

(a) The initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) The initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

CHAPTER II

DIGITAL SIGNATURE


CHAPTER III

ELECTRONIC GOVERNANCE

S.4. Legal recognition of electronic records.


S.6. Use of electronic records and digital signatures in Government and its agencies


S.8. Publication of rule, regulation, etc., in Electronic Gazette
S.9. Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form.


CHAPTER IV

ATTRIBUTION, ACKNOWLEDGMENT AND DESPATCH OF ELECTRONIC RECORDS


S.13. Time and place of despatch and receipt of electronic record.


CHAPTER VI

REGULATION OF CERTIFYING AUTHORITIES

S.17. Appointment of Controller and other officers.

S.18. Functions of Controller.


S.20. Controller to act as repository.
S.21. Licence to issue Digital Signature Certificates.

S.22. Application for licence.

S.23. Renewal of licence.

S.24. Procedure for grant or rejection of licence.

S.25. Suspension of licence.


S.27. Power to delegate.

S.28. Power to investigate contravention.

S.29. Access to computers and data.

S.30. Certifying Authority to follow certain procedures.

S.31. Certifying Authority to ensure compliance of the Act, etc.

S.32. Display of licence.

S.33. Surrender of licence.

S.34. Disclosure.

CHAPTER VII

Digital Signature Certificates

S.35. Certifying Authority to issue Digital Signature Certificate.

S.36. Representations upon issuance of Digital Signature Certificate.

S.37. Suspension of Digital Signature Certificate.
S.38. Revocation of Digital Signature Certificate.

S.39. Notice of suspension or revocation.

CHAPTER VIII

DUTIES OF SUBSCRIBERS

S.40. Generating key pair.

S.41. Acceptance of Digital Signature Certificate.

S.42. Control of private key.

CHAPTER IX

PENALTIES AND ADJUDICATION

S.43. Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network, —

(a) Accesses or secures access to such computer, computer system or computer network;

(b) Downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
(d) Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any computer, computer system or computer network;

(f) Denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.—For the purposes of this section,—

(i) "Computer contaminant" means any set of computer instructions that are designed—

(a) To modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) By any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that
are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, or instruction is executed or some other event takes place in that computer resource;

(iv) "Damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

S.44. Penalty for failure to furnish information return, etc.

S.45. Residuary penalty.

S.46. Power to adjudicate.

S.47. Factors to be taken into account by the adjudicating officer.

CHAPTER X

The Cyber Regulations Appellate Tribunal


S.49. Composition of Cyber Appellate Tribunal.

S.50. Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal.

S.51. Term of office
S.52. Salary, allowances and other terms and conditions of service of Presiding Officer.

S.53. Filling up of vacancies.

S.54. Resignation and removal.

S.55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.

S.56. Staff of the Cyber Appellate Tribunal.

S.57. Appeal to Cyber Appellate Tribunal.

S.58. Procedure and powers of the Cyber Appellate Tribunal.

S.59. Right to legal representation.

S.60. Limitation.

S.61. Civil court not to have jurisdiction.

S.62. Appeal to High Court.

S.63. Compounding of contraventions.

S.64. Recovery of penalty

CHAPTER XI

OFFENCES

S.65. Tampering with computer source documents.

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any
computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.—For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

S.66. Hacking with computer system.

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

S.67. Publishing of information which is obscene in electronic form.

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.
S.65. Tampering with computer source documents.

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.—For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and Programme analysis of computer resource in any form.

S.66. Hacking with computer system.

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

S.67. Publishing of information which is obscene in electronic form.

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to
five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

S.68. Power of Controller to give directions.

S.69. Directions of Controller to a subscriber to extend facilities to decrypt information.

S.70. Protected system.

S.71. Penalty for misrepresentation.

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be. shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

S.72. Penalty for breach of confidentiality and privacy.

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

S.73. Penalty for publishing Digital Signature Certificate false in certain particulars.
S.74. Publication for fraudulent purpose.

S.75. Act to apply for offence or contravention committed outside India.

S.76. Confiscation.

S.77. Penalties or confiscation not to interfere with other punishments.

S.78. Power to investigate offences.

CHAPTER XII

NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

S.79. Network service providers not to be liable in certain cases.

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation.—For the purposes of this section, —

(a) "Network service provider" means an intermediary;

(b) "Third party information" means any information dealt with by a network service provider in his capacity as an intermediary;

CHAPTER: XIII
Miscellaneous

S.80. Power of police officer and other officers to enter, search, etc.

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act

Explanation.—For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

S.81. Act to have overriding effect.

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

S.82. Controller, Deputy Controller and Assistant Controllers to be public servants.
S.83. Power to give directions.

S.85. Offences by companies.

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation.—For the purposes of this section,—

(i) "Company" means any body corporate and includes a firm or other association of individuals; and

(ii) "Director", in relation to a firm, means a partner in the firm.
S.86. Removal of difficulties.

S.87. Power of Central Government to make rules.


S.89. Power of Controller to make regulations.

S.90. Power of State Government to make rules.

Enabling provisions:

The preamble of the Act mentions that the purpose of this Act is “to provide legal recognition of transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as “electronic commerce”, which involve the alternatives to paper based methods of communication and storage of information; facilitate electronic filing of documents with Governmental agencies; to usher in the field of modern methods of commercial activities, it was considered essential as a first step to give legal recognition to the electronic transactions alternative to paper-based transactions. With the above purpose in view, S.4, S.5, S.6, S.7 and S.8 of the Information Technology Act, 2000 recognises digital signature, Electronic Security, Electronic Publication by the way of an Electronic Gazette. These enabling provisions of the Act has paved way for the amendment of other Acts. They are:-

1. Amendment to The Indian Penal Code, 1860 [45 of 1860]: Sections 29, 167, 172, 173, 175, 192, 204, 463, 464, 466, 468, 470, 471, 476 and 477-A have been amended vide S.91 of the Act, and has been mentioned in the First Schedule of the Act.

2. Amendments to the Indian Evidence Act, 1872: Sections 3, 17, 22, 34, 35, 39, 47, 59, 65, 67, 73, 81, 85, 88, 89 and 131, vide S.92 of
the IT Act, 2000 and has been mentioned in the Second Schedule of the Act.

3. **The Bankers Book of Evidence Act, 1891**: Section 2 of the Act has been amended by S.93 of the IT Act, 2000 and has been indicated in the Third Schedule of the Act.

4. **The Reserve Bank of India Act of 1934**: Section 58 of the Act has been amended vide Sec.94 of the Act and has been mentioned in the Fourth Schedule of the Act.