# Cyber Laws For Everyone

A Primer on Cyber Laws applicable in India

[BY NAAVI]

[October 2015]

***Cyber Space is all round us Laws of the Cyber Space is impacting us every day. Is it not necessary for all of us to know what this law means to us?...Read on***

# Cyber Laws
# For
# Everyone

***A Primer on Cyber Laws applicable in India***

***[Based on ITA 2008 and Rules notified in April 2011]***

**By**

Naavi

**Publisher**

**UJVALA CONSULTANTS PRIVATE LIMITED**

**Published By**

**UJVALA CONSULTANTS PRIVATE LIMITED**

**No 37, "Ujvala", 20th Main, B S K Stage I, Bangalore 560050**

**Ph: 91-080-26603490,**

**E-Mail: naavi.bangalore@gmail.com**

**Web: www.ujvala.com**



# Price: Rs 150/-

# PREFACE

In 1999, I had produced a book titled "Cyber Laws For Every Netizen in India' which contained a simple explanation of the Information Technology Bill 1999 as presented in the Indian Parliament in December 1999. Since then Cyber Laws in India has evolved. Information Technology Bill 1999 was finally passed in May 2000 to be called Information Technology Act 2000 (ITA 2000). It became effective from 17th October 2000.

In December 2008, substantial amendments were passed to ITA 2000 by the Parliament. The present version of ITA 2000 is therefore referred to as ITA 2008 and has been effective from 27th October 2009. On April 11, 2011, some very important rules were notified under ITA 2008 introducing more

Privacy and Data protection requirements into the law.

I have tried to include all these developments in this book to the extent they are relevant to this Primer.

I have called this as "Cyber Laws for Everyone" because it focuses on the legal implications of ITA 2008 on the general public whether they are Netizens or simply Citizens.

I hope it would be found useful.

Na.Vijayashankar

6th October 2011

# CONTENT

# Volume I

*"Cyber Space is the imaginary space created by binary expressions"*

# Chapter No 1

## Nature and Scope of Cyber laws

Cyber Laws represent the legal frame work surrounding transactions in Cyber space.

## What is Cyber Space?

"Cyber space" was a term coined by a novelist William Gibson in his novel Neuromancer to describe the transaction space in which computer hackers operated.

In simple terms, Cyber Space is the imaginary space created by Electronic Documents generated by Computers or Computer like devices. Electronic Documents themselves can be better understood as "Documents expressed in binary language".

According to Information Technology Act 2000 (ITA 2000) as amended by Information Technology Amendment act 2008 (ITA 2008), the definition of "Computer" includes any automated data processing device, or a data storage device or input and output devices attached to a Computer. The Act is equally applicable for Communication Devices such as Mobiles, Satellite Phones, WiFi devices etc.

Similarly, "Data" is defined to include not only information generated by a computer but also information in any form meant to be processed or being processed or having been processed by a Computer. This definition makes even some paper documents such as Computer print outs and input data sheets (e.g. OCR sheets) as "Electronic Documents" for legal purposes.

One category of Cyber Space which is of interest to us is the "imaginary Space" created when two computers are connected. When computers are connected in a Network, they are able to communicate with each other in such a manner that a person operating Computer 1 can see on his screen the information actually stored in Computer 2 while the connection is on but vanishes when the connection is broken. One way to explain this is to say that certain data in Computer 2 has been temporarily transferred to Computer 1. The data does not reside in Computer 1 since it vanishes as soon as the connectivity is broken.

In such cases we can say that the information existed in the Cyber space during the period the two Computers were connected.

On the Internet, millions of Computers are connected and information is continuously exchanged as long as the connection lasts. This may lead to not only simple reading of web pages but also in conducting commercial transactions such as Banking, Buying, Selling, listening to audio or watching video etc. The entire functionality is lost the moment the connectivity is lost.

Technically speaking, the file which a computer user sees on his screen might have been temporarily transferred to his computer into a "Cache Memory Zone". But as long as its transfer into cache and out of cache is an automatic process, this process is different from saving a file on the local computer, seeing it and then deleting it. It may however be observed that these temporary "Cache" files can be saved if required but

such saving is an exceptional process and not a process which occurs in the normal course of operation. Such documents can be called "Transient Electronic Documents" and are a special category of documents from the point of view of being an "Evidence" in a Court of Law. Such transient documents cannot form a good evidence unless it is captured by an expert and properly certified by a trusted third party.

All internet activities take place with documents being moved into the user's computer screen and removed automatically when the activity is over. These are the activities that we shall recognize as taking place in the "Cyber space".

Computers, Modems, ISP servers are devices that provide an entry into cyber space. Web Servers provide the data and applications

that operate in the Cyber space and become available to the person who moves into the Cyber space.

Since the laws which are recognized as "Cyber Laws" apply even to activities that occur in a single computer as distinguished from a "Connected system of Computers", the concept of "Cyber Space" needs to be expanded to cover individual "Computer Space". It is therefore recommended that we adopt a modified definition of "Cyber Space" as follows:

"Cyber Space means the imaginary space constituted by binary expressions"

In this definition, "Binary Expression" means "Electronic Documents" constructed by "Zeros and Ones". It does not matter if the document is a text, picture, audio or a video.

It also does not matter if the equipment generating the binary expression or processing the binary expression is called a "Computer", "Mobile", "ATM" or any other name.

The term we use for the users of Cyber Space namely "Netizens" was derived from the use of "network" or "Internet" but will cover all those persons who use "Electronic Documents" or "Binary Expressions".

**Netizens:**

Those who travel in Cyber space and use the services available there-in are the "Netizens". At present these Netizens do not have a separate legal existence. They are Citizens of a country in geographic space and are governed by the general laws applicable to their physical existence. Just as an Indian

passport owner travelling to Saudi Arabia continues to be governed by the Indian laws, Netizens are governed by the laws of their own country.

Similarly just as the Indian living in Saudi Arabia is subject to the laws of the local country during his stay, it would be appropriate to think that there should be laws of the Cyber space that should be applicable to those who traverse through them.

Unfortunately, the laws of jurisdiction in Cyber space are still evolving and quite often Countries try to impose their physical space laws to the cyber space transactions as long as the person is residing in their country or some of his assets are present there.

The scope of Cyber Laws is therefore to be seen in this relatively unsettled state of things.

## Scope of Cyber Laws

The scope of cyber laws covers the following four areas.

1. Laws affecting Cyber property

2. Laws affecting Cyber person

3. Laws affecting Real World person but involving cyber medium in some manner

4. Laws affecting Real World property but involving cyber medium in some manner.

Obviously, Laws affecting the real world property and real world persons are already codified into several legal enactments. Many of these laws were enacted when the concept of internet or cyber space was not in the

realm of thinking. Hence they do not address any of the issues that this new medium of transaction raises. Even though there are attempts to extend the legal principles embedded in these laws to the new cyber space, it often leads to unsatisfactory results.

In contrast, some new laws are being enacted today with particular focus on cyber space transactions. These laws not only address transactions in cyber space but also address issues such as the impact on the laws of the real world when the Cyber medium is involved in some manner.

In future, whenever laws are enacted they will take into account the transactions both in the real world and the cyber world.

In the course of our study, we shall focus on the Laws applicable to cyber space and cyber

property and the impact on the real world property because of the involvement of the cyber medium would be discussed only in brief.

In the Indian context, the Information Technology Act 2000 (ITA-2008) is the most important piece of legislation that we need to study under Cyber Laws. ITA-2008 deals with the Laws of Cyber Contract and one set of Cyber Crimes. It also deals with the regulatory mechanism for administering Cyber Laws in India. We shall discuss this in detail in subsequent Chapters.

Additionally, Intellectual Property Rights (IPR) applicable to Cyber properties need to be studied with reference to some Indian IPR laws and prevailing practices in the international scene. Law of Right to Privacy and Freedom of Expression are also relevant

to a Netizen. We shall discuss this briefly in some of the forthcoming Chapters.

Further the laws of Cyber space often overlap over different geographical boundaries. Hence the laws of digital contract, consumer protection, Cyber crimes etc of other countries also become relevant to understand the full impact of cyber laws on the society. We may not however deal with such laws during this course.

In order to understand the laws of cyber space, it is necessary for us to be familiar with some of the basic technology features that make the cyber space work. A brief introduction to such features is given below.

## What is Internet?

Internet is often described as a "Network of Networks". It consists of millions of

Computers (including other communication devices) that are inter connected and can communicate with each other. The worldwide Net is a complex web of smaller regional networks. It is like a modern road network of trans-continental superhighways connecting large cities. From these large cities come smaller freeways and parkways to link together small towns, whose residents travel on slower, narrow residential ways.

The Net superhighway is the high speed Internet. Connected to this are computers that use a particular system of transferring data at high speeds. Major Internet "Backbone" theoretically can move data at rates of billions of bits per second .

Connected to the backbone computers are smaller networks serving particular geographic regions, which generally move

data at speeds around a few million bits per second.

Feeding off these in turn are even smaller networks or individual computers.

Each Internet user is connected to his ISP (Internet Service Provider) or a Mobile Service Provider (MSP) who may in turn be connected to the national backbone of connectivity. The national backbone itself is connected to an International network through the “Gateway”.

The last mile connectivity (Between the Internet user and the ISP/MSP) can be through dial up telephone lines, leased telecom lines, TV cables, DSL cables. Wireless and Mobile phone connectivity is also used in recent days.

The second level connectivity between the ISP/MSP and the national backbone could be through V-SAT or Optical fiber connectivity. International connectivity could be through satellite or under sea Cables.

There are therefore several levels of service providers between the Internet user and the Internet.

When a network of computers is connected to the Internet, all individual nodes connected to the network also get connected to the Internet through the “Proxy server”. In such a system, there are several human beings who share one Connected “Proxy server” and still enjoy all the privileges of being in the Cyber Society.

Similarly, a single Computer can be used by different persons at different points of time to exercise their rights as members of the Cyber society.

## The Role of Each Connected Computer:

The computers connected to the Internet are capable of exchanging information with each other. Some of these computers act as "servers" (dedicated or otherwise) to serve information to other users. Normal users are the clients who use this information. Some users could be acting simultaneously as servers and clients. Special software enables sharing of files on one computer with another on the Internet making every member a "Host" as well as a "Client" at the same time. This is being referred to as "Peer to Peer connectivity" as distinguished from

"Client-Server Connectivity" in a normal network.

In between the Client and the Server, there are "Routers", "Responders", "Firewalls" and other automatic Computer devices which substitute humans to take some routine decisions. Even though they are not necessarily "Intelligent", their decisions do influence the transactions of the Netizen in the Cyber Society.

## How does the Information Exchange take place?

When information is to be exchanged, one computer sends a "Request" "Addressed" to the target computer.

The target computer will keep a "Door" (Port) to its Computer open , if it is "Listening" to such requests.

Some times, the door is kept open to all and sundry. Some times there will be a Gate keeper (Firewall) who asks “Who are You?”. The Computer seeking entry then has to “Identify” itself and say “I’m so and so (My login ID is xxx, My Password is yyy” etc). The Gate keeper will then check with his master (may be a database) and if the person is in the approved list, will let him in. (This is the "Access Control" mechanism that is the backbone of Information Security). Then the target computer will respond to the “Request” and the visitor can access the information available.

## Protocols:

In order to enable machines exchange information particularly on the Internet where unrelated devices need to communicate with each other, they need to

have a common standard language. This is achieved through the use of certain "Protocols".

The term protocol is used to refer to the set of rules that govern the communications between nodes. Since there are a wide number of functions to be performed, there are a considerable number of protocols operating in Internet. The complete family of protocols is referred to as the Internet Protocol Suite. Sometimes the family is referred to by the combined names of just the two most important protocols, TCP/IP.

"TCP/IP" stands for Transmission Control Protocol / Internet Protocol". Additionally, FTP (File Transfer Protocol), SMTP (Simple Mail Transport Protocol), POP3 (Post office Protocol, version 3), HTTP (Hyper Text Transmission Protocol), TELNET (Terminal

Emulation), PPP (Point to Point Protocol) etc are other protocols that work with the TCP/IP to enable Internet to work the way it works today.

Most of these protocols are global industry standards and the user doesn't have much freedom in making any changes in the way these protocols work. There may only be a few customization options which a system expert can manipulate.

