CYBER CRIMES AND EFFECTIVENESS OF LAWS IN INDIA TO CONTROL THEM

Mubashshir Sarshar, National Law University, Delhi
CYBER CRIMES AND EFFECTIVENESS OF LAWS TO CONTROL THEM

National Law University, Delhi

1 Mubashshir Sarshar, Student at National Law University, Delhi
# Table of Contents

List of Abbreviation i
List of Statutes ii
List of Cases iii

## CHAPTER – I
**INTRODUCTION** 1

- Research Methodology
- Research questions
- Hypothesis

## CHAPTER – II
**CYBER CRIMES - A BROAD CATEGORISATION** 6

- Cybercrimes against persons
- Cybercrimes against property
- Cybercrimes against government

## CHAPTER – III
**THE VARIOUS KINDS OF CYBER CRIMES** 9

- Hacking
- Virus, Trojans and Worms
- Cyber Pornography
- Cyber Stalking
- Cyber Terrorism
- Cybercrimes related to finance
- Cybercrimes involving mobile and wireless technology
- Phishing
- Denial of Service Attacks (DoS Attacks)
- Email bombing
- Email spoofing
- Data Diddling
- Salami Attacks
- Logic Bombs
- Internet time theft
- Web Jacking

## CHAPTER – IV
**THE HIGH TECH CRIMINALS** 18

- Black Hat hackers
CHAPTER – V ESSENTIAL PRE-REQUISITES OF AN EFFECTIVE CYBER LAW 22

CHAPTER – VI THE INFORMATION TECHNOLOGY ACT, 2000 24

- Advantages
- Disadvantages
- The recent proposed amendments in the IT Act, 2000

CHAPTER – VII SOME IMPORTANT CASES CONCERNING CYBER LAW IN INDIA 29

- Ritu Kohli case
- State of Maharashtra v. Anand Ashok Khare
- State of UP v. Saket Sanghania
- State v. Amit Prasad
- State of Chattisgarh v. Prakash Yadav and Ors
- State of Delhi v. Aneesh Chopra
- The Arzika Case
- The Air Force Bal Bharti School Case
- State of Tamil Nadu v. Dr. L. Prakash
- Arif Azim Case

CHAPTER – VIII INTERNATIONAL ORGANISATIONS BATTLING CYBER CRIME 32

- The United Nation
- The Council of Europe
- The European Union
- ASEAN
- APEC
- G-8 States

CHAPTER – IX CONCLUSION 35

BIBLIOGRAPHY iv
List of Abbreviations

§. Section
AIR All India Report
Art. Article
Ed. edition
ILR Indian Law Report
p. page
Rev. revised
s. Section
U.S. United States of America
UETA United Electronic Transaction Act
UK United Kingdom
Vol. Volume
Vol. volume
WTO World Trade Organization
List of Statutes

Indian Telegraph Act.

The Information Technology Act, 2000

UNICITRAL Model Laws
List of Cases

State of Chattisgarh v. Prakash Yadav and Manoj Singhania

State of Delhi v. Aneesh Chopra

State of Maharashtra v. Anand Ashok Khare

State of Tamil Nadu v. Dr L. Prakash

State of Uttar Pradesh v. Saket Sanghania

State v. Amit Prasad
CHAPTER – I

INTRODUCTION

The modern thief can steal more with a computer than with a gun. Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb


In the present era of rapid growth, information technology is encompassing all walks of life all over the world. These technological developments have made the transition for paper to paperless transaction possible. We are now creating new standards of speed, efficiency and, accuracy in communication, which has become key tools for boosting innovations, creativity and increasing overall productivity. Computers are extensively used in the storage of confidential data of political, social and economic or personal nature which are of immense benefit to the society.

The use of Computers is increasingly spreading, and more and more users are connecting to the internet. The internet is a source for almost anybody to access, manipulate and destroy other’s information. The rapid development of the Internet and computer technology globally has also led to the growth of new forms of transnational crimes especially those which are internet related. These criminal activities directly relate to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored data, or sabotage of systems and data. Characteristic feature of these crimes are that these crimes are considered as illegal, unethical or unauthorized behaviour of people relating to the automatic processing and transmission of data by the use of Computer Systems and Networks. These crimes have virtually no boundaries and may affect any country across the globe within a fraction of second. Ways of tackling cyber crimes through legislation may vary from one country to another, especially when cyber crimes occur within a specific national jurisdiction with different definition and socio-political environment.

Cybercrime spans not only state but national boundaries as well. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop

---

devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

Firstly, cybercrime in a narrow sense is any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them. And, secondly cybercrime in a broader sense is any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession offering or distributing information by means of a computer system or network.³

Cyber Crime is the latest type of crime which affects many people. It refers to the criminal activities taking place in computer or computer networks, intentionally access without permission, alters, damages, deletes and destroys the database available on the computer or network, and also includes access without permission on a database or programme of a computer in order to devise or execute any unlawful scheme or wrongfully control or obtain money, property or data. It poses the biggest challenge for the Police, Prosecutors and legislators. Crimes of this nature are usually indulged in by young teens, recreational computer programmers and persons having vested interest. Cyber crime in its most practiced form includes offences such as tampering with the source code of a programme, hacking into computer systems, publication of obscene information and misuse of licences and digital signatures. The problem is multifold as it covers the crime related to economy as well as other crimes such as pornography which has its basis in certain moral standards and uses parameters like indecency and obscenity.⁴

In a day and age where everything from a microwave oven to nuclear plants run on computer and computer programmes, Cyber crimes has assumed a rather sinister implication. Life is about a mix of good and evil. So is the internet. For all the good it does to us, Cyber crimes have its dark side too. Unlike conventional crimes though, there is no policeman patrolling the information superhighway, leaving it open to everything from Trojan horses and Viruses to Cyber stalking, trademark counterfeiting and Cyber terrorism.⁵

Enormous amount of money is earned by the Cybercriminals, either by causing huge damage to the computer systems or by stealing information which is marketable or by way of some foul play through the network. The question here is what constitutes a computer crime and

---
⁵ Laura E. Quarantiello, CYBER CRIME: HOW TO PROTECT YOURSELF FROM COMPUTER CRIMINALS. Tiare Publications, 1996.
how can it be distinguished from routine crime. The query has no legal answer because in India neither the IT Act, 2000 nor the Indian Penal Code gives any precise or concise definition for the same. However some recent changes in the IPC provides punishments to certain acts without making any specific reference to computers. This create a lot of imbroglio in the minds of cyber users because of the confusion arising out of how any rule or doctrine should be made applicable in case of infringements or violations made by parties within the country and outside.