## How does the Internet Addressing System Work?

The Internet works on a global system of addressing based on the TCP/IP protocol. All the computers connected to the Internet have a unique identity which is the IP address. Under the widely used addressing system called IPV4, the IP address is the four part number such as 202.54.6.20 etc. There could

be several networks where a group of IP addresses are shared by a larger number of Computers through what is called a "Dynamic IP Addressing System". In this system, it is possible for different computers to be assigned the same IP address when connected at different points of time. Similarly one computer may be allotted different IP numbers when connected at different points of time.

In India, ISP s like VSNL providing Internet connectivity through telephone lines typically adopts this "Dynamic IP system". ISP s providing leased line, Cable modem and DSL connectivity can provide a static IP address to a user on request. Such static address is required for hosting services where a Computer has to be connected to

Internet and serve as a host to other computers. (eg: Website host).

## World Wide Web:

The biggest part of the Internet is the "World Wide Web" (www) which consists of a network where documents created in hypertext markup language (html) or equivalent is placed in different "Host Computers" and can be accessed through "Hyper linking".

In this system, each object such as a text page or an image or a file has a unique address called "Uniform Resource Locator" (URL). When this URL is entered in an application called the "Browser", the document is transported to the Computer in which the Browser is running. The files are copied onto a special temporary area in the

Browser folder called “Cache”. Depending on the settings in the Browser, these files are automatically removed periodically.

Similarly, when the Internet is accessed through the Proxy server in a Network, the requested Web pages are temporarily stored in the cache of the Proxy server. The browsers are programmed to fetch the page from the Cache if available. When the user chooses to “Refresh” his browser, the host is contacted for a fresh copy of the page.

When files are accessed through FTP protocol, they are downloaded into the user’s machine to be viewed through an appropriate application.

The Telnet protocol on the other hand doesnot download the files but transports the user to the target machine by creating an

interface as if he is sitting in front of the host machine itself.

Every URL consists of the IP address of the Computer in which the target file is residing along with the path to the actual file. The URL itself directs the visiting machine onto what is called a "Root Directory and a default page/file". Other files have to be addressed along with the name of the folder and the file.

## How does the TCP/IP work?

TCP/IP stands for Transmission Control Protocol/ Internet Protocol. The Internet Protocol takes care of the addressing system based on the IP addresses. In order to enable the connectivity, the IP request is routed through different regional routers where a database of IP addresses and their location is maintained. The router directs the

communication through any available route towards the destination network. The system is designed for a "Multiple Routing Path" so that each time the communication may travel through different paths even though the originating and destination computers are the same. There is therefore no "fixed path" for communication.

In order to enable users remember the identity of the networked machines, the system of addressing provides for a descriptive name to be assigned through a Domain Name Service (DNS). When this is entered as a URL on a browser, a suitable search of the DNS database (Registry) is undertaken to find the matching IP address to route the communication.

The extensions .com, .net, .org. etc., are called the Top Level domain Names (TLDs)

and enable different sub registries to be created for the mapping purpose. The parts behind the TLD s such as VSNL (in "vsnl.com") are the second level domain names and behind them there can be sub domains.

The TCP protocol also divides each communication into small segments or Packets for easy transmission. Each packet will therefore have a “From” and “To” address as well as a “Part identification number”. The protocol ensures that at the receiving end the broken packets are reassembled in proper sequence to recreate the file in original form. Within each piece of communication, different packets may travel to the destination through different routes and therefore reach at different points of time. It may also be possible that they don't

reach in the right sequence. The protocol still manages to monitor the packets and sends back information to the destination if any packet is not received. Thus transfer of each file between two computers may involve a to and fro dialogue.

## Interdependence of Technology and Laws in cyber laws:

It is important for us to appreciate that cyber laws are as much an integral part of Technology study as much as Legal Study. It is the technology that creates the Cyber space and it is the technology that facilitates the crimes in the space. it is the technology itself which enables evidence collection. Hence every aspect of law including the definition of crimes and how they are to be resolved are technology dependent. Even such fundamental aspects

such as writing and signing in a Cyber medium are a technology factor. Writing means using a computer and an application such as "MS Word" and signing may mean applying a digital signature software to a document.

It is therefore essential that Software and Communication Engineers who create the Cyber space elements, and Professionals who work using Cyber tools are as much in need of the knowledge of this law as the lawyers who need to argue in courts of law when there is a dispute.

With a clear understanding of these laws, non legal professionals can contribute to the development of a fair set of cyber laws that are in conformity with the expectations of the majority in the society.

## Consequences of Ignorance

It is important for all of us to reflect on some of the following incidents and understand the scope of cyber laws and their impact.

1. Dmitry Sklylrov, a Russian software professional was arrested in USA where he landed to attend a conference on an allegation that his Company had developed some software that violated the Copyright laws of USA.

2. Directors of Rediff.com and Times of India received notices for offence of causing distribution of obscene documents through their websites for which they could be jailed for 5 years.

3. A 16 year old high school student in Delhi was arrested for allegedly creating a website containing obscene comments about some of

his teachers. He was later rusticated from the school.

4. A Doctor in Bangalore was defrauded by an unknown person promising a job in a Hospital in Nigeria

5. An IT professional in Mumbai lost lakhs of Rupees from his Bank account since he responded to a phishing mail.

6. A businessman in Andhra took a massive Bank Loan based on a "Lottery Prize" which he thought he had won.

7. Reuter, the well known news agency was charged of hacking into a Corporate network and picking up a press release about its financial performance.

8. Maruti software pvt ltd, a Company in Delhi running a website www.marutionline.com was charged of

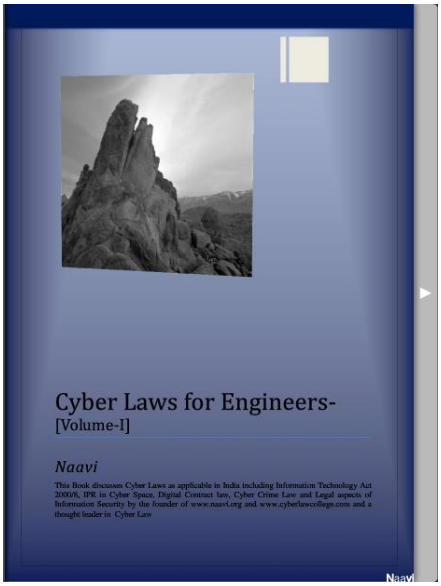
violating the trade mark rights of Maruti Suzuki ltd.

9. Computer world, a reputed magazine carried an interview ostensibly from a terrorist who turned out to be another journalist impersonating as a terrorist.

10. A student in Chennai found to his dismay that e-mails were sent in his name to many girl students of his college damaging his reputation and exposing himself to a serious crime charge.

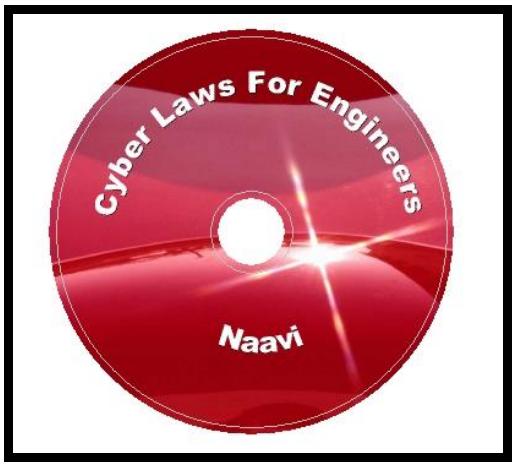
There are several such incidents that affect a Netizen and land them in trouble if we are ignorant of our rights and responsibilities in Cyber space.

The Scope of Cyber Laws extends to all the above incidents and many more.




*Cyber Laws for Engineers*.. E Book by Naavi

Also available on CD



# Chapter No 2

## Relevance of Cyber Laws

In order to understand the relevance of Cyber Laws in general, let us look at it from the various perspectives and in the light of some identifiable Internet experiences.

### 1. An encounter at a Cyber Cafe::

Let us assume that you walk into a Cyber Cafe. The first thing you do is to sign a visitor's book noting your name, address and the time of entry. The owner may allot you a specific computer which is free at the point of time and note down a number that identifies the Computer in the register.

At this point of time, you are establishing a legal relationship with the Cyber Cafe owner. Now you have been authorized by the owner of the Cyber Cafe to use a particular

terminal to connect to Internet and for browsing websites or for sending or receiving e-mails or to conduct a chat etc. In a way, you are renting the facilities required to drive into the Cyber Space just as you rent a self driven Taxi. Any actions undertaken by you during the time you were in charge of the Computer will now be your responsibility until you hand over the terminal back to the owner.

This simple activity of renting the Computer exposes you to a variety of risks. Let us assume that you open the Internet Explorer by clicking on the icon on the desktop. It may open with a home page of a pornographic site. You may try to get out of the page, but the moment you click the mouse any where on the page, new pornographic pages may start opening.

You are wondering what you can do when a Policeman walks upto you and charges you with the possession of obscene pictures and accuses you of violating Section 292 of the Indian Penal Code and Section 67 and 67 B of ITA 2008. In a situation like this, if you know a bit of Cyber Laws, perhaps you can confidently face the Policeman.

Let us examine the incident from the point of view of the key elements that you need to remember here such as .....

Is there any offence committed?

If so whether you are responsible for it?

What are the rights of the Policeman to question you?

What you should do to protect yourself?

## Is there any offence committed?

Indian Penal Code (IPC) is the principle Criminal Law codification in India. It has certain provisions to prevent publication, selling and distribution of obscene materials in print form. Under the section, possession of obscene material meant for distribution or sale is also an offence. Offence under this section can result in an imprisonment of upto 2 years and a fine of upto Rs 2000 for first conviction which can be increased to 5 years and Rs 5000 for a second offence.

However, the current incident is regarding a web page and not a publication in print to which section 292 of IPC covers. The information that gets displayed on a Computer screen is what is called an "Electronic Document" and any offences regarding "Obscenity in Electronic Form" is

covered by the Information Technology Act 2008(ITA-2008) and not IPC.

Now let us see what the ITA-2008 says regarding Obscenity in Electronic Form.

According to Section 67 of the ITA-2008,

***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 three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.***

From the above section, it is clear that the offence is committed only when a person publishes or transmits an obscene electronic material and not otherwise. Viewing an obscene material is therefore not directly within the purview of this section.

If however, you are sending an e-mail containing an obscene picture, or maintaining a website with such material, the section is applicable.

The amendments brought in through ITA 2008 have introduced two additional sections in which "Obscenity in electronic space" is punishable.

Firstly, under the newly added section 67A,

If the content published or transmitted or caused to be published contains "sexually explicit or conduct", the imprisonment term may extend to five years and the fine extends to ten lakh rupees. In the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Additionally, as a measure to punish "Child Pornography", ITA 2008 under Section 67B, makes several acts dealing with material depicting children in sexually explicit act in

electronic form punishable with imprisonment for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

For example, section 67 B does not stop at punishing "publishing, transmission and causing publishing or transmission" of obscene content. Under the sub sections (b) to (e),

***whoever***

***"Creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material***

***in any electronic form depicting children in obscene or indecent or sexually explicit manner" or***

***"Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource" or***

***"Facilitates abusing children online" or***

***"records in any electronic form own abuse or that of others pertaining to sexually explicit act with children",***

is also punishable with five/seven year imprisonment and RS 5/10 lakh fine.

Hence, though there is a scope for debating whether an offence has at all been committed in this case, the odds are heavily against the browser at the Cyber Cafe particularly, if the

content depicts "Sexual Content in which children are involved".

## Are you responsible ?

In the instant case, it appears that the Internet Explorer had a default home page configuration to open the objectionable site. Hence it may be interpreted as a defect in the device rather than a deliberate attempt by you to access the page.

This could reflect a "Negligence" by the Cyber Cafe owner rather than the user. Hence if the Cyber Cafe owner is deliberately using the obscene electronic material to further his business, then he may be exposed to the risk of being charged with "Causing to Be Published".

In such a case you may be called upon by the Police to be a "Prosecution Witness" and you cannot refuse such a responsibility.

Leaving aside the deliberate actions, it is also necessary for us to remember that what is narrated here is a common occurrence and if you are wise, you can educate the Policeman as well as the Cyber Cafe owner and prevent such things from happening again. There are some websites which when visited, automatically re-set the Internet Explorer default home page to itself or some other page. Some times this is done after a prompt and many times without such a prompt. It might have been inadvertently re-set in an earlier session when some body else was using the Computer. It is also likely that any virus could have caused a similar effect.