One of the critical issues in the cyber era is the matter of jurisdiction, which is the authority of a court to hear a case and resolve a dispute within a sovereign territory. Because the legal establishment of e-commerce has no geographical boundaries, it establishes immediate long-distance communications with anyone who can access the internet. For example, an online e-merchant has no way of knowing where the information on its site is being accessed. Hence, the issue of jurisdiction is of primary importance in cyberspace. Engaging in e-commerce on the internet may expose the company to the risk of being sued in any State or foreign country, where an internet user can establish a legal claim. In consideration of all these issues under the scope of cyber-crimes subject to each country's jurisdiction and their impacts on global socio-economy beyond the jurisdiction, we may need to be more aware of them and take appropriate legislative measures to govern the cyber world before it is too late. In order to achieve this end many countries of the world including India have enacted Laws related to Information Technology, these laws have been usually termed as Cyber Laws.⁶

Cyber law is a term used to describe the legal issues related to the use of communications technology, particularly ‘cyber-space’ It is a less distinct field of law in the way that property or contract are, as it is an inter-section of many fields, including intellectual property, privacy, freedom of expression and jurisdiction. In essence, Cyber law is an attempt to integrate the challenges presented by human activity on the internet with legacy system of laws applicable to the physical world. Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber law is a very technical field and that it does not have any bearing activities in Cyberspace, but the actual truth is remotely different.⁷

---

⁷ www.cybercrimelaw.net/content/history.html.
When the Internet was developed, its founding fathers hardly had any inclination that the internet could transform itself into an all pervading revolution which could be misused for criminal activities and which would require regulation. Today however the situation is quite different and due to the anonymous nature of the internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence, there has been felt the need for cyber laws in India.

Keeping this in mind, in May 2000, both houses of the Indian Parliament passed the Information Technology Bill. The bill received the assent of the President in August 2000, and came to be known as the Information Technology Act, 2000. Cyber laws are contained in this IT Act and it aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India.

Cyber crimes and attacks cost Indian companies Rs 58 lakh in revenue in 2009 and affected over 66% of Indian enterprises, according to a study by internet security providers, Symantec Corp.

According to the findings on India in the research titled 2010 State of Enterprise Security, over and above these revenue losses, Indian enterprises also lost an average of Rs 94.56 lakh in organisation, customer and employee data, and an average of Rs 84.57 lakhs in productivity costs last year. Protecting information today is more challenging than ever. By putting in place a security blueprint that protects their infrastructure and information, enforces IT policies, and manages systems more efficiently, businesses can increase their competitive edge in today’s information-driven world.

The study further found that close to half of the of Indian Enterprises saw cyber security as their top issue, rating it above threats from natural disasters, terrorism and traditional crime combined. With the rate of attacks increasing in several organizations, a sizeable chunk of the companies said that the nature of cyber attacks consisted of external threats as well as internal threats and negligence.

RESEARCH METHODOLOGY:

The doctrinal method has been adopted for this research under the supervision of Professor (Dr.) Seshan Radha. The researcher has consulted Bare Act, books, websites, cases, articles and journals for conducting the research attained from National Law University Library and resources from the World Wide Web.

RESEARCH QUESTION

(i) Is the Information Technology Act, 2000 effective and efficient enough for controlling the recent developments in Cyber Crimes in India?

(ii) Will the recent proposed amendment to the Information Technology Act, 2000 answer the contemporary complications in the cyber crime arena in India?

HYPOTHESIS

(i) No

(ii) No
CHAPTER – II

CYBER CRIMES- A BROAD CATEGORISATION

According to the researcher, Cybercrimes can be basically divided into 3 major categories:

- Cybercrimes against persons.
- Cybercrimes against property.
- Cybercrimes against government

Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be amplified. This is one Cybercrime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled. Cyber-harassment is a distinct Cybercrime. Various kinds of harassment can and do occur in cyberspace, or through the use of cyberspace. Harassment can be sexual, racial, religious, or other. Persons perpetuating such harassment are also guilty of cybercrimes. Cyber-harassment as a crime also brings us to another related area of violation of privacy of citizens. Violation of privacy of online citizens is a Cybercrime of a grave nature. No one likes any other person invading the invaluable and extremely touchy area of his or her own privacy which the medium of internet grants to the citizen.

The second category of Cyber-crimes is that of Cybercrimes against all forms of property. These crimes include computer vandalism (destruction of others' property), transmission of harmful programmes. There are numerous examples of such computer viruses few of them being "Melissa" and "love bug", which appeared on the internet in March of 1999. It spread rapidly throughout computer systems in the United States and Europe. It is estimated that the virus caused 80 million dollars in damages to computers worldwide. Companies lose much money in the business when the rival companies, steal the technical database from their computers with the help of a corporate cyberspy.
The third category of Cyber-crimes relate to Cybercrimes against Government. Cyber-terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorise the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website. it was said that internet was becoming a boon for the terrorist organisations. Cracking is amongst the gravest Cyber-crimes known. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information. Coupled with this the actuality is that no computer system in the world is cracking proof. It is unanimously agreed that any and every system in the world can be cracked. The recent denial of service attacks seen over the popular commercial sites like E-bay, Yahoo, Amazon and others are a new category of Cyber-crimes which are slowly emerging as being extremely dangerous.  

The Ten Commandments of Cyber Ethics

1. Thou shalt not use a computer to harm other people.  
2. Thou shalt not interfere with other people's computer work.  
3. Thou shalt not snoop around in other people's computer files.  
4. Thou shalt not use a computer to steal.  
5. Thou shalt not use a computer to bear false witness.  
6. Thou shalt not copy or use proprietary software for which you have not paid.  
7. Thou shalt not use other people's computer resources without authorization or proper compensation.  
8. Thou shalt not appropriate other people's intellectual output.  
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.  

---

12 The Computer Ethics Institute, a leader in the field, has comprised a guideline to help computer users in their ethical decisions. They have called this guideline “The Ten Commandments”.

10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.
CHAPTER – III

THE VARIOUS KINDS OF CYBER CRIMES

Cyber crimes involve a modification of a conventional crime by using computers. Following is a comprehensive list of the various types of Crimes which have been committed in the recent times.

HACKING

‘Hacking’ means unauthorized access to a computer system.\textsuperscript{13} It is the most common type of Cyber crime being committed across the world. The word ‘hacking’ has been defined in section 66 of the Information Technology Act, 2000 as follows, “whoever with the intent to cause or knowingly 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 hacking”
Punishment for hacking under the above mentioned section is imprisonment for three years or fine which may extend up to two lakh rupees or both.\textsuperscript{14}

VIRUS, TROJANS AND WORMS

A computer virus is a programme designed to replicate and spread, generally with the victim being oblivious to its existence. Computer viruses spread by attaching themselves to programme like word-processors or spreadsheets or they attach themselves to the boot sector of a disk. Thus when an infected file is activated, the virus itself is also executed.\textsuperscript{15}

Trojan horse is defined a “malicious, security-breaking program that is disguised as something benign” such as a directory lister, archiver, game, or a programme to search or destroy viruses.\textsuperscript{16}

\textsuperscript{13} Section 66 of Information Technology Act, 2000.
\textsuperscript{14} Ibid.
\textsuperscript{16} The word ‘Trojan Horse’ is generally attributed to Daniel Edwards of the NSA. He is given the credit for identifying the attack form in the report ‘Computer Security Technology Planning Study’
A computer worm is a self contained program that is able to spread functional copies of itself or its segments to other computer systems. Unlike viruses, worms do not need to attach themselves to a host program.\textsuperscript{17}