As a responsible Netizen therefore, if you observe in a Cyber Cafe that the browser has been set to a default opening page to any objectionable site, please re-set it by going to the menu item (Tools-Internet Options in Internet Explorer or Edit-Preferences in Netscape).You can also inform if you feel necessary the Cyber Café owner that if he does not properly check the computers he may be punished for violation of ITA 2008 under various grounds

## What are the rights of the Policeman to question you?

It is interesting to note that appreciating the technological complexities in assessing Crimes related to Computers, ITA-2000 has restricted investigation of a Cyber Crime to Police officers of the rank of Inspectors and above. Even for searching and effecting

seizures of any evidence or to effect any arrests without warrants, the powers are available only to Inspectors and not to other lower ranked Police personnel.

As regards the powers of the Policeman the following Section 80 of ITA-2000 is very important.

***Section 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 an Inspector, 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 of 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.***

From the provisions of this section it is clear that the powers given to the Police under ITA-2000 are restricted and can be exercised only by higher ranking officials under certain special circumstances only.

## What should you do to protect yourself?

In case you are unfortunately caught in an incident of this nature, it is important to remember that you have to protect yourself from any unlawful intimidation by the Police.

Apart from explaining to the Policeman that the opening of the page is automatic and you had no control over it, you may need to ensure that the incident is properly

documented in front of independent witnesses before you leave the scene and hold a copy of the same with you.

This will prevent your being harassed with any false charges on a later date.

As a general precaution, before you start your work in the Cyber Cafe, if you observe that the home page of the browser is set to a wrong site, correct it voluntarily. Then check the system clock and ensure that it is showing a correct time. These are essential precautions that you need to take. Also ensure that if you have visited any site such as say yahoo mail, before you close the session, log out of the site. Do not leave open windows when you leave the computer as it may be misused.

*(P.S: The discussions presented above are only for the purpose of academic understanding and this is neither to support the activity represented therein nor a guarantee that the Policeman would listen to your reasoned arguments.)*

The above incident is discussed in detail so as to give an understanding to the Reader how a simple use of a Cyber Cafe can lead to several legal complications and how a knowledge of Cyber Laws may be helpful even in such a situation.

In a case in Bangalore it was found that a "Key Logger" software had been planted in a Cyber Cafe computer and when some customer used the computer to log in to his Bank account, his log in ID and Password were stolen by the "Key logger" software and was misused by its owner to draw

money from the Bank account of the customer.

In this case the "Key Logger" software would be considered as an "agent " of its owner who would be guilty of not only committing a "Fraud" under IPC but also an offence under ITA 2000 under Section 66 which is discussed in detail later.

In all incidents which involve negligence by a Cyber Cafe the owner of a Cyber Cafe would also be held liable both for criminal negligence as well as paying compensation to the victim. They can however avoid liability if they can prove that they had exercised all due diligence to prevent occurrence of the Crime. (Section 79 of the ITA 2000). Under the provisions of Section 67C of the ITA 2008, the Cyber Cafe owner would also be required to keep any records

designated by the Government for a certain specified duration if any. Any failure to do so would be punishable with imprisonment of three years.

Before the amendments to ITA 2000 become effective, the Cyber Cafes are bound by the current regulations under which many State Governments have notified what documents are to be retained and for how long. For example, under Karnataka Cyber Cafe regulations, the Cyber Cafe owner needs to retain the visitor's register entries (some of which like name, address and signature are to be made by the customer in his handwriting) and the photo ID of the customer are to be retained for a period of one year. After the ITA 2008 is notified for effectiveness, the Central Government has issued fresh due diligence guidelines for

Cyber Cafes. According to these guidelines, under Section 79 of the ITA 2008 the Cyber Café owner has to ensure a very high level of security including synchronization of clocks on the computers, installation of a good anti virus software, maintenance of log records of the computer usage as well as the identification of the users. They also require registration with a designated authority. (Most states are yet to designate an authority for this purpose). Any failure in maintaining the security would make the Cyber Café owner liable for any offence committed by any user of the Cyber Café.

We shall now briefly look at other incidents that make a study of Cyber Laws relevant for any Internet user.

## 2. Spoofed E-mail:

It is not very common for some body to charge that you had sent an offensive e-mail to him. Such a person may be your boss or the CM of the state or simply a girl student of your college.

Such things can happen either when some body logs on to your e-mail account by knowing your password or by simply configuring their e-mail to show your name as the sender of the offensive mail. There are also some Viruses that send spoofed e-mails in your name.

In such circumstances, you need to know how use of digitally signed e-mails as a regular habit can provide you with an alibi. We will discuss this topic in greater detail in a subsequent Chapter.

Further there is a need to appreciate the benefits of the use anti virus protection devices to protect your computer and need to protect the passwords.

According to Section 43 of the ITA-2000, if any damage occurs on account of virus, the victim can claim a damage from the person who caused it. While this could be an option you can use against anybody who introduces virus into your computer, you may also face a similar claim from others since may times virus distribution occurs from an infected computer and yours may be one such.

Protection of Passwords is also essential since use of your password by another to commit a fraud or an offence can make you a prima-facie suspect. Hence it is necessary to configure good passwords and protect them from leakage. It is also necessary to change

the passwords often so that any damages on account of accidental leakage of the password can be limited.

Spoofing of e-mail is however considered an offence under Section 66A of ITA 2008 and is punishable with an imprisonment of 3 years and a fine.

Similarly, sending of mails or SMS which can be considered "annoying" or "menacing" or "Grossly offensive" etc is punishable under section 66A with a punishment of three years and also fine.

## 3. IPR Violations:

Apart from the possible consequences arising out of lack of Cyber Law knowledge discussed above, the violations falling in the area of Intellectual Property Rights (IPR) are of increasing importance to the Netizen.

One of the most important aspect of IPR that the Netizen should be aware of is the possible violation of Copyright. Copyright violations may take place first in the use of pirated software by a Netizen. Whether it is the MS Windows or MS Office, it is essential that the Netizen uses only licensed software so that he does not become liable for copyright violations which may lead to fine and imprisonment.

We may recall here the incident in Chennai where two of the managers of a company called Radiant Software were arrested for using a software beyond the licensing provisions. In this case the Company Radiant Software was engaged in training of Readers on Oracle application and had bought one licensed software. The Company had however loaded the software on several

Computers against the license which allowed loading of the software on only one Computer. For this alleged offense, the managers who were employees in charge of two of the offices of the Company were arrested. They were released on bail after a week and the Company went into an out of court settlement with Oracle.

Similarly, in an international case, a Russian software professional, Mr Dmitry Sklyarov was arrested while in USA, for allegedly producing a software in his Company which helped public to break a copyright lock on Adobe E-books.

Another incident of importance is the case of a Company called Napster which was running a service by which its members could share music files on the Internet through a peer to peer technology. The music

industry representatives alleged that the service resulted in an organized copyright violation and forced closure of the Company.

In India the Copyright Act 1957 deals with the Copyright provisions. Initially the law was meant to protect the rights of the authors of books. It was then extended to protect the performance of artists and later was made applicable to software. In USA, a separate act called DMCA (Digital Millennium Copyright Act) has been enacted to cover the Copyright aspects of electronic documents. Some of the provisions of DMCA could affect the work of a software professional and a research Reader if he is involved in any related activity where by a copyrighted software is affected.

Ordinary Netizens have to be careful in not copying material on the web indiscriminately

particularly for commercial use. They should also avoid using pirated versions of software for producing any work that is commercially distributed.

The second aspect of IPR that affects Netizens is the "Trade Mark" right of an entity which has registered a word or a phrase under the Trade mark right of a country. When a website address (domain name) is registered in a name which could confuse the public with the registered trade mark, the trade mark owner can take objection to the use of the domain name.

For example, some time back, a person in Kerala had registered a domain name www.dreamworkzweb.com which was objected to by Mr Spielberg the celebrated movie maker of USA. Within India itself, Maruti Udyog similarly took objection for a

company called Maruti Software Pvt Ltd in Delhi to the use of the name www.marutionline.com.

There are many such cases which a Netizen should be aware of so that he does not book domain names which may later be objected to by others.

The third aspect of IPR which a Netizen should be aware of is the operation of "Patent" for both software on a CD as well as software that works on the web. This mostly affects business people who maintain websites and the users may not directly come under legal barrage. However, if Netizens are themselves professionals, they should look for protecting their own ideas by global patents to the extent possible so that their intellectual wealth is preserved and nurtured.

Cyber Laws will also apply to the domain of Telephony and Broadcasting since these two fields already share a common digital technology with IT.

Also, the Indian Government is contemplating a law to regulate medical transactions conducted over the electronic media including sharing of diagnostic reports and medical advice between hospitals and tendering of telemedicinal advice.

Hence from browsing the Internet , to sending and receiving e-mails and from listening to music on the net to use of Internet telephony, Cyber Laws have a wide influence on the activities of a Netizen.

A reasonable knowledge of Cyber Laws are therefore essential for any user of the Net and more so the professionals and

businessmen who use the Internet and Computers for their day to day use.

Since ignorance is not a defense in law, Cyber Law literacy is vital to survive in the digital era.

# Chapter No 3

# Objectives and Scope of Information Technology Act-2008

Information Technology Act 2000, (ITA-2000) is the first legislation in India to address the Cyber Space law issues and came into effect from October 17, 2000.

## Origin of ITA-2000:

The origin of the Act can be traced to the growth in the use of E-Commerce in the global trade and the concerns of the United Nations Commission on International Trade Law (UNCITRAL) about the need to provide a legal environment for trade related activities over the Internet and with the use of Electronic Data Interchange. (EDI).

As early as in 1985, in its 18th session, UNCITRAL, had adopted a resolution

recognizing the legal value of Computer records in International Trade and had urged the Governments of member nations to take suitable steps to ensure adequate legal security.

Since different countries had different legal, social and economic systems it was felt that for harmonious international trade relations, a common law for E-Commerce transactions was required. Adoption of such a model law was expected to assist legislation in the respective countries for governing the use of alternatives to paper based methods of communication and storage of information and in formulating such legislation.

United Nations General Assembly in its 85th plenary session recommended a "Model Law for Electronic Commerce" through its resolution dated 30th January 1997. This

UNCITRAL Model Law thus became the mother of all Cyber Law Regulations through out the world.

The resolution therefore recommended that all States give favourable consideration to the Model Law when they enact or revise their laws.

Based on the Model Law, the Ministry of Commerce in the Government of India developed a "Draft E-Commerce Act 1998" and released the copy to the public for comments in the middle of 1998. Following the setting up of a separate ministry for Information technology under Mr Pramod Mahajan, in December 1999, the Draft E-Commerce Act was reintroduced as the Information Technology Bill 1999 and later became the ITA-2000 in was passed by the Parliament in May 2000 and came to be

known as the Information technology Act-2000.

After some minor amendments to the Act in 2003, a major amendment has been passed to the Act in December 2008. This has expanded the scope of the Act substantially.

## Objectives:

It is clear from the origin of the Bill itself that the primary objective of the Bill was to Promote E-Commerce by providing legal recognition for electronic transactions. Two other key objectives were to define Cyber Crimes and set up a Cyber Justice dispensation system to ensure that the threat of Cyber Crimes did not hurt the growth of the E-Commerce industry.

These requirements have been met in ITA-2000 with the legal recognition for

Electronic documents and Digital signatures and the setting up of the system of Adjudication and an Appellate Tribunal specially to address the requirements of the providing justice against Cyber Crimes.

Further the need to attend to the International requirements meant that there had to be some uniformity in the laws of different countries regarding Cyber Laws and also a mechanism to make the laws applicable across the physical boundaries of the countries.

This objective has been met in the ITA-2000 by providing an extra-territorial jurisdiction for the operation of the Cyber Crime section of the law.

With the passage of Information Technology Amendment Act 2008, the scope of the Act has undergone further expansion. While ITA

2000 had the basic objective of promoting E-Commerce, ITA 2008 has shifted the focus on "Cyber Security". Several provisions have therefore been added to the Act to expand the definition of Cyber Crimes, enhancing the compensation payable under the Act, responsibilities of the Intermediaries and instituting a more comprehensive regulatory agency framework.

## Scope of ITA-2008:

The scope of ITA-2008 can be seen from the angle of the type of transactions that it covers and also from the angle of its jurisdiction.

According to Section 4 of the Act,

***"Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then,***

***notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is***

***(a) rendered or made available in an electronic form; and***

***(b) accessible so as to be usable for a subsequent reference"***

In view of this provision, the legal recognition of documents in electronic form stand extended to all laws applicable in India.

In order to remove conflicts if any in some of the other laws, the Indian Penal Code, The Indian Evidence Act, The Bankers Books Evidence Act and the RBI Act were amended with the passage of the ITA-2000,

However, Section 4 stated above operates with the following exceptions stated under Section 1(4). (First Schedule of ITA 2008)

***"Nothing in this Act shall apply to,***

***(a) a "Negotiable Instrument" (Other than a Cheque)*as defined in section 13 of the Negotiable Instruments Act, 1881; (* amended vide Negotiable Instruments Amendment Act 2002, Date of effect to be notified.)***

***(b) a "Power-of-Attorney" as defined in section 1 A of the Powers-of-Attorney Act,1882***

***(c) a "Trust" as defined in section 3 of the Indian Trusts Act, 1882;***

***(d) a "Will" as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other***

***testamentary disposition by whatever name called;***

***(e) any "Contract for the Sale "or "Conveyance "of Immovable property or any interest in such property;***

***(f) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette. "***

Further, Section 10A or the ITA 2008 provides specific validity to contracts formed through electronic documents. It states as under

***"Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by***

***means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose"***

In view of the operation of these three sections, laws such as Indian Contract Act and Indian Companies Act are automatically updated for the use of Electronic documents.

Simultaneously, Sections 6, 6A, 7 and 8 of the ITA-2008 also extend the legal acceptance of the use of Electronic documents to the Government sector including filing of applications, Delivery of Services by service providers, issue and submission of tenders, receipt of money, retention of documents and issue of Gazette notifications.

It is clear from the above provisions that a majority of transactions that an average Indian is interested in has been automatically extended for Electronic Documents.

## Digital Signatures

The legal recognition of Electronic documents has to seen along with the Section 5 of the Act which provides legal recognition to "Digital Signatures" (As defined in the Act-explained in greater detail later) as an acceptable means of authentication of any Electronic documents.

We can therefore conclude that except for the excluded transactions mentioned in Schedule I, in any other transaction, an electronic document duly authenticated with

a digital signature is as good as a written document with a signature.

## Legal Jurisdiction:

ITA-2000 is applicable through out India including the State of Jammu and Kashmir.

Additionally, according to Section 75 of the ITA-2000 the provisions of the Act are also applicable to persons residing outside India and persons who are not Citizens of India provided an of the contravention committed involves at lest one of the Computers used is located in India.

ITA-2000 is a special Act and to the extent of involvement of an Electronic document it has an overriding effect in respect of any other law in force.

Section 81 of the Act makes this amply clear with the statement

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

***Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act 1970 "***

Further, the powers of the Adjudicating officers and Cyber regulations Appellate Tribunal have also been explicitly recognized under Section 61 to bar any interference from other wings of justice. This section states:

***"No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber***

***Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act."***

***Provided that the court may exercise jurisdiction in cases where the claim for injury or damage suffered by any person exceeds the maximum amount which can be awarded under this Chapter."***

In summary therefore it can be stated that the ITA-2000 has been structured to provide a wide scope for applicability extending over several other legislations in the country. It is therefore a fundamental law with an impact in every aspect of our transaction.

## Netizen's Context:

In the context of the Netizens, it can therefore be stated that

-Every e-mail sent and received is a legally recognizable electronic document. If the e-mail is digitally signed, it will be equivalent to a written letter. Otherwise, it will be a document that can be proved with the help of ancillary documents.

-Every Web page is a valid Electronic document binding the owner of the web page to the statements made there in.

-Every time the Netizen clicks the "I Agree" button for the terms of agreement on a webs site, he is providing an authentication to a legally valid document like an oral statement in the off line context.

-Any loss suffered by a Netizen through a Cyber Crime can be taken to the Adjudicating officer if it is within the provisions of the Act and a quick decision can be obtained.

[Please note that ITA 2008 is a term used here to recognize ITA 2000 with amendments made in 2008. Officially the Act is still called ITA 2000 only and hence both terms are to be treated as referring to the same Act]

# Chapter No 4

# Law of Cyber Contracts

The passage of Information Technology Act 2000 (ITA-2000) ushered in a new era in business for Indians because it made it possible for Indian residents to enter into legally valid Cyber Contracts.

## What Are Cyber Contracts?

The word "Contract" is derived from the Latin word “Contractum” meaning “Drawing together”. Contracts are the backbone of Business. Contract is what enables two unknown parties to enter into a business deal with the confidence that they can resort to an intervention of the judicial system for resolving disputes if any. If it were not for the fact that a Valid Contract can be taken to a Court of Law, Business would not have

grown across communities and through out the World. On the Internet, Digital Contracts are the backbone of E-Commerce.

Every country already has laws of the Non Cyber Society or the "Meta society" that define "What is a Contract" and various aspects of the same. In India, Indian Contract Act 1872, defines "Contracts" and codifies all aspects of Contract law. Neither the Information Technology Act-2000 in India nor the UNCITRAL model law for Cyber Transactions has defined what a "Digital Contract" is. However, both in India as well as in Singapore and many other countries, the Cyber Law statute has used the following clause or its equivalent to extend the validity of the "Meta Society" law to the "Cyber Society ".

..”Wherever any Law requires a document to be in writing , such a requirement is deemed to have been fulfilled if the document is in electronic form…”

As a result of this provision, we need y to derive most of the Cyber law interpretations from the statutes applicable to “Meta Society”. We may however continue to look at the Cyber Laws with a different perspective so that the ambiguities that would creep in the interpretations because of the attempt to “Extend the Laws of the Meta Society” can be properly resolved.

We can therefore define a “ Cyber Contract” (or Digital Contract) as a “Contract” where either a part or whole of the transaction contains an “Electronic Document”.

In order to study the "Cyber Contracts" therefore, we need to study the law of Contracts and understand the definition of "Electronic Documents". Inter-alia we will also need to study the "Digital Signatures" which replace the normal signatures that are used in non-digital contracts.

The general definition of "Electronic Document" is that it is, any information generated, sent, received, or stored in media, magnetic, optical, computer memory, microfilm, computer generated microfiche, or similar device.

In general, an "E-Mail", a "Web page", a "Chat" or a "Message Board entry" are examples of electronic documents on the Internet. Similarly, a "Word" file, a "Power Point presentation" file, an "MP 3" file, a

"Jpg or Gif" file as well as a ".java" source code file may all be different forms of electronic documents. The web based agreements which we click "I agree" before downloading a free software are also examples of "Electronic Documents".

Similarly, contents of a floppy or a Compact Disk, or a Hard Disk, either attached to a computer or in the virtual server or on a removable device, constitute "Electronic Documents"

Some of these such as "E-mail" are by fundamental nature documents meant for "Transmission" to an addressee. The "word" type of files may however be fundamentally, "Meant for Private Storage". "Chat" is a unique document which is transient in nature and by fundamental nature not meant to be held for future reference" even though

technically the transcripts can be recorded just as telephone conversations can be recorded.

## Elements of Contract Law ( as in Meta Society Law):

Contracts are defined as "Agreements Enforceable in Law".

Agreements are entered into between two or more persons. It is a combination of an "Offer" and an "Acceptance".

An "Offer" is made by one person and is "Accepted" by the other to conclude an agreement. The offer/acceptance involves "A promise to do" or "A promise not to do" a certain thing at the request of or for the benefit of one party to a contract by the other/s.

The act of such "Doing" or "Not doing" is called "Consideration" for the Contract.

Contracts can be oral or written and may be Express Contracts, (recorded by oral or written words) or Implied (by conduct).

For any agreement to be valid in law as a "Contract" the following five prerequisites must be satisfied.

1. The agreement should have the free consent of the parties.
2. The parties should be competent to contract
3. The agreement should be for a lawful consideration
4. The agreement should be for a lawful object
5. The agreement is not expressly declared void.

“Free Consent” of the parties means, consent without “Coercion”, “Undue influence”, “Fraud”, Misrepresentation”, or “Mistake”.

“Coercion” is committing or threatening to commit any act forbidden by law.

"Undue influence" refers to the special relationship between two parties where one is in a position to dominate the will of the other person (ex: husband over wife, employer over employee etc).

"Fraud" generally means suggesting as a fact of that which is not true, by one who doesn’t believe it to be true.

"Misrepresentation" means a positive assertion of a false information, in a manner not warranted by the person making it, even if he believes it to be true.

"Mistake" refers to mistake as to a matter of "Fact" essential to the agreement.

Any contract that doesn't have the free consent of one of the parties is "Voidable" against such person.

Persons who are "Minors", of "Unsound Mind", or "Undischarged Insolvents" are considered "Not competent to contract".

## Applicability of Law and Jurisdiction:

Under traditional law, where both parties are situated in the same "Jurisdictional territory", the law applicable to the contract will typically be of the same territory unless otherwise specifically agreed to between the parties.

Presently, the Cyber Society is yet to develop its own legal regime except to some

limited extent in the "Domain Name Area".

However, since the parties to a contract over the Internet often reside over different territories, the applicability of law as well as the jurisdiction of implementation is always subject to dispute.

The Information Technology Act-2000 (ITA-2000) of India has specifically clarified how to determine the "Time and Place" of a "Message". This can be used to determine the time and place of "Offer" or "Acceptance". A Contract is concluded when an "Offer is Accepted". If the Contract doesn't specify the jurisdiction or applicability of law, one can try to identify the place where the "Contract was concluded" to determine the applicability. In the case of Cyber contracts, the contracting

parties are located in different locations and the “Cyber Space” is in between. If there is a specific recognition of the “Law of Contracts for the Cyber Space”, then it would have been easy to identify the applicability. In the absence of such a common understanding we may have to tag the “Cyber Space” as an extended space of one of the parties.

If there is a “Website” where the owner has made some “offer” which the visiting Netizen “Accepts”, we may say that the Netizen has visited the Virtual office of the buyer and this office is an extension of the “Buyer” who is bound by the Meta Laws of the place from which the seller is responding. Hence, if the seller is servicing the contract from the state of Maharashtra, then perhaps it is correct to consider that the seller is using the website as an extension of

his Maharashtra office and apply laws applicable therein. If there are multiple addresses of the Seller available on the site, and the responding office cannot be identified, the "location" of the principal office of the Company may be considered as the originator of the transaction.

If the sale happens on account of an e-mail marketing message, it may be presumed that the seller has visited the "Buyer's Cyber space" with an intention to conclude the business there. In such a case, the location of the buyer will be material to the contract and can be fixed as to the address specifically recorded in his e-mail or in its absence, the address recorded in the "Digital Signature" (if any) or in its absence, the address recorded with the ISP managing the e-mail, in that order.

In the US, the laws seem to allow jurisdiction if the Contracting party has a place of business in the relevant state. For this purpose, any contact office mentioned in the Website for Customer Contact could be interpreted as maintaining a place of business and extend the jurisdiction to such a State.

This school of thought interprets that it is the website which visits the jurisdiction of the Netizen (by maintaining a minimum contact with the community in that jurisdiction) and it is not the Netizen who walks into the jurisdiction of the website. Discerning Readers may spot a difference between this line of thinking from the one presented earlier. Probably this needs to be explored further.

In one of the noted Judgments in the case of Metro-Goldwyn-Mayer Studios, et al. v. Grokster, Ltd., et al in the United States, a District Court has opened up some controversies regarding the jurisdiction laws applicable to E-Business, in US. This Judgment clearly sets out the rules under which the Californian Courts assume Jurisdictional control over any service which is being used by the Citizens of the State.

According to the judgment,

California authorizes its courts to exercise personal jurisdiction over non-resident defendants to the full extent permitted by the United States Constitution. As such, its courts can exercise jurisdiction over a defendant if he has "certain minimum contacts with the forum [state] such that the maintenance of the suit does not offend

'traditional notions of fair play and substantial justice."

In Other Words, if you have a successful business run from India and have clients in California, then you must adhere to the regulations of California.

To avoid such confusion, it is always better for the owner of a website to clearly state the jurisdiction criteria as part of the terms of his sales contract (as found on the sales agreement). For the Netizens, it is also beneficial if they always state in their e-mail communications, the physical address as a part of the signature. The more legally conscious netizens may even append a foot note- “I am a resident of xxx and any liability arising out of this communication would be a subject matter of the Courts in

xxx only except otherwise agreed to specifically".

## Agency:

Contracts are often entered into between two persons directly or through their "Authorised Agents". An agent can by his actions bind his principal to a contract. The actions of the "Agent" are sources of many legal complications since the " An Agent's authority" can be disputed or rendered unclear by circumstances.