**CYBER PORNOGRAPHY**

The growth of technology has flip side to it causing multiple problems in everyday life. The Internet has provided a medium for the facilitation of crimes like pornography. Cyber porn as it is popularly known is widespread. Almost 50\% of the websites exhibit pornographic material today. Pornographic materials can also be reproduced more quickly and cheaply on new media like hard disks and cd-roms. The new technology is not merely limited to texts and images but have full motion video clips and movies too. These have serious consequences and have result in serious offences which have universal disapproval like child pornography which are far easier for offenders to hide and propagate through the medium of the internet.\textsuperscript{18}

**CYBER STALKING**

Cyber stalking can be defined as the repeated acts harassment or threatening behaviour of the cyber criminal towards the victim by using the internet services. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously. It all depends on the course of conduct of the stalker. Cyber Stalking is a problem which many people especially young teenage girls complain about.\textsuperscript{19}

**CYBER TERRORISM**

Cyber terrorism may be defined to be “the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives”.\textsuperscript{20}

The role of computer with respect to terrorism is that a modern thief can steal more with a computer than with a gun and a future terrorist may be able to cause more damage with a keyboard than with a bomb. No doubt, the great fears are combined in terrorism, the fear of

\textsuperscript{17}http://cybercrime.planetindia.net/worms.htm
\textsuperscript{19}Dudeja V D, CRIMES IN CYBERSPACE- SCAMS AND FRAUDS (ISSUES AND REMEDIES)
\textsuperscript{20}http://www/fbi.gov/quickfacts.htm
random, violent, victimisation segues well with the distrust and out of fear of computer technology. Technology is complex, abstract and indirect in its impact on individual and it is easy to distrust that which one is not able to control. People believe that technology has the ability to become the master and humanity its servant.\textsuperscript{21}

**CYBER CRIME RELATED TO FINANCE**

There are various types of Cyber Crimes which are directly related to financial or monetary gains by illegal means. To achieve this end, the persons on the cyber world who could be suitably called as fraudsters uses different techniques and schemes to befool other people on the internet. Online fraud and cheating is one the most lucrative businesses that are growing today in the cyberspace. It may assume different forms. Some of the cases of online fraud and cheating have come to light are pertaining to credit-card crimes, contractual crimes, online auction frauds, online investment schemes, job offerings, etc.\textsuperscript{22}

**CYBER CRIMES INVOLVING MOBILE AND WIRELESS TECHNOLOGY**

At present the mobile technology has developed so much that is becomes somewhat equivalent to a personal computer. There is also increase in the services which were never available on mobile phones before, such as mobile banking, which is also prone to cyber crimes. Due to the development in the wireless technology the cyber crimes on the mobile device is coming at par with the cyber crimes on the net day by day.\textsuperscript{23}

**PHISHING**

In computing, phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit cards, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message.\textsuperscript{24} The term phishing arises from the use of increasingly sophisticated lures to a ‘fish’ for users’ financial information and passwords.\textsuperscript{25} The act of

\textsuperscript{22} US Department of Justice, Criminal Division, Fraud Section, http://www.usdoj.gov/criminal/fraud/internet.
\textsuperscript{23} http://www/trai.gov.in
\textsuperscript{24} Lance James, Phishing Exposed, Elsevier 2005.
\textsuperscript{25} Tan, Koon. Phishing and Spamming via IM. Internet Storm Center. December 5\textsuperscript{th}, 2006.
sending an email to a user falsely claiming to be an established and legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security no. and bank account no. that the legitimate organization already has. The website, however is bogus and is setup only to steal the user’s information. By spamming large group of people, the ‘phisher’ counted on the email being read by a percentage of people who actually had listed credit cards numbers with legitimacy. Phishing also refers to a brand spoofing or carding, is a variation on ‘fishing’, the idea being that the bait is thrown out with the hope that while most will ignore the bait, some will be tempted into biting it. With the growing no. of reported phishing incidents, additional methods of protection are needed. Attempts include legislation, user training and technical measures. More recent phishing attempts have started to target the customers of banks and online payment services. While the first such example are sent indiscriminately in the hope of finding a customer of a given bank or service, recent research has shown that phishers may in principle be able to establish what bank a potential victim has a relation with, and then sends an appropriate spoofed email to the victim. In general such targeted versions of phishing have been termed as spear phishing.

DENIAL OF SERVICE ATTACKS (DoS ATTACK)

This is an act by a criminal who floods the bandwidth of the victim’s network or fills his email box with spam mail depriving him of the service he is entitled to access or provide. Short for denial-of-service attack, a type of service attack on a network which is designed to bring the network down to its knees by flooding it with useless traffic. Many DoS attack such as Ping of Death and Teardrop attack, exploit limitation in the TCP/IP protocols. For all known DoS attacks, there are softwares fixes that system administrators can install to limit the damage.

29 A Ping of Death is type of attack on a computer network that involves sending a malformed or otherwise malicious ping. A ping is normally of 64 bytes in size. Sending a ping which is larger than the maximum IP packet size can crash the target computer.
30 A tear drop attack is a DoS attack where fragmented packets are forged to overlap each other when the receiving host tries to reassemble them.
caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by hackers. This involves flooding computer resources with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. \(^{31}\) Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim’s computer, exceeding the limit that the victim’s server can support and making the servers crash. Denial-of-service attacks have had an impressive history in the past and have brought down websites like the Amazon, CNN, Yahoo and eBay.

**EMAIL BOMBING**

In internet usage, an email-bomb is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox. \(^{32}\) Mailbombing is the act of sending an email bomb, a term shared with the act of sending actual exploding devices. There are two ways of e-mail bombing, mass mailing and list linking. Mass mailing consists of sending numerous duplicate mails to the same email ID. These types of mail bombers are simple to design, but due to their extreme simplicity they can be easily filtered by spam filters. List linking on the other hand, consists of signing a particular email ID up to several subscriptions. This type of bombing is effective as the person has to unsubscribe from all the services manually. In order to prevent this type of bombing most type of services send a confirmation to the mailbox when we register for the subscription on a particular website.

E-mail spamming is a variant of bombing; it refers to sending email to hundreds or thousands of users. E-mail spamming can be made worse of the recipients reply to the email, causing all the original addresses to receive the reply. \(^{33}\)

**EMAIL SPOOFING**

E-mail spoofing is a term used to describe fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. Email spoofing is a technique commonly used for spam email and

---


\(^{32}\) [http://www.cert.org/tech_tips/e-mail_bombing_spamming.html.](http://www.cert.org/tech_tips/e-mail_bombing_spamming.html)

\(^{33}\) [http://www.lse.ac.uk/itservices/help/spamming&spoofing.htm.](http://www.lse.ac.uk/itservices/help/spamming&spoofing.htm)
phishing to hide the origin of an email message. By changing certain properties of the email, such as the From, Return-Path and Reply-To fields, ill-intentioned users can make the email appear to be from someone other than the actual sender. It is often associated with website spoofing which mimic an actual well-known website but are run by other party either with fraudulent intentions or as a means of criticism of the organisation’s activities. It is forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual code. Distributors of spam often use spoofing in an attempt to get recipient to open, and possibly respond to such solicitations. Spoofing can be used legitimately. Classic examples of senders who might prefer to disguise the source of the email include a sender reporting mistreatment by a spouse to a welfare agency or a “whistle blower” who fears retaliation. However, spoofing anyone other than yourself is illegal in many jurisdictions.³⁴

Email spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending email, does not allow a authentication mechanism. Although an SMTP service extension allows an SMTP client to negotiate a security level with a mail server, however this precaution is not always taken.