In the cyber society, often "Computers" act as de-facto agents. The ITA-2000 and the UNCITRAL model law states that "An electronic Document will be attributed to the originator if it was sent by an information system programmed by or on behalf of the originator to operate automatically". This is a

de-facto recognition of "Agency" relationship for a computer and recognition of a Computer as a "Digital Personality".

However, cases such as malfunctioning of software for various reasons may create difficulty in interpreting the liabilities of the originator since "Attribution" does not necessarily prevent the originator from denying the liability under "Mistake of Fact" or any other ground.

The role of "Mechanical Agents" will remain to be one of the grey areas of Cyber Law.

## Contracts involving "Cyber Goods":

Contracts are often related to the "Buying and Selling of Goods or Services". Cyber Contracts may involve, contracts entered into in the Cyber space for delivery of goods or services in the meta space. In such

circumstances, there is an interaction between the Cyber Society and the Meta Society by the very nature of the transaction. The legal implication of performance or non performance of the promises envisaged in such a Contract need to be analysed with reference to both the Meta Law and Cyber law. If there is a conflict it may be necessary to consider that the basic objective of the contract is to perform a promise in the Meta society using Cyber Space as a tool.

However, Cyber Society creates several "Goods and Services" and "Cyber Properties" exclusive to the society. Even if they are similar to some products or services which we know in the Meta Society, "they have no existence except in a Cyber Society". These are what can be identified as "Cyber Goods" or "Cyber Properties".

In the virtual world, all "Goods" are "Services" since they do not have a physical "Existence". Hence, there may not be a need to distinguish between "Cyber Goods" and "Cyber Services". Either name may be equally descriptive of the nature of the "Exchanged item". We shall therefore use the term interchangeably even though we would like to use the term "Cyber Goods" more often since it helps to distinguish between the "Meta Society Goods".

Contracts relating to "Cyber Goods" cannot be adequately interpreted with reference to the Meta Law since these laws were never conceived with reference to such goods. If we try to use the Meta law to interpret the Contracts relating to Cyber goods, we will end up with confusion.

Sometime back there was a case reported in Delhi where the Internet access hours belonging to a person were used by another. Many tried to interpret it as "Cyber theft" of "Internet Hours" and said that the law cannot punish the criminal since the "Stolen property" is not adequately described. The reason is obvious. When the Criminal laws of the land were drafted, there was no way a "Virtual Property" like "Internet Access Hours" could be visualised. Hence it restricted itself to defining "Theft" with reference to "Movable Property".

An even more interesting case was reported recently from US. In this case a complainant alleged that some virtual furniture owned by him and installed at his virtual hotel on a website had been stolen!

It is clear therefore that it is necessary to codify the offences relating to Cyber goods separately or leave them as "Grey Areas where law is yet to evolve". "Domain Names" or "Web sites" are other examples of Pure Cyber Property to which no law of the Meta Society can be applied without bending it awkwardly.

## Web Development Contract:

The web development contracts are one of the most common contracts that any Cyber Business man comes across. Some past cases in India such as the go2nextjob.com case (Refer article http://www.naavi.org/cl_editorial/edit_09feb01_2.html ) have highlighted the problems of not having proper documentation of inter-se liabilities in a web development contract. While web development contracts will have

to cover all the aspects of a software contract described above, they may have to additionally provide for losses arising due to negligence of the server management contractor who may himself be a sub contractor of the web developer.

## The Nature of unsigned Electronic Documents:

In the Meta Law, contracts can be oral and also implied by conduct. Written contracts and properly "Signed" contracts may make it easy to prove a contract in a court of law. They are however not mandatory for a valid contract. Similarly, Digital contracts can be "Digitally signed" to be beyond dispute. However, nothing prevents an unsigned electronic document to be treated as a legally accepted offer or acceptance.

In interpreting the legal liabilities of the owners of electronic documents, it may be necessary to give weightage to the "Fundamental nature" of the document. Meta society Law does recognize such collaterals for drawing conclusions on the real intentions of the contracting parties or at least to fix the onus of proof.

In the Cyber world, a statement made in a chat room, an ordinary e-mail and an e-mail which is "Digitally signed" cannot all be given the same weightage as to fixing the intention of parties. For example, an "Obscene" statement made in a chat room may be considered a passing remark while an "Obscene" website may be considered a deliberate attempt to "publish obscene material". The two crimes (if they are considered so) cannot perhaps be considered

same since the fundamental nature of the two types of electronic documents used is different.

It is because of such reasons that “Cyber Laws” and “Technology” are inseparable and ideally, no judgment should be arrived at on the legal aspects of a transaction without considering the “Cyber nature” of any of the elements of the contracts involved in the transaction.

## Responsibilities of a Netizen Towards Cyber Communications

In view of the legal position explained above, any e-mail or a webpage can be construed as a contractual document. If a Netizen therefore avails any service on the Web by clicking "I Agree" button found at the end of "Terms and Conditions" at say

yahoo.com or similar sites, by implication, it is equivalent to signing ( or atleast initialing) a written document.

Netizens should therefore avoid the negligence of clicking without understanding the terms of the agreement. This is particularly true of downloading "Trial Version" of a software where the software vendor may aggressively pursue his copyright if the trial version is used beyond the terms permitted.

In India many of the Government transactions are governed by separate procedures. To enable use of Electronic documents in such transactions, ITA-2000 has made provisions for Tenders, Applications etc to be made to the Government to be in Electronic form if the Government department so desires.

Thus with the passage of ITA-2000, India has taken a definite step towards the "Cyber Contract Era".

In recognition of this major change that has occurred in the Indian business history, Cyber Law College has declared October 17th as the "Digital Society Day" and every year, Digital Society Foundation (A Trust established in Bangalore) undertakes some programmes each year to commemorate the day.

# *Chapter No 5*

# *Digital Signatures and Their Usage*

## Signatures-Essence of Contracts

In the previous Chapter, we discussed about "Digital Contracts" which are agreements enforceable in Law made partly or fully of "Electronic Documents". In the case of paper based contracts, the parties bind themselves to the contract by affixing signatures to the documents. Even though "Contracts" can be legal, the commercial world largely operates only on the basis of "Written Contracts". The key element of all such written Contracts is the "Signature". Similarly, in the Digital Contract world, digital substitute for a "signature" is the "Digital Signature".

The first thing we need to understand about digital signatures is that it is not a “Visual Image of a written signature”. When you scan a written picture of a signature you produce a “Digital Image of the Signature”. This is not the “Digital Signature” that we will be talking about in respect of Digital Contracts. Such scanned signatures are better distinguished as “Digitised Signatures”.

In the Paper based world, there is a system of affixing “Thumb Impressions” in place of written signatures. In what appears to be a similar system, in the Digital world , there are authentication procedures involving “Thumb Impression Scanning” or “IRIS Scanning”. (Iris scanning is a system which compares the iris print of the eye of a person, which like thumb impressions, are said to be unique). These are sometimes

referred to as “E-Signatures”. But these are again not “Digital Signatures”.

There is also a system of signing on a "Digital Pad" which can capture the image along with the strokes, pressure variations etc. This is also a kind of Electronic Signature, but again not the "Digital Signature" we are talking of.

Digital Signature is a “System” which enables Contracts to be entered in the Cyber Society. It is much more than an authentication mechanism based on Thumb impression or Iris print or Digital pad writing or Voice recognition. In order to understand what this “System” means we need to understand certain principles of “Written Signatures”.

## Some Common myths about Signatures:

Let us therefore discuss some common misunderstandings about Written Signatures:

1. Signature is one standard mark representing a person in any document.

If so, how do we accept the same person signing in two different ways? In India, the RBI Governor signs on a currency note both in English and Hindi. All official circulars of the Government also carry signatures in English and Hindi. Obviously, the two signatures of the official who authenticates such documents are not same. We should therefore conclude that "Signature" can be in many forms.

Some persons have the habit of maintaining different forms of signatures for different

types of transactions. For example, some times they may sign in full and some times they may sign in short form. Is it acceptable? If signatures in two different languages are acceptable, why not in two different forms in the same language?

Signature is therefore not necessarily, a " Unique way of writing one's name". It is a form of writing that is accepted as a representation of the person and indicating his consent to what is written above the signature. . There can also be "Multiple signatures" for a same person.

It is true that in Banking transactions, signature has to "tally" with a specimen already lodged. Hence if it is in a different language or form, it would be rejected even if there is collateral evidence to prove that it has been affixed by the signatory himself.

This is more a “Contractual Agreement” and “Procedural Convenience” rather than a “Law”.

Further, a signature of a person may become the signature of an organization, if the signature is embedded in a "For .... Company Ltd, Director" or any such property. The signature that represents a person may therefore represent some other legal entity if such intention is declared at the time of signing.

## 2. Signature has to be legible.

Once we accept that signatures can be in different languages, the question of legibility does not arise. For a person who doesn’t know Urdu, the signature in Urdu is illegible whether it is neat or not.

## 3. Signature is “Writing of Name” .

Not necessarily. A thumb impression is a mark of a person and constitutes a “Signature” which binds a person to the contents. In fact in property documents, this is considered a better form of “Signature” than the written name.

A Common Seal could be a signature of a Company much the same way as our ancestor Kings used to use the "Raja Mudra".

## 4. A Signature on a written document is “Binding”.

Even though it is a presumption that a “Signature” of a “literate” person on a document is a binding evidence against him in a Court of law, there are many instances in which the signature even if correct is not binding. One such instance is

when there is a reason to believe that the contents of the document have been altered after the signature of the person, without his consent.

Thus , when we look at a “Valid Signature”, it represents “The person” who originates the document and also confirms that the contents of the document have not been changed. In other words, the Signature represents “Authentication” and "Data Integrity" of the contents of the document. Because of these it provides a “Non Repudiation” guarantee on behalf of the signatory as to the contents of what is signed..

We can therefore identify the objectives of “Signature” on a paper document as “Authentication”, “Data Integrity” and “Non Repudiation”.

A Digital Signature should therefore satisfy all these characteristics to qualify as a worthy substitute of the Paper based signature.

Additionally, the “Digital Document” more often than not, floats on a “Virtual Space” and is transmitted from the originating computer through Internet. Even when stored in a network computer, it can become accessible to other computers. In view of this, it is necessary to consider the need of “Confidentiality” while dealing with Digital documents.

“Digital Signatures” are therefore conceived as a ”system” that takes care of these four requirements, namely

1. Authentication
2. Data Integrity

3. Non Repudiation
4.Confidentiality.

## How the Digital Signature System Functions:

Digital Signature system uses two software sub components. One is the "Hash Algorithm". The other is "Public Key Encryption".

Hash algorithm is a special function which when applied to a document produces a unique "Hash code". The algorithm is such a system that every time it is applied on a document, it consistently produces the same hash code. Also, even if a single comma or dot is changed, it produces a different hash code. Further the hash methodology is a "one way" operator and the original message cannot be reconstructed with the hash code.

We can see an example of a hashcode in the following:

Let us take a sentence "My Name is Naavi".

If we apply MD5 algorithm which is one of the standard algorithm, it produces the hash code

"ece376f327f3128a4aca3e823a5ab334".

If we now take a slightly modified sentence "My name is Naavi", the same algorithm produces the hashcode " 4dd7fe3dd404bd0fca37592a8bbd6c75 ".

Similarly, if we take another slightly different sentence "My nameis Naavi", the hashcode would be

" 10e027bf3930330493047ffefafcb9f6 ".

We can observe in these examples that even with a small change of a lower case letter to

upper case letter or a removal of a "Space", the hashcode produced is very much different.

Public Key Encryption is a technology where by a digital document can be encrypted and decrypted using a unique pair of keys called the pair of “Public Key” and “Private Key”. The uniqueness of this pair is that a document encrypted with one of the keys of a pair can be decrypted only with the other. Because of this characteristic , a document, which is decryptable with one of the member keys, is presumed legally to have been encrypted with the corresponding other key of the pair.

For the purpose of usage, one of the keys referred to as the “Private Key” is always held by its owner and originator of the key pair. The other key referred to as the “Public

Key" is distributed to all the intended recipients to whom the originator wants to send an encrypted message.

Now, let us look at an example of how the encryption works:

Let us say that Rama wants to send this plain text message" Lakshmana, this golden deer is a hoax. Be careful" in an encrypted form.

The encrypted Cipher text may look like

"gdBPNN3+PI7rlMWmJAPx2rLPEBOJMu
8pKtbKd0KLSFEh5JDw1YBbpVnsY9FRC
m+yXu3nierQhsS7R+ctb/VTYiX7Z1czH+U
GLJRd6ByczUhkF8oAr4HoTCPDMMYdaL
Hi9b8LZNjiHh6KovmVQITC8wZ65a0Mlcq
6DmsU9pFrj6U="

If this message is to be decrypted, one needs the corresponding decryption key. If the message has been encrypted with the private

key of the sender, it can be decrypted with his public key which should be available in the public domain. If the message has been encrypted with the public key of any person, it can be decrypted only with the private key of such a person.

When Rama wants to send a message in confidence to Lakshmana, he can encrypt the message using his private key and let Lakshmana use Rama's public key to decipher the document.

Alternatively, Rama can use the public key of Lakshmana to encrypt the document and Lakshmana can use his private key to decrypt. In either case the confidentiality of the document is protected between the originator of the encrypted document and the holder of the decryption key.

While Rama's message encrypted with his private key can be read by any body having his public key, the message encrypted with the public key of Lakshmana can be read only by Lakshmana and not any body else. This follows the principle that "Private Key" is always held by the "Originator". However, Lakshmana cannot conclusively determine who has sent the message encrypted with his public key. It could be Rama or any body masquerading for Rama.

It is also possible for a message to be encrypted both with the private key of Rama and the public key of Lakshmana. In this case, the message can be read only by Lakshmana and additionally, Lakshmana is also certain that it could not have been generated by any body other than the holder

of Rama's private key which can be none other than Rama himself.

This principle of double encryption is used in the "Digital Signature System" along with the "One way hash function" to corroborate the data integrity.

The usual procedure of Digital Signature is as follows:

1. Pick the document to be signed.
2. Apply the hash algorithm to calculate the hash code
3. Encrypt the hash code with the sender's private key
4. Send the message in normal text along with encrypted hashcode to the addressee.

The "Digital Signature is therefore defined as follows:

**The "Digital Signature" of a person, of a document is the hashcode of the document encrypted with the private key of the person".**

(This is the definition that follows from Section 3 of ITA 2000)

The receiver will get the message in the normal form along with the encrypted hash code.
He will then proceed as follows.

1. He will use the public key of the sender, which is with him to decipher the hashcode. If he can decipher with the public key of the sender, it ensures that no body else could have sent the same.

2. He will then separately calculate the hash code on the message received,

applying the same system, which the sender has used.

3. He will then compare the two-hashcode values. If they are same, it means that the message has come from no body other than the sender and no change has been made in the data after it has been signed.

This procedure is called a "Transparent Signature". It is so called since it doesn't conceal the document being sent. It however ensures data integrity through a hash code and also authentication and non-repudiation.

A variation of this process is the "Opaque Signature" wherein the entire message is also encrypted so that even if the message is intercepted in transit, it cannot be read by somebody not having the decryption key.

The popular procedure for such “Wrapping” messages sent over networks are to use the public key of the addressee. If messages are to be stored in confidence, the private key of the originator is used.

In the above mechanism, the person who has to verify a signature needs to have the “Public Key” of the originator. Since in digital transactions, the sender and the receiver of the message may never meet in person, even the key exchange has to take place on the digital media itself. If this is so, what prevents a Maaricha to send a public key to Lakshmana and say that it is the public key of Rama?. If Lakshmana is keeping the key in the belief that it belongs to Rama, any message received from Maaricha will look like coming from Rama.

In order to prevent such happenings, the key exchanges are done through a “Trusted Third party” whose signature is recognizable to both the sender and the intended receiver. This trusted third party is the “Certifying Authority”.

In practice, affixing a Digital Signature and Verifying a Digital Signature is done automatically by software installed for the purpose. For example affixing a digital signature for an outgoing e-mail is as simple as clicking on the "Sign" icon on the Outlook Express or checking the box meant for the purpose in the Netscape Messenger. Forwarding of the public key and verification at the other end is inbuilt into the Outlook Express or the Netscape Messenger at the other end. Similarly, the system of

verifying the digital signatures of "Servers" is inbuilt into the browser software.

## Electronic Signature

ITA 2008 has defined the term "Electronic Signatures" under Section 3A as also a means of authentication of electronic documents in addition to "Digital Signatures" discussed in greater detail above.

This is to ensure that if technology provides any new form of electronic authentication which is

a) considered reliable and

b) appropriately notified

then such techniques can be used as legally recognized means of authentication of electronic documents.

The reliability of such techniques are measured under the following criteria, namely,

(a) the signature creation data or the authentication data are, within the context in which they are used, are linked to the signatory or , as the case may be, the authenticator and of no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfills such other conditions which may be prescribed.

By this section the Government has retained the flexibility to make use of any new techniques that may be discovered or invented in due course. At present however the Digital Signature technology based on hashing and asymmetric cryptosystem remains the only form of authentication legally recognized in ITA 2000 as well as ITA 2008.

## How To Use Digital Signatures

If one has to use digital signatures to authenticate an electronic document, he needs to

a) Obtain a Digital Certificate from one of the licensed certifying authorities in India

b) He should possess an appropriate software to apply digital signature on a given document.

## Obtaining a Digital Certificate

Under the ITA 2000/2008, the Government of India has appointed a "Controller of Certifying Authorities" (CCA) as an apex authority to manage the Digital Signature system in the country. The CCA is called the "Root Certifying Authority" in India. CCA has so far licensed several other agencies/Companies as licensed Certifying Authorities to issue Digital Certificates to the public. The Certifying Authorities presently operating in India are

1. Safescrypt (Subsidiary of Sify.com)

2. N Code (Division of GNFC)

3. e-Mudhra CA, (Division of 3i Infotech)

4. NIC (National Informatic Center, a division of Department of IT, GOI)

5. IDRBT (Subsidiary of RBI)

Details of the websites of these Certifying Authorities is available at www.cca.gov.in

Out of these agencies, NIC issues digital certificates only for Government servants, IDRBT issues digital certificate only for Bankers and Department of Customs issues digital certificates only for exporters for Import Export documentation. MTNL issues digital certificates for its customers in Mumbai and Delhi. Other members of the

public can obtain the digital certificates from Safescrypt or TCS or N Code or e-Mudhra.

The Certificates are issued with different classifications at different rates. It may normally cost around Rs 900 per annum.

For obtaining the certificates, intending persons have to apply to one of the agencies along with documents such as their ID proof and address proof. After approval of the documents and receipt of payment, the Certifying authority will provide a special password and invite the applicant to receive the digital certificate through a designated web page. The applicant has to himself enter the web page and pick up the certificate. The Certificate gets installed in the computer.

While generating the certificate the user's computer generates a random pair of keys

one of which is called the "private key" which is held in the computer of the user and used for the encryption of a hash code for the purpose of "Signing". The other key called the "Public key" is picked up by the certifying authority and embedded in an electronic document called "Digital Certificate" which contains the name and other particulars of the holder. At the end of this process the holder is called the "Subscriber" of a digital certificate and gets the legal power to use the private key associated with the certificate for the purpose of affixing digital signature.

In a premium digital signature service called "Secured Digital Signature", the private key is stored in a USB device or a Smart Card which the user can remove from the computer and keep safely. Whenever the

user has to apply the digital signature, he has to use the USB device or the Smart Card.

While installing the digital certificate in his computer, the user has to also download and install the digital certificate of the Certifying authority who issues the certificate as well as the digital certificate of the CCA. The legal authority for the signature flows from the CCA to the Certifying Authority and onto the subscriber.

In order to use the digital certificate for the purpose of signing, the user needs a suitable software. normally if an user wants to sign an e-mail, the popular e-mail applications such as Outlook Express or Thunder Bird etc are capable of using the available digital certificate and affix the digital signature on an outgoing e-mail. These applications can also check the digital certificates in the

incoming e-mails. Similarly the Microsoft Word application can be used for digitally signing a word application. In certain transactions such as submission of IT return or Corporate return (MCA returns), the Government has enabled digital signature usage in the respective websites. In case a user has to sign any other document, he needs to obtain suitable applications.

# Chapter No 6

# Cyber Crimes Under ITA-2008

Crime and Law are closely interrelated. The basic definition of Crime is that it is an activity, which the society considers as "Wrong". The society considers certain acts wrong because it disturbs the harmony and peace in the community. The governing body of the society therefore decides that if the society has to remain in peace, there is a set of rules to be followed. These are the "Laws" of the society. Any one violating the "Law" is said to commit a crime. In order to provide sanctity to the law, there is an "Enforcement Mechanism" that "Punishes" the person who commits a crime. In order to examine and decide whether a crime has really been committed, there is a body called "Judiciary".

In practice however, the society cannot always determine the law first before it starts its activity. Hence, the society starts off without any laws in the first place. Soon the members of the society realize that certain types of activities indulged in by certain persons are creating problem for others and in the larger interests of the society, the activities are to be regulated or banned. The elders in the society then get together and "write the law". In such a case when does an offensive act becomes a Crime? Is it when an "Anti society activity" is committed? Or when the activity is declared "Illegal?" . There are cases when a law is written with "Retrospective" effect. In such a case, an act becomes a crime after it has been committed because the "Law" says so. The reverse of this is also true. i. e. An act, which is a Crime

today, may be declared “legal” due to the retrospective change in the law.

When we talk of a “Crime” therefore we need to understand that we speak with reference to the prevalent laws to which the society belongs.

In the Real world society (Meta Society), we know that Crime can be committed against a Person, his Personal Rights or his Property. Crimes against the Person are Assault, Murder etc. Properties may be Movable or Immovable and crimes against them are activities, which deprive the person of the use of the property to its full value. In between these two there are “Rights”. Certain rights are like “Contractual Rights” which is a proxy to the “Physical Property”. For example, “Right to Receive Money” is a “Proxy” to money. Right to live in a house is

similarly, a proxy to the right of usage of the Immovable Property. There are also other kinds of “Human Rights” such as Freedom of Speech, Privacy etc.

In the Cyber World also, crimes can be defined with reference to this general understanding of what is a Crime. However, since there is no “Physical Existence” in the Virtual world, a murder or injury similar to what happens in the Meta society may not happen in the Cyber society. If a person hacks into a hospital network changes diagnosis of a patient and causes his death due to wrong administration of drugs, it would amount to a "Murder in Physical Space caused through Cyber Space activity".

Cyber crimes may be committed on “Virtual Property” as well as “Meta Society

Property". For example, a "Web site" is a "Virtual Property". If some body destroys a web site, it is a crime against the "Virtual Property". On the other hand if some body uses your credit card number to fraudulently purchase on the net, it will deprive you of the meta society property of "Bank Balance". It is therefore a crime against a meta society property but committed on the Cyber space.

It is like an Indian picking the pocket of another Indian while both are in Saudi Arabia. Now it is necessary to determine whether a Crime has been committed and if so what is the extent of the crime and the relative punishment. It is also possible to debate whether the punishment has to be based on Indian law or the Saudi Law, and tried in an Indian Court or a Saudi Court.

We can also imagine a case where an Indian picks the pocket of a Saudi Arabian in Saudi Arabia. or conversely, the pocket of an Indian is picked by a Saudi Arabian in Saudi Arabia. In this particular case, the act of pick pocketing may be against the law of both India as well as Saudi Arabia.

Situation would be more complicated when the dispute is between an Indian and an American occurring in the Saudi Soil.

In such cases, the crime has been committed against a member of one society- Indian or Saudi Arabian or American by another in Saudi Arabian territory. In such a case, should the hands of the pick -pocketer be cut off as per the Saudi Arabian law? Or should he be punished as per Indian law? or the US law? would be an issue.

Since the Crime has been committed in Saudi Arabia, should the person be tried in Saudi Arabia, or should he be handed over to the Indian or US law enforcement authorities? Or should it be simply Ignored? .. are points to be determined.

A similar dilemma often confronts us when we discuss Computer Crimes. To add to the complications, here we have interplay of three societies, namely the Meta societies of the victim and the criminal as well as the Cyber society. If the Cyber society is also bifurcated into two parts, depending on the "Control" of the local governments, we will have a Cyber society attached to the Meta society of the victim and the Cyber society attached to the Meta society of the Criminal. An example would be when a Chinese

national plants a virus and damages the property belonging to an Indian.

The determination of what is a Crime in Cyber transactions is therefore very complicated. It requires the alleged criminal act to be weighed against the laws of different countries (since we still donot have a law for the Cyber society as an independent entity). What we therefore discuss in the rest of this Chapter are Crimes "Relative to the laws which are generally prevailing" in most countries.