If the precaution is not taken, anyone with the requisite knowledge can connect to the server and use it to send messages. To send spoofed messages, senders insert commands in headers that alters the message information. It is possible to send a message that appears from anyone and anywhere, saying whatever the sender wants to say.³⁵

DATA DIDDLING

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, or a virus that changes data, or the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved the process of creating, recording, encoding, examining, checking, converting or transmitting data.³⁶ This kind of an attack involves altering raw data just before it is processed.

³⁴ Tom Merritt, What is Email Spoofing? See www.g4tv.com.
³⁵ http://www.mailsbroadcast.com/e-email.broadcast.faq/46.e-mail.spoofing.htm.
by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing, the cost can be considerable. To deal with this crime, a company must implement policies and internal controls. This may include performing regular audits, using softwares with built in features to combat such problems, and supervising employees.

SALAMI ATTACKS

A salami attack is a series of minor data-security attack that together result in a larger attack. For example, a fraud activity in a bank, where an employee steals a small amount of funds from several accounts, can be considered a Salami Attack. Crimes involving salami attacks are typically difficult to detect and trace. These attack are used for commission of financial crimes. These key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program into the bank servers that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount each month.

To cite an example, an employee of a bank in USA was dismissed from his job. Disgruntled at having been mistreated by his employers, he introduced a program into the bank systems. This program was programmed to take ten cents from all accounts in the bank and put them into the account of the person whose name was alphabetically the last name in the bank’s rosters. Then he went and opened an account in the name of ‘Ziegler’. The amount being withdrawn from each of the accounts in the bank was so insignificant that neither the account holders nor the bank officials noticed the fault. It was brought to their notice when a person by

37 [http://www.cyberpolicebangalore.nic.in/cybercrimes.htm](http://www.cyberpolicebangalore.nic.in/cybercrimes.htm)
38 David Bowen, Viruses, Worms and Other Nasties, Protecting yourself online; Department of Interdisciplinary Studies, 2003.
the name of ‘Zygler’ opened his account in that bank. He was surprised to find a sizable amount of money being transferred into his account every Saturday.\(^{41}\)

From a systems development standpoint, such scams reinforce the critical importance of sound quality assurance throughout the software development life cycle.\(^{42}\)

**LOGIC BOMBS**

A logic bomb is a programming code, inserted surreptitiously or intentionally and which is designed to execute under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command.\(^{43}\) Softwares that is inherently malicious, such as viruses and worms, often contains logic bombs that execute a certain payload at the pre-defined time or when some other conditions are met. Many viruses attack their hosts systems on specific days, e.g. Friday the 13\(^{\text{th}}\) and April fool’s day logic bombs. A logic bomb when exploded may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects.\(^{44}\)

Some logic bombs can be detected and eliminated before they execute through a periodic scan of all computer files, including compresses files, with an up to date anti-virus program. For best results, the auto-protect and email screening functions should be activated by the user whenever the machine is online. A logic bomb can also be programmed to wait for a certain message from the programmer. However in some ways a logic bomb is the most civilized programmed threat, because it targeted against a particular victim. The classic use of a logic bomb is to ensure the payment for software. If payment is not made by a certain date, the logic bomb gets activated and the software automatically deletes itself.

**INTERNET TIME THEFT**

Theft of Internet hours refers to using someone else’s internet hours. Secion 43 (h) of the IT Act, 2000 lays down civil liability for this offence. It reads as , whosoever without the permission of the owner or any other person who is in charge a computer system or computer network, charges the service availed of by a person to the account of another person by

\(^{42}\) B. Michael Hale, Salami Attacks, http://all.net/CID/Attack/papers/Salami2.html.  
tampering with or manipulating any computer, computer systems or network is liable to pay damages not exceeding one crore to the person in office.45

In the Colonel Bajwa’s case46, the economic offences wing, IPR section crime branch of Delhi Police registered its first case involving theft of internet hours. In this case, the accused, Mukesh Gupta, an engineer with Nicom System (p) Ltd was sent to the residence of the complainant to activate internet connection. However, the accused used Col. Bajwa’s login name and password from various places causing wrongful loss of 100 hours to him.

Initially the Police could not believe that time could be stolen. They were not aware of the concept of time theft at all and his report was rejected. He decided to approach the Times of India, New Delhi which in turn carried a report on the inadequacy of the Delhi Police in handling Cyber crimes. The Commissioner of Police, then took the case in his own hands and the Police then registered a case under Section 379, 411, 34 of the IPC and section 25 of the Indian Telegraph Act.

WEB JACKING

This term is derived from the term hijacking. This occurs when someone forcefully takes control of a website by cracking the password and then changing it. The actual owner of the website does not have any control over what appears on that website.47 In a recent incident reported in USA, the owner of a hobby website for children received an email informing her that a group of hackers had gained control over her website. The owner did not take the threat seriously. Three days later she came know from phone calls from across the globe that the hackers had web jacked her website. Subsequently they had altered a portion of text in the website which said ‘How to have fun with a goldfish’ to ‘how to have fun with pirhanas’. Many children believed the content of the website and unfortunately were seriously injured as they tried playing with the pirhanas which they bought from pet shops.48

45 Section 43 of the IT Act, 2000.
CHAPTER – IV

THE HIGH-TECH CRIMINALS

Cyber crime has become a profession and the demographic of your typical cyber criminal is changing rapidly, from bedroom-bound geek to the type of organized gangster more traditionally associated with drug-trafficking, extortion and money laundering. It has become possible for people with comparatively low technical skills to steal thousands of pounds a day without leaving their homes. In fact, to make more money than can be made selling heroin, the only time the criminal need leave his PC is to collect his cash. Sometimes they don't even need to do that. The rise of cyber crime is inextricably linked to the ubiquity of credit card transactions and online bank accounts. Get hold of this financial data and not only can you steal silently, but also through a process of virus-driven automation with ruthlessly efficient and hypothetically infinite frequency.\(^{49}\)

Out of the pool of these hi-tech cyberpunks, the most prominent and well-known ones are known as hackers. Until the 1980s, all people with a high level of skills at computing were known as "hackers". A group that calls themselves hackers refers to "a group that consists of skilled computer enthusiasts". Over time, the distinction between those perceived to use such skills with social responsibility and those who used them maliciously or criminally became perceived as an important divide. The general public tends to use the term "hackers" for both types, a source of some conflict when the word is perceived to be used incorrectly; for example Linux has been criticised as "written by hackers". In computer jargon the meaning of "hacker" can be much broader. Now, these are broadly classified under three broad categories.

- Black Hat Hackers
- White Hat Hackers
- Grey Hat Hackers

A black hat Hacker is a person who compromises the security of a computer system without permission from an authorized party, typically with malicious intent. Usually, a black hat is a person who uses their knowledge of vulnerabilities and exploits for private gain, rather than

---

revealing them either to the general public or the manufacturer for correction. Many black hats hack networks and web pages solely for financial gain. Black hats may seek to expand holes in systems; any attempts made to patch software are generally done to prevent others from also compromising a system they have already obtained secure control over. A black hat hacker may write their own zero-day exploits, which is private software that exploits security vulnerabilities. The general public does not have access to 0-day exploits. In the most extreme cases, black hats may work to cause damage maliciously, and/or make threats to do so as extortion.

A white hat hacker, also rendered as ethical hacker, is, in the realm of information technology, a person who is ethically opposed to the abuse of computer systems. Realization that the Internet now represents human voices from around the world has made the defense of its integrity an important pastime for many. A white hat generally focuses on securing IT systems, whereas a black hat would like to break into them. The term white hat hacker is also often used to describe those who attempt to break into systems or networks in order to help the owners of the system by making them aware of security flaws, or to perform some other altruistic activity. Many such people are employed by computer security companies; these professionals are sometimes called sneakers. Groups of these people are often called tiger teams.

A Grey Hat in the computer security community, refers to a skilled hacker who sometimes acts legally, sometimes in good will, and sometimes not. They are a hybrid between white and black hat hackers. They usually do not hack for personal gain or have malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits. One reason a grey hat might consider himself to be grey is to disambiguate from the other two extremes: black and white. It might be a little misleading to say that grey hat hackers do not hack for personal gain. While they do not necessarily hack for malicious purposes, grey hats do hack for a reason, a reason which more often than not remains undisclosed. A grey hat will not necessarily notify the system admin of a penetrated system of their penetration. Such a hacker will prefer anonymity at almost all cost, carrying out their penetration undetected and then exiting said system still undetected with minimal damages. Consequently, grey hat penetrations of systems tend to be for far more passive activities such as testing, monitoring, or less destructive forms of data transfer and retrieval.

---

50 http://webzone.k3.mah.se/k3jolo/HackerCultures/origins.htm.
Not all cyber-criminals operate at the coalface, and certainly don’t work exclusively of one another; different protagonists in the crime community perform a range of important, specialized functions. These broadly encompass,

1. Coders – comparative veterans of the hacking community. With a few years' experience at the art and a list of established contacts, ‘coders’ produce ready-to-use tools (i.e. Trojans, mailers, custom bots) or services (such as making a binary code undetectable to AV engines) to the cyber crime labour force – the ‘kids’. Coders can make a few hundred dollars for every criminal activity they engage in.

2. Script Kids – so-called because of their tender age: most are under 18. They buy, trade and resell the elementary building blocks of effective cyber-scams such as spam lists, php mailers, proxies, credit card numbers, hacked hosts, scam pages etc. ‘Kids’ will make less than $100 a month, largely because of the frequency of being ‘ripped off’ by one another.

3. Drops – the individuals who convert the ‘virtual money’ obtained in cyber crime into real cash. Usually located in countries with lax e-crime laws (Bolivia, Indonesia and Malaysia are currently very popular), they represent ‘safe’ addresses for goods purchased with stolen financial details to be sent, or else ‘safe’ legitimate bank accounts for money to be transferred into illegally, and paid out of legitimately.

4. Mobs – professionally operating criminal organizations combining or utilizing all of the functions covered by the above. Organized crime makes particularly good use of safe ‘drops’, as well as recruiting accomplished ‘coders’ onto their payrolls. Gaining control of a bank account is increasingly accomplished through phishing.\(^5\)

The alarming efficiency of cybercrime can be illustrated starkly by comparing it to the illegal narcotics business. One is faster, less detectable, more profitable (generating a return around 400 times higher than the outlay) and primarily non-violent. The other takes months or years to set-up or realise an investment, is cracked down upon by all almost all governments internationally, fraught with expensive overheads, and extremely dangerous.

On top of viruses, worms, bots and Trojan attacks, organizations in particular are contending with social engineering deception and traffic masquerading as legitimate applications

on the network. In a reactive approach to this onslaught, companies have been layering their networks with stand alone firewalls, intrusion prevention devices, anti-virus and anti-spyware solutions in a desperate attempt to plug holes in the armoury. They're beginning to recognize it's a failed strategy. After all, billions of pounds are being spent on security technology, and yet security breaches continue to rise.

To fight cyber crime there needs to be a tightening of international digital legislation and of cross-border law enforcement co-ordination but, there also needs to be a more creative and inventive response from the organisations under threat. Piecemeal, reactive security solutions are giving way to strategically deployed multi-threat security systems. Instead of having to install, manage and maintain disparate devices, organizations can consolidate their security capabilities into a commonly managed appliance. These measures combined, in addition to greater user education are the best safeguard against the deviousness and pure innovation of cyber-criminal activities.
CHAPTER – V

ESSENTIAL PRE-REQUISITES OF AN EFFECTIVE CYBER LAW

The cyber law, in any country of the World, cannot be effective unless the concerned legal system has the following three pre requisites

Firstly, a Sound Cyber Law regime: The Cyber law in India can be found in the form of IT Act, 2000. Now the IT Act, as originally enacted, was suffering from various loopholes and lacunas. These “grey areas” were excusable since India introduced the law recently and every law needs some time to mature and grow. It was understood that over a period of time it will grow and further amendments will be introduced to make it compatible with the International standards. It is important to realise that we need “qualitative law” and not “quantitative laws”. In other words, one single Act can fulfil the need of the hour provided we give it a “dedicated and futuristic treatment”. The dedicated law essentially requires a consideration of “public interest” as against interest of few influential segments. Further, the futuristic aspect requires an additional exercise and pain of deciding the trend that may be faced in future. This exercise is not needed while legislating for traditional laws but the nature of cyber space is such that we have to take additional precautions. Since the Internet is boundary less, any person sitting in an alien territory can do havoc with the computer system of India. For instance, the Information Technology is much more advanced in other countries. If India does not shed its traditional core that it will be vulnerable to numerous cyber threats in the future. The need of the hour is not only to consider the “contemporary standards” of the countries having developed Information Technology standards but to “anticipate” future threats as well in advance. Thus, a “futuristic aspect’ of the current law has to be considered. Now the big question is whether India is following this approach? Unfortunately, the answer is in NEGATIVE. Firstly, the IT Act was deficient in certain aspects, though that was bound to happen. However, instead of bringing the suitable amendments, the Proposed IT Act, 2000 amendments have further “diluted” the criminal provisions of the Act. The “national interest” was ignored for the sake of “commercial expediencies”. The proposed amendments have made the IT Act a “tiger without teeth” and a “remedy worst than malady”.
Secondly, sound enforcement machinery: A law might have been properly enacted and may be theoretically effective too but it is useless unless enforced in its true letter and spirit. The law enforcement machinery in India is not well equipped to deal with cyber law offences and contraventions. They must be trained appropriately and should be provided with suitable technological support.