With reference to India, Cyber Crimes are mainly relative to what the Information Technology Act-2008 has defined. In countries such as Malaysia and Singapore also separate acts in the style of "Cyber Crimes Act" have been enacted. There are many countries including USA which relies

mainly on the “Meta Society Laws” to determine what is a Crime or not, using “Cyber documents” as “Equivalents” to the written documents. Hence when an American court looks at a Napster case, its view may be substantially influenced by the Copyright provisions in the Meta society.

However, in India, it is a common practice for the Police to charge an alleged criminal of a crime both under the ITA-2000 as well as other laws of the country such as the Indian Penal Code, Copyright Act etc. All offences that are defined in statutes other than ITA 2000 but committed with the use of Cyber property such as a Computer or an Electronic Document are also considered generally as "Cyber Crimes" (may perhaps be Called Non ITA Cyber Crimes) though they are tried under the respective statutes.

With this background on the "Theory of Cyber Crimes", let us address ourselves to the task of understanding Cyber crimes from our immediate practical viewpoint.

## Types of Crimes:

The various broad types of Cyber Crimes that we should be familiar with are

1. Unauthorised Access to a Computer (on the Internet or on a Private network)

2. Causing Damage to the property of another person using a Computer.

3. Fraudulent use of the property belonging to others using a Computer.

4. Violation of Privacy using a Computer

5. Curbing of the Freedom of speech using the Computer.

Under the generic description of crimes mentioned above, we can specify the following popular terms by which different crimes are often described.

1. Hacking (Cracking)
2. Virus Contamination
3. Impersonation
4. Publishing obscene material
5. Cyber Squatting
6. Copyright Infringement
7. Patent Infringement
8. Cyber Stalking
9. Spam
10. Eavesdropping
12. Cyber-jacking

13. Theft of Computer/Mobile

14. Cyber Terrorism

15. Cyber War

Let's try to understand the nature of these crimes.

## 1. Hacking (Cracking):

Hacking by far is the most common of the Cyber crimes and covers a wide variety of activities. The net impact of "hacking" is that a person gets into another computer without the permission of the owner. After gaining such access, he may simply watch the contents in an espionage activity or change or destroy the contents.

Some times "Hacking" can be without a criminal intention to damage the data on the

computer but it may result in such damage accidentally.

Historically, the term “Hacking” has been associated with the activity of finding out security loopholes in software or hardware systems. Those who were otherwise entering the systems with criminal intent were referred to as “Crackers”. “Hacking” was therefore was considered a respectable service to the Cyber community.

However in the recent days, the common man’s perception has undergone a change and the term “Hacker” is today used for a "Cracker" and he is considered a “Criminal”. This view was legally forced since the Information Technology Act 2000 had actually defined “Hacking” and proceeded to prescribe a punishment for the same under Section 66. The naming of section 66

offence as "Hacking" has however been removed in ITA 2008.

For immediate reference, the relevant sec 66 of the Act can be recalled here. Please note that the offence under Section 66 of ITA 2008 has now been defined in association with Section 43 of the same Act and hence we need to look at both sections simultaneously.

Sec 66 states as follows:

> ***66: Computer Related Offences:***
>
> ***If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.***

***Explanation: For the purpose of this section,-***

***a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;***

***b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.***

Section 43 States

***43: Penalty and Compensation for damage to Computer, Computer System, etc***

***If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network -***

***(a) accesses or secures access to such computer, computer system or computer network or computer resource (ITAA2008)***

***(b) downloads, copies or extracts any data, computer data base 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,***

***(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means***

***(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,***

***he shall be liable to pay damages by way of compensation 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 Database" 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, data or instruction is executed or some other event takes place in that computer resource;***

***(iv) "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.***

***(v) "Computer Source code" means the listing of programmes, computer***

***commands, design and layout and programme analysis of computer resource in any form***

As can be observed, the Indian Act covers "Unauthorised acts" as defined under Sec 66+43 as a crime punishable with imprisonment and fine. At the same time "Unauthorised Acts" are also covered as civil wrongs and entitles a right on the affected person to claim damages.

One can also observe that Sec 43 covers "Assistance to contravention". This clause is of importance since many of the computer related offence take place with the knowledge of a "Password" which is extracted in some casual conversation with an "authorised employee" or because of the weak security measures employed by the systems manager. In all such

cases of “Negligence” on the part of a user or a systems manager, one can allege “Assistance-intended or unintended”.

Other than through such assistance, “Hacking” can be done through “Guessing” of a password, or through “Cracking” the password through a “Brute Force Attack”, which is a systematic attempt to try and find out the pass word through trial and error.

"Assistance" becomes "Abetment" under section 84B when there is "instigation" or "Conspiracy".

We may also observe that Section 66 applies even when the system owner may not have suffered any harm but it is somebody else who suffers the harm. It is also notable that the section is applicable irrespective of the "means" used to cause harm.

The use of the word "Diminishing the value" or "Diminishing the Utility" is again general description of the effect of the offence and can be applied to a wide variety of offences such as "browsing through a confidential document", "Implanting a Virus or Adware/spyware or spamming which reduces the utility of the system".

The Indian law has also provided for some systems to be declared by the Government as “Protected Systems” and an attempt to access such systems can be punished with an imprisonment of 10 years.

There are software that helps in such “Password Cracking” and development and distribution of such software could be treated as “Assistance for Hacking”.

In order to prevent hacking, it would be necessary for the system owner to install a suitable hardware or software "firewall" that is configured to allow only authorised persons to the Computer.

## 2.Virus Contamination:

The second most prevalent Cyber Crime is creating and distributing "Virus" which causes damages of various kinds. "Virus " by definition is a computer programme that can "Reproduce itself" while residing in a target computer. Subsequently it may "Attack" causing destruction of data. It may also distribute itself, enter other computers in the net work through e-mail or otherwise (like a worm that crawls into other computers) and later repeat the process in the new "host computer".

Over the years, “Virus” has become a matter of great concern to the society and is being used as a tool for hacking or for disabling vital E-Commerce services and Corporate networks.

A virus normally attaches itself to a programme through a “security hole” or enters a computer piggy backing on an e-mail or a web page. Once inside a computer, it may get activated through some pre programmed trigger. Some viruses get activated on an appointed day. Some come in disguise and get activated when a seemingly friendly file is opened. Once activated, it occupies a vacant space on the hard disk. Some are programmed just to replicate themselves and cause the hard disk to crash. Some are programmed to alter the functioning of other programmes temporarily

or permanently. Some alter one class of files by renaming all of them or deleting them from the system.

A few viruses enter like a “Trojan Horse" and wait for an appointed time to attack. Such Trojans are some times sent to thousands of computers and triggered to attack a target computer simultaneously, rendering the attacked computer dysfunctional. This is called a “Distributed Denial of service attack” normally employed against popular e-commerce sites shutting them off as long as the attack lasts. Such attacks are also employed for a conducting a “Brute Force attack” to crack a password. Some specialize in identifying when the user enters a Bank or e-mail website and try to capture the log in ID or password by capturing the key strokes (Key

Loggers). Some employ a method called "Phishing" and lure the victims into a false web page disguised as a known website and capture the login data entered there in by the user.

A technology called "Steganography" (hiding one file in another) may also be employed for sneaking in a malicious virus as a file embedded in a picture or some other file.

The viruses that get distributed through e-mails or participate in distributed operations may render the victim himself as an “accomplice” to a crime using him for further distribution. In resolving Cyber crimes such technical issues have to be carefully examined so that innocent persons are not charged with crimes which they have not committed.

Creating a virus and leaving it in the wild is a recognized Cyber crime, which calls for a strong punishment. In India, it is specifically covered under Sec 43 of the Information Technology Act. Under Section 43, computer programmes which function without permission of the owner and send data out of the machine or otherwise affect its functioning is referred to as a "Computer Contaminant" and is treated on par with a "Virus". The remedy under this section is for the victim to file a complaint to the adjudicator appointed under the ITA 2000 to recover the damages if any.

Virus introduction is also be considered as a Section 66 offence and made punishable.

In order to protect oneself against the attack of a virus, it is essential to install the latest virus protection software and keep it

updated. Not providing a network with the appropriate virus protection could be construed as negligence of a net work manager and consequent damages if any.

**3. Impersonation :**

Impersonation could usually be a means of committing a financial fraud. In the simplest form it could be a case of entering an ISP service using a stolen password. In a more serious version, it could be using somebody else's credit card information to buy on the Net. In another version of impersonation, it could be a means of disguising and committing a crime such as hacking or virus introduction.

In all such cases, the criminal provides an identity when asked that is false and is aimed to deprive the genuine owner of the identity

of a “right”. It would involve telling a lie to get a financial gain and therefore tantamount to a fraud.

Under Section 66 D, Cheating by Personation using a computer resource or a Communication device is punishable with three years imprisonment and fine of RS 1 lakh.

One of the ways Impersonation is done at the Computer level is called “Spoofing”, where the IP address of the Computer is made to appear different so that access can be gained to other restricted Networks working with IP filters.

Impersonation normally follows an "Identity Theft" which may involve password theft or extracting personal information through a phishing attack.

Identity Theft is also separately covered under Section 66C under which

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

## 4. Publishing of Obscene Material:

We have already discussed the offence resulting from "Obscenity" in the earlier Chapter 2 under Section 67, 67 A and 67 B.

Additionally ITA 2008 also has a section on Video Voyeurism under Section 66 E according to which

*"Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both"*

## 5. Cyber Squatting

Cyber Squatting is a term, which has come to be associated with the registration of domain names without the intention of using them, in the names of popular brands or personalities solely for the purpose of making money.

The key ingredients are that "Name" belongs more appropriately to another entity.

Second the registrant is intending to trade the name.

Domain name registration system started on the basis of the "First come first served" basis.". The registrant authority, did not take the responsibility for checking the ownership of the name.

However, as the Internet became more popular, large popular companies wanted to enter the Internet with their own web sites and often found that the domain name they were seeking had already been booked. Some of these companies bought the names for a price, which were sometimes astronomical.

The increasing cost of buying back of domains resulted in "Meta Society" trade mark owners coming together and claiming

that their intellectual property rights on a registered trademark should be extended to "Domain Names". This has redefined the registrants ion of Domain Names without the intention of using them as "Cyber Squatting".

In an effort to prevent cyber-squatting, some countries have imposed limitations on registration of domain names. These limitations include restrictions on the choice of domain name, such as requiring the domain name to match the registrant company's name or to contain no generic terms. In some cases, a certain time is reserved for trade mark owners to register the domain names after which the registration is thrown open for others.

USA has passed a specific law regarding the domain names called the "Anti- Cyber

Piracy Act" to define the rights on Domain names.

The Act establishes that a registrant of a domain name may be liable to the owner of a trademark or others that may be affected by the "bad faith" of the domain name registrant.

The Act defines bad faith to include:

> *"the person's offer to transfer, sell or otherwise assign the domain name to the owner of the mark for financial gain without having used or (having) the intent to use the domain name in a bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct."*

The Act applies to domain names registered both before and after the Act's effective date (November 29, 1999).

The Act further provides that the owner of the domain name

*" ... shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act."*

There is no such specific law regarding Domain Name rights in India.

In the absence of any law, disputes regarding Domain Names are resolved through the Uniform Dispute Resolution Process (UDRP) that the Registrants have agreed to practice. The WIPO has been supporting the Dispute Resolution based on "Trade Mark Rights". Disputes are mainly resolved through an "Arbitration Process".

In India there have been cases like Rediff.com Vs Radiff.com, Yahoo Vs yahooinida.com and between ICICI and LIC on www.jeevanbhima.com which have come up for scrutiny in Courts. The Rediff case was decided in their favour and the name www.radiff.com was held to be confusingly similar to their name and forced to withdraw. Similarly yahoo also won its case against an Indian registrant of yahooindia.com. ICICI and LIC settled their disputes out of court. Another case between an Indian registrant of www.indiainfospace.com was decided in favour of infospace.com, through an uncontested arbitration in WIPO. These could be conceptually like Cyber Squatting disputes.

Settlement of disputes regarding .in domain names is done through INDRP process

similar to the UDRP process through arbitration.

## 6. Copyright Infringement:

Copyright Infringement arises when the rights of the owner of a Copyright material are infringed by another. On the Cyber world, it can happen through copying of Web content without permission or reproduction of a copyrighted physical society material (songs or articles or books) in electronic form.