And, lastly, a sound judicial system: A sound judicial system is the backbone for preserving the law and order in a society. It is commonly misunderstood that it is the “sole” responsibility of the “Bench” alone to maintain law and order. That is a misleading notion and the “Bar” is equally responsible for maintaining it. This essentially means a rigorous training of the members of both the Bar and the Bench. The fact is that the cyber law is in its infancy stage in India hence not much Judges and Lawyers are aware of it. Thus, a sound cyber law training of the Judges and Lawyers is the need of the hour. In short, the dream for an “Ideal Cyber Law in India” requires a “considerable” amount of time, money and resources. In the present state of things, it may take five more years to appreciate its application. The good news is that Government has sanctioned a considerable amount as a grant to bring e-governance within the judicial functioning. The need of the hour is to appreciate the difference between mere “computerisation” and “cyber law literacy”. The judges and lawyers must be trained in the contemporary legal issues like cyber law so that their enforcement in India is effective. With all the challenges that India is facing in education and training, e-learning has a lot of answers and needs to be addressed seriously by the countries planners and private industry alike. E-learning can provide education to a large population not having access to it.52

---

CHAPTER – VI

THE EFFECTIVENESS OF THE CYBER LAW OF INDIA-
THE INFORMATION TECHNOLOGY ACT, 2000

The IT Act, 2000 came at a time when cyber-specific legislation was much needed. It filled up the lacunae for a law in the field of e-commerce. Taking cue from its base-document, i.e. the UNICITRAL Model Law on electronic commerce, adopted in 1996, a law attuned to the Indian needs has been formulated. Apart from e-commerce related provisions, computer crimes and offences along with punishments have been enumerated and defined. The powers of the police to investigate and power of search and seizure, etc have been provided for. However, certain points need a re-working right from the scratch or require revamping.

At the first instance, though the IT Act, 2000 purports to have followed the pattern of the UNICITRAL Model Law on Electronic Commerce, yet what took people by surprise is its coverage not only of e-commerce, but something more, i.e. computer crime and amendments to the Indian Penal Code. The UNICITRAL Model Law did not cover any of the other aspects. Therefore in a way, the IT Act, 2000 has been an attempt to include other issues relating to cyber world as well which might have an impact on the ecommerce transactions and its smooth functioning. Though, that of course is not reflected even from the Statements of Objectives and reasons or the preamble of the Statute. Amendments to the Indian evidence Act are evidently made to permit electronic evidence in court. This is a step in the right direction.

Secondly, a single section devoted to liability of the Network Service Provider is highly inadequate. The issues are many more. Apart from classification of the Network Service provider itself there can be various other instances in which the Provider can be made liable specially under other enactments like the Copyright Act or the Trade Marks Act. However the provision in the IT Act, 2000 devoted to ISP protection against any liability is restricted only to the Act or rules or regulations made there under. The section is not very clear as to whether the protection for the ISP’s extends even under the other enactments.

It has been argued that the Act of this nature would divide the society into digital haves and digital have-nots. This argument is based on the premise that with an extremely low PC penetration, poor Internet connectivity and other poor communication infrastructure facilities, a country like India would have islands of digital haves surrounded by digital have-nots’. Logically speaking, such an argument is untenable as the ‘digital core’ has been expanding horizontally and everyday communication connectivity is rising across India.

There has been a general criticism of the wide powers given to the police under the Act. Fear, specially among cyber café owners, regarding misuse of powers under the IT Act, 2000 is not misplaced. Anyone can be searched and arrested without warrant at any point of time in a public place. But at the same time, the fact that committing a computer crime over the net and the possibility of escaping thereafter is so much more viable, that providing such policing powers check the menace of computer crimes is also equally important. Yet this is no reason for giving draconian powers to the police. For example, interception of electronic messages and emails might be necessary under certain situations but the authorities cannot be given a free-hand in interception as and when they feel. Similarly, we need to enquire and delve deeper into the police power of investigation, search and warrant under the IT Act, 2000 and look for a more balanced solution.

In addition to this, various other Advantages and Disadvantages of the IT Act, 2000 can be attributed which are highlighted below

**ADVANTAGES**

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.

From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects.

Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
Second, Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.

Third, Digital signatures have been given legal validity and sanction in the Act.

Fourth, the Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

Fifth, the Act now allows Government to issue notification on the web thus heralding e-governance.

Sixth, the Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

Seventh, the IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

Eighth, under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

DISADVANTAGES

The IT Law 2000, though appears to be self sufficient, it takes mixed stand when it comes to many practical situations. It loses its certainty at many places like

First, the law misses out completely the issue of Intellectual Property Rights, and makes no provisions whatsoever for copyrighting, trade marking or patenting of electronic information and data. The law even doesn’t talk of the rights and liabilities of domain name holders, the first step of entering into the e-commerce.

Second, the law even stays silent over the regulation of electronic payments gateway and segregates the negotiable instruments from the applicability of the IT Act, which may have
major effect on the growth of e-commerce in India. It leads to make the banking and financial sectors irresolute in their stands.

Third, the act empowers the Deputy Superintendent of Police to look up into the investigations and filling of charge sheet when any case related to cyber law is called. This approach is likely to result in misuse in the context of Corporate India as companies have public offices which would come within the ambit of "public place" under the Act. As a result, companies will not be able to escape potential harassment at the hands of the DSP.

Fourth, internet is a borderless medium, it spreads to every corner of the world where life is possible and hence is the cyber criminal. Then how come is it possible to feel relaxed and secured once this law is enforced in the nation?

Fifth, the Act initially was supposed to apply to crimes committed all over the world, but nobody knows how can this be achieved in practice, how to enforce it all over the world at the same time?

Sixth, the IT Act is silent on filming anyone’s personal actions in public and then distributing it electronically. It holds ISPs (Internet Service Providers) responsible for third party data and information, unless contravention is committed without their knowledge or unless the ISP has undertaken due diligence to prevent the contravention. This is a practically impossible approach.

Further according to the researcher, the recently proposed IT Act, 2000 amendments are neither desirable nor conducive for the growth of ICT in India. They are suffering from numerous drawbacks and grey areas and they must not be transformed into the law of the land. These amendments must be seen in the light of contemporary standards and requirements. Some of the more pressing and genuine requirements in this regard are

1. There are no security concerns for e-governance in India.
2. The concept of due diligence for companies and its officers is not clear to the concerned segments.
3. The use of ICT for justice administration must be enhanced and improved.
4. The offence of cyber extortions must be added to the IT Act, 2000 along with Cyber Terrorism and other contemporary cyber crimes.
5. The increasing nuisance of e-mail hijacking and hacking must also be addressed.
6. The use of ICT for day to day procedural matters must be considered.
7. The legal risks of e-commerce in India must be kept in mind.
8. The concepts of private defence and aggressive defence are missing from the IT Act, 2000.
9. Internet banking and its legal challenges in India must be considered
10. Adequate and reasonable provisions must be made in the IT Act, 2000 regarding “Internet censorship”
11. The use of private defence for cyber terrorism must be introduced in the IT Act, 2000
12. The legality of sting operations (like Channel 4) must be adjudged.
13. The deficiencies of Indian ICT strategies must be removed as soon as possible.
14. A sound BPO platform must be established in India, etc.

The act, on an overall analysis, demonstrates a lack of discussion and incorporation of various issues relating to cyber law. Through the Act has been given the name ‘Information Technology Act’ yet many legal issues like online rights of consumers, privacy concerns, domain names disputes, payment and security- bugbears, etc have not been addressed. Finally, how the act will be implemented by a Court of law and its implementation and flaws in the long run are yet to be tested in the case-specific factual terrain.
CHAPTER – VII

SOME IMPORTANT CASES CONCERNING CYBER-CRIMES IN INDIA

There have been various cases that have been reported in India and which have a bearing upon the growth and revolution of Cyberlaw in India. The present page encapsulates some of the important landmark cases that have impacted the evolution and growth of Cyberlaw jurisprudence in India.

The following are some of the important cases impacting the growth of Cyberlaw in India:

RITU KOHLI CASE

Ritu Kohli Case, being India’s first case of cyber stalking, was indeed an important revelation into the mind of the Indian cyber stalker. A young Indian girl being cyber stalked by a former colleague of her husband, Ritu Kohli’s case took the imagination of India by storm. The case which got cracked however predated the passing of the Indian Cyberlaw and hence it was just registered as a minor offence under Section 509 the Indian Penal Code.

STATE OF MAHARASHTRA V. ANAND ASHOK KHARE

This case related to the activities of the 23-year-old Telecom engineer Anand Ashok Khare from Mumbai who posed as the famous hacker Dr Neuker and made several attempts to hack the Mumbai police Cyber Cell website.

STATE OF UTTAR PRADESH V. SAKET SANGHANIA

This case which was registered under Section 65 of the IT Act, related to theft of computer source code. Saket Singhania an engineer, was sent by his employer to America to develop a software program for the company. Singhania, instead of working for the company, allegedly sold the source code of the programme to an American client of his employer by which his employer suffered losses.
STATE V. AMIT PRASAD

State v/s Amit Prasad, was India's first case of hacking registered under Section 66 of the Information Technology Act 2000. A case with unique facts, this case demonstrated how the provisions of the Indian Cyberlaw could be interpreted in any manner, depending on which side of the offence you were on.

STATE OF CHATTISGARH V. PRAKASH YADAV AND MANOJ SINGHANIA

This was a case registered on the complaint of State Bank of India, Raigarh branch. Clearly a case of Spyware and Malware, this case demonstrated in early days how the IT Act could be applicable to constantly different scenarios.

STATE OF DELHI V. ANEESH CHOPRA

State of Delhi v/s Aneesh Chopra Case was a case of hacking of websites of a corporate house.

THE ARZIKA CASE

Pornography and obscene electronic content has continued to engage the attention of the Indian mind. Cases pertaining to online obscenity, although reported in media, often have not been registered. The Arzika case was the first in this regard.

THE AIR FORCE BAL BHARTI SCHOOL CASE

The Air Force Bal Bharti School case demonstrated how Section 67 of the Information Technology Act 2000 could be applicable for obscene content created by a school going boy.

STATE OF TAMIL NADU V. DR L. PRAKASH

State of Tamilnadu v/s Dr L. Prakash was the landmark case in which Dr L. Prakash was sentenced to life imprisonment in a case pertaining to online obscenity. This case was also landmark in a variety of ways since it demonstrated the resolve of the law enforcement and the judiciary not to let off the hook one of the very educated and sophisticated professionals of India.
ARIF AZIM CASE

Arif Azim case was India's first convicted cyber crime case. A case pertaining to the misuse of credit cards numbers by a Call Center employee, this case generated a lot of interest. This was the first case in which any cyber criminal India was convicted. However, keeping in mind the age of the accused and no past criminal record, Arif Azim the accused was sentenced to probation for a period of one year.
CHAPTER – VIII

INTERNATIONAL ORGANISATIONS BATTLING CYBERCRIME

The global world network which united millions of computers located in different countries and opened broad opportunities to obtain and exchange information, is used for criminal purpose more often nowadays. The introduction of electronic money and virtual banks, exchanges and shops became one of the factors of the appearance of a new kind of crime-transnational computer crimes. Today law enforcements face tasks of counteraction and investigation of crimes in a sphere of computer technologies and cyber crimes. Still, the definition of cyber crimes remains unclear to law enforcement, through criminal action on the Internet pose great social danger. Transnational characters of these crimes give the ground today in the development of a mutual policy to regulate a strategy to fight cyber crime.54

One of the most serious steps to regulate this problem was the adoption of Cyber Crimes Convention by European Council on 23rd November 2001, the first ever agreement on juridical and procedural aspects of investigating and cyber crimes. It specifies efforts coordinated at the national and international levels and directed at preventing illegal intervention into the work of computer systems. The convention stipulates actions targeted at national and international level, directed to prevent unlawful infringement of computer systems functions. The convention divides cyber crimes into four main kinds: hacking of computer systems, fraud, forbidden content and breaking copyright laws.55

By ways and measures these crimes are specific, have high latency and low exposure levels. There is another descriptive feature of these crimes, they are mostly committed only with the purpose to commit other more gravy crimes, for example, theft from bank accounts, getting restricted information, counterfeit of money or securities, extortion, espionage, etc.56

There are various initiatives taken by the organization worldwide from time to time to control the growing menace of cyber crime. Some of the initiatives taken by various organizations are-

---

54 Vladimar Golubev, International cooperation in fighting cybercrime; Computer Crime research Center.
THE UNITED NATION

A resolution on combating the criminal misuse of information technologies was adopted by the General Assembly on December 4th, 2000\(^{57}\) (A/res/55/63),\(^ {58}\) including the following

(a) States should ensure that their laws and practice eliminates safe havens for those who criminally misuse information technologies.

(b) Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalised.

THE COUNCIL OF EUROPE

Convention on Cyber Crime of 2001 is a historic milestone in the combat against cyber crime. Member states should complete the ratification and other states should consider the possibility of acceding to the convention or evaluate the advisability of implementing the principles of the convention. The council of Europe established a Committee of experts on crime in Cyber-space in 1997. The committee prepared the proposal for a convention on Cyber-crime, and the Council of Europe convention on Cyber Crime was adopted and opened for signatures at a conference in Budapest, Hungary in 2001. The total no. of ratifications/accessions at present is 21.\(^ {59}\)

THE EUROPEAN UNION

In the European Union, the Commission of the European Communities presented on April 19, 2002 was a proposal for a council framework decision on attacks against information systems. The proposal was adopted by the Council in 2005 and includes Article 2: Illegal access to Information Systems, Article 3: Illegal Systems Interference and Article 4: Illegal Data Interference.

---


\(^{59}\) Albania, Armenia, Bulgaria, Bosnia, Croatia, Cyprus, Denmark, France, Hungary, Netherlands and USA among some of them.
ASEAN

The Association of South East Asian Nations (ASEAN) had established a high level ministerial meeting on Transnational Crime. ASEAN and China would jointly pursue a joint actions and measure and formulate a cooperative and emergency response procedures for purposes of maintaining and enhancing cyber-security and preventing and combating cybercrime.

APEC

The Ministers and leaders of the Asia Pacific Economic Cooperation (APEC) had made a commitment at a meeting in 2002 which included, “An endeavor to enact a comprehensive set of laws relating to cyber-security and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 and the Convention on Cyber Crime by October 2003.

G-8 STATES

At the Moscow meeting in 2006 for the G8 Justice and Home Affairs Ministers discussed cybercrime and issues of cybercrime. In a statement it was emphasized, “We also discussed issues related to sharing accumulated international experience in combating terrorism, as well as comparative analysis of relevant pieces of legislation on that score. We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that it is necessary to set a measure to prevent such possible criminal acts, including on the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and internet sites for hiring new terrorist and the recruitment of other illegal actors.”

---

60 http://www.usdoj.gov/criminal/cybercrime/g82004/97Communique.pdf.
CHAPTER – IX

CONCLUSION

The ICT Trends of India 2009 have proved that India has failed to enact a strong and stringent Cyber Law in India. On the contrary, the Information Technology Act 2008 (IT Act 2008) has made India a safe haven for cyber criminals, say cyber law experts of India. The problem seems to be multi-faceted in nature. Firstly, the cyber law of India contained in the IT Act, 2000 is highly deficient in many aspects. Thus, there is an absence of proper legal enablement of ICT systems in India. Secondly, there is a lack of cyber law training to the police, lawyers, judges, etc in India. Thirdly, the cyber security and cyber forensics capabilities are missing in India. Fourthly, the ICT strategies and policies of India are deficient and needs an urgent overhaul. Fifthly, the Government of India is indifferent towards the ICT reforms in India. This results in a declining ranking of India in the spheres of e-readiness, e-governance, etc. While International communities like European Union, ITU, NATO, Department of Homeland Security, etc are stressing for an enhanced cyber security and tougher cyber laws, India seems to be treading on the wrong side of weaker regulatory and legal regime.

Praveen Dalal, Managing Partner of Perry4Law and the leading Techno-Legal Expert of India sent an open letter to the Government of India including the Prime Minister of India, President of India, Supreme Court of India, Ministry of Parliamentary Affairs, etc and brought to their attention the growing menace of cyber crimes in India. At last, somebody in the government has shown some concern regarding the growing menace of cyber crimes in India. However, the task is difficult since we do not have trained lawyers, judges and police officers in India in respect of Cybercrimes. However, at least a step has been taken in the right direction by the law minister of India.

Police in India are trying to become cyber crime savvy and hiring people who are trained in the area. The pace of the investigation however can be faster, judicial sensitivity and knowledge needs to improve. Focus needs to be on educating the Police and district judiciary. IT Institutions can also play an integral role in this area. We need to sensitize our prosecutors and judges to the nuances of the system. Since the law enforcement agencies find it easier to handle the cases under IPC, IT Act cases are not getting reported and when reported are not dealt with
under the IT Act. A lengthy and intensive process of learning is required. A whole series of initiatives of cyber forensics were undertaken and cyber law procedures resulted out of it. This is an area where learning takes place every day as we are all beginners in this area. We are looking for solutions faster than the problems are invented. We need to move faster than the criminals. The real issue is how to prevent cyber crime. For this there is a need to raise the probability of apprehension and conviction. India has a law on evidence that considers admissibility, authenticity, accuracy and completeness to convince the judiciary. The challenges in cyber crime cases include getting evidence that will stand scrutiny in a foreign court. For this India needs total international cooperation with specialized agencies of different countries. Police has to ensure that they have seized exactly what was there at the scene of crime, is the same that has been analysed and reported in the court based on this evidence. It has to maintain the chain of custody. The threat is not from the intelligence of criminals but from our ignorance and the will to fight it.

Criminal Justice systems all over the world, must also remember that because of certain inherent difficulties in the identification of the real cyber criminal, cyber law must be applied so as to distinguish between the innocent and the deviant. A restraint must be exercised on the general tendency to apply the principle of deterrence as a response to rising cyber crime, without being sensitive to the rights of the accused. Our law makers and the criminal law system must not forget the basic difference between an accused and a convict. There is only a delicate difference between the need to ensure that no innocent is punished and the need to punish the cyber criminal.

Thus lastly, there were two research questions which were proposed by the researcher for the purpose of the project. The first one being, is the Information Technology Act, 2000 effective and efficient enough for controlling the recent developments in Cyber Crimes in India? The Hypothesis for the question was ‘No’ and it has been proved.

The second research question was, Will the recent proposed amendment to the Information Technology Act, 2000 answer the contemporary complications in the cyber crime arena in India? The hypothesis for the same was ‘No’ and to conclude the researcher has proved it.
BIBLIOGRAPHY

BOOKS AND REPORTS:

Andrew Grant-Adamson, Cyber Crime, Mason Crest Publishers, 2003

David Bowen, Viruses, Worms and Other Nasties, Protecting yourself online; Department of Interdisciplinary Studies, 2003

Dudeja V D, CRIMES IN CYBERSPACE- SCAMS AND FRAUDS (ISSUES AND REMEDIES) Commonwealth Publishers, New Delhi, 2003


John Townsend, CYBER CRIME, Raintree, 2004

Laura E. Quarantiello, CYBER CRIME: HOW TO PROTECT YOURSELF FROM COMPUTER CRIMINALS. Tiare Publications, 1996.


Vladimir Golubev, International cooperation in fighting cybercrime; Computer Crime research Center.

ARTICLES AND WEBSITES:

Adam, and McLaughlin, Charles. “MALWARE: WHAT IT IS AND HOW TO PREVENT IT”


Aderucci, Scott. Salami Fraud, www.all.net/CID/attack/papers/Salami.html..


http://webzone.k3.mah.se/k3jolo/HackerCultures/origins.htm


http://www.cert.org/tech_tips/e-mail_bombing_spamming.html.

http://www.cyberpolicebangalore.nic.in/cybercrimes.htm


http://www.mailsbroadcast.com/e-email.broadcast.faq/46.e-mail.spoo.pnging.htm.

http://www.nrps.com/community/comprev.asp.

http://www.uncitral.org/english/texts/electcom/.


http://www.fbi.gov/quickfacts.htm

http://www.trai.gov.in

Introduction to Cyber Crime,
http://cybercrome.planetindia.net/cybercrime_cell.htm


Kerr, Orin S. THE PROBLEM OF PERSPECTIVE IN INTERNET LAW, Georgetown Law Journal, 91, 357-405

Lance James, Phishing Exposed, Elsevier 2005


The Computer Ethics Institute, a leader in the field, has comprised a guideline to help computer users in their ethical decisions. They have called this guideline “The Ten Commandments”, http://www.computerethicsinstitute.org/images/TheTenCommandmentsofComputerEthics.pdf


Tom Merritt, What is Email Spoofing? See www.g4tv.com.

Understanding Denial of Service Attacks (US CERT) http://www.us-cert.gov/cas/tips/ST04-015.html


www.cybercrimelaw.net/content/history.html.