Copyright infringement happens either as "Piracy" or "Violation of Rights". Piracy is when there are no rights and the material is put to commercial use. "Violation" happens when there is some right but there is a dispute as to whether the use is within the interpretation of the "Permitted Rights" or

not. Where there is no specific Contract the benchmark would be what is called " Fair Use".

The main remedy for Copyright infringement is "Compensation" to the Copyright owner. However most copyright laws including the Indian Copyright Act as well as the Digital Millennium Copyright Act of USA, provide for imprisonment and fine in certain cases. It is a matter of debate when the harsher punishments are to be invoked. It should be ideally left to the discretion of the Judge on the basis of the specific case.

## 7. Patent Infringement

Patent is a Right created out of specific registration of an Invention with an appropriate authority. Patents can be registered within the jurisdiction of a

country. Priority for the date of invention and common examination system can however be invoked through International treaties such as the Patent Cooperation Treaty. (PCT)

India is a party to the PCT but has not yet established a full Software patent System.

The remedy to a patent Owner for infringement of patent rights is compensation for the loss caused by the infringement.

Information Technology Act –2000 doesnot cover the Patent infringements. The Semi conductor Act however covers Patent procedure for "Electronic Layout Designs" and prescribes a punishment of a fine of upto Rs 10 lakhs and imprisonment upto 3 years.

## 8. Cyber Stalking

Cyber Stalking is a term used for following a person while he is on the Net observing where he goes and what he does on the Net. This can be done by a marketing agency to profile a potential customer or by a potential criminal in search of information that can be sued to commit further crimes. The effect of stalking is to annoy the person stalked.

Cyber stalking is normally considered a "Privacy Invasion" and if it is done with the intention of committing a crime, the normal laws have to take care of the punishments. Laws are yet to be developed specifically for controlling this type of crime.

In USA, Federal laws are being attempted to punish "online Stalking". Several states

already have some laws for the real world which can be invoked for “Cyber Stalking”. In California, the criminal penalty for stalking is imprisonment for up to a year and/or a fine of up to $500. If the stalker pursues the victim in violation of a previous court order, the punishment may be two to four years imprisonment. In Canada, stalkers may be imprisoned for up to five years. In California, one may request to be notified 15 days before his stalker is released from prison.

Under Section 66 A, ITA 2008 penalized by three years imprisonment and fine for sending by means of a computer resource or a communication device,

a) any information that is grossly offensive or has menacing character or

b) any information that the person knows to be false but sends for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will by persistently making use of a computer resource or communication device

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.

(P.S: Section 66A is since scrapped by Supreme Court and is expected to be replaced in due course)

## 9. Spam

Spam is another Privacy Invasion crime where "Unsolicited e-mails" are sent to a

person. Normally “Spam” will be a bulk mail without a “Return” address.

Apart from causing annoyance, a Spam imposes a financial burden on the receiver since he has to spend money and Internet time to see the Spam mail even before discarding.

Anti Spam laws are also under development and usually it holds the “Spam Server” owner responsible for paying compensation to the affected person.

The US Federal anti spam law is under consideration. Many states have however passed laws that prescribe imprisonment upto 3 years and fine upto US $ 10000 for Spamming.

Under Sections 66 (C) of ITA 2008, "Spamming" under false sender's address is punishable.

## 10. Eavesdropping

Evesdropping happens along with a "Hacking Crime" where an unauthorised person watches the communication flow between two persons. The Communication could be an e-mail or a dialogue between the browser and a web server. Typically it may relate to forms containing vital information being submitted by a person to a trusted website.

It is to prevent such possibilities that digital signatures and cryptography are used.

ITA 2008 provides certain powers to designated security agencies to intercept, monitor, decrypt any message under Sections

69, 69A and 69 B. Other than by such authorized persons, interception by any other person will be considered as "Unauthorized Access" and therefore becomes punishable.

## 11. Espionage

Espionage is also a hacking activity done for the purpose of collecting confidential information. It may be done either by entering the confidential area of a website or a Corporate Intranet through password theft or otherwise. It can also be done by introducing Trojans into the system that collects information and sends it out the owners.

## 12. Cyber-jacking

Cyber Jacking is a term used when the http packets meant for an address are diverted to a wrong destination through manipulation of

routers and registers in between. Imagine for example that the domain name www.basmati.com belongs to a well known Indian basmati rice manufacturer. When you type the URL accordingly, if the router sends you to another server maintained by a competitor, you may be browsing through the site without knowing that it is a fake site. The genuine site may however may still exist in a server. Such Cyberjacking can even be selective in the sense that only visitors from Pakistan may be directed to the fake site while others may continue to reach the genuine site. The diversion may even be intermittent so that the genuine site may not find out a significant fall in sales while the fake site may be clandestinely hijacking the orders.

Such crimes are a combination of hacking and Fraud and need to be treated accordingly for the purpose of law.

## 13. Cyber Terrorism:

ITA 2008 has defined the offence of "Cyber Terrorism" under Section 66 F of the Act as follows:

***(1) Whoever,-***

***(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –***

***(i) denying or cause the denial of access to any person authorized to access computer resource; or***

***(ii) attempting to penetrate or access a computer resource without***

***authorisation or exceeding authorized access; or***

***(iii) introducing or causing to introduce any Computer Contaminant.***

***and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or***

***(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by***

***means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,***

***commits the offence of cyber terrorism.***

***(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.***

It may be noted that any one held as an accomplice of a terrorist activity in India will also be punished with the same punishment of "Life Sentence". In the event the activity results in a terrorist action on physical space causing death such a person may also be liable for punishment under IPC also.

## 14: Cyber Wars

The term "Cyber War" is normally associated with an action by one Government resulting in damage of the Information property belonging to another country. It is used as a part of the conventional war strategy to launch parallel

attacks on the Cyber economy of an enemy country.

Some time non state actors also do indulge in such activities under the pretext that it is a defense of national interests. However such activities may have to be classified as Cyber Terrorism by the other country instead of Cyber Wars.

## 15. Theft of Computers, Mobiles etc.

One of the unique features of the amendments to ITA 2000 brought by ITA 2008 is the introduction of a section 66 B, according to which

> ***"Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or***

***communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both."***

This particular section criminalizes the act of receiving, retaining a stolen computer or Mobile. The actual theft may still have to be covered under IPC.

The varieties of Crimes that can be committed under the banner of Cyber Crimes are endless. Until laws are established to deal with them, the Meta Society laws will be applied to the Cyber Crimes.

Information Technology Act 2000 not only defines the crimes and the associated punishments but also defines an "Adjudication Procedure" where the

Government can appoint an adjudicating officer to conduct an enquiry and award compensation for the victims of Cyber Crimes for the financial loss suffered by them. The Criminal offences are prosecuted by the Police.

Some times the "Freedom of Speech" is misused to run "Rogue Sites" that carry messages aimed at hurting the sentiments of sections of the society or affecting the sovereignty and integrity of a Country. The Governments have in turn reacted with "Cyber Patrolling" and "Censorship" raising the cries of "Privacy Invasion".

Criminals also use Social Networking sites such as orkut.com, youtube.com etc to carry out their criminal activities. handling such crimes where the Intermediaries provide the platform for commission of a crime and help

their members to operate under hidden IP addresses etc as a part of "Privacy protection" is a matter of serious concern in Cyber Crime prevention.

The handling of such anti social elements on the Net is a challenge to the Governments across the Globe. To handle such high tech crimes, the enforcement authorities in each country are creating special cells with appropriate skills. Besides the Cyber Police, countries are creating a network of Cyber Informers who help them patrol the Cyber space. Countries have also come up with “Computer Emergency Response Teams” that provide technological support to the Community to fight Cyber crimes.

ITA 2008 has provided for creation of a suitable agency to undertake interception, monitoring and decryption of data in storage,

or transit if required in the interest of National security or to prevent commission of Crimes. An Indian Computer Emergency Response team is also being designated to address the issue of securing the "Critical Infrastructure Resource" to be notified by the Government under Section 70 of the Act.

ITA 2008 has also provided a few sections specially to prevent misuse of the Digital Signature system under Sections 71, 73 and 74. Accordingly, "Misrepresentation" for obtaining a digital certificate, "Using a certificate with false particulars" and using a digital certificate for "Fraudulent purpose" are offences carrying an imprisonment of 2 years and fine of RS 1 lakh.

# Data Protection

In order to provide for security of information and to protect "Privacy" of individuals whose "Sensitive Personal Data" may be handed over to Companies and Intermediaries for various purposes, ITA 2008 has provided "Civil" and "Criminal" punishments.

Under Section 43 A,

> ***any body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall***

***be liable to pay damages by way of compensation, to the person so affected***

Under Section 72 A, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

Additionally, Section 72 also states that if any authority which obtains certain information in pursuance of powers

conferred under this Act breaches the privacy of the data collected, the offence is punishable with imprisonment upto 2 years.

## Responsibility of Intermediaries

ITA 2008 empowers the Government to prescribe norms for data retention under Section 67C and also to intercept, block and call for traffic data information under Sections 69, 69A and 69B. Under Section 79, Intermediaries are also required to follow due diligence failing which they will be held vicariously liable for offences committed using the facilities of the Intermediary.

## Responsibility of Digital Certificate Owners.

ITA 2000/2008 requires applicants of digital certificate to ensure that they donot "misrepresent" while obtaining the digital

certificates. They are also required to ensure that the particulars in a digital certificate are not false or used for fraudulent purposes. Otherwise he will be liable for imprisonment of upto 2 years.

Subscribers of digital certificates are also expected that if they come to know that the confidentiality of the private key is compromised, then they should ensure that the certificate is revoked. Otherwise they may be liable for the fraudulent use of the compromised key.

## Powers of the Police

Under ITA 2008 all offences for which the imprisonment term is not less than 3 years is considered "Cognizable" and "Bailable". An officer of the rank not below the rank of an Inspector can investigate any offence under

the Act and also search, seize or arrest a person in a public place in the event an offence is being committed.

Under ITA 2000, the powers of investigation were only with the Police officers of the rank of DySPs. With the change in ITA 2008, it has become necessary for all Inspectors to be adequately trained in the handling of Cyber Crimes.

## Information Security Structure

In order to introduce the Information Security provisions of the Act under ITA 2008, the Act prescribes that the CERT-IN is designated as a "Nodal Agency" for the security of Critical Information Infrastructure and to issue necessary guidelines to the Industry.

## The Problem Of Jurisdiction:

One of the important problems in prosecuting Cyber Criminals is the jurisdictional problems that arise both at the investigation stage as well as the trial and stage. Even after the trial, enforcing the decree also could be a problem. The problems may arise first due to non cooperation of different Countries involved as well as the lack of uniformity in defining the crimes. Even though the adoption of the UNCTRAL model by most countries has brought in some uniformity amongst the countries, in matters such as "Obscenity" , "Spamming", Cyber Squatting" etc, there is still a wide difference in the interpretation of different countries.

There is therefore some attempt for different countries to establish "Cyber Crime" treaties.

The European countries have been the first off the block in this regard and developed a "Draft Convention" on Cyber crimes. The union is also discussing with the US to extend the convention to the American continent. India is yet to take part in such initiatives.

The ITA-2000 has made an attempt to vest extra territorial jurisdiction to the Act since as per Sec 75 of the Act, persons outside India and even those who are not Indian nationals would be liable under the Act. The establishment of Treaties is therefore of utmost importance to give effect to the provision.

## Evidentiary Challenge

In addressing the issue of prosecuting Cyber Crimes, it is necessary to ensure that

appropriate evidence is collected and presented to the Court. Section 65B of Indian Evidence Act introduced with ITA 2000 enactment provides an excellent means of providing admissible evidence in Cyber Crime cases. Cyber Evidence Archival Center ( www.ceac.in ) provides services connected with collection and presentation of cyber evidence.

Under Section 79 A of ITA 2008, Government may also notify for the purposes of providing expert opinion on electronic form evidence before any court or other authority, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence by a notification. Such an examiner is expected to be used by the Police as an "Expert" where required.

## Civil Liabilities

Under Section 43 of ITA 2000/8, (quoted earlier in this Chapter), a person who contravenes the provisions of the Act is liable to pay compensation to the person who suffers a wrongful harm. There is no upper limit for the damages that can be claimed under this section.

The process for claiming damages under this section is to make an "Adjudication" application to the "Adjudicators" appointed for this purpose in every State. (IT Secretaries of the State are designated as the Adjudicators for the respective State). The adjudicator who has the powers equal to a Civil Court will follow a simple procedure (not bound by Civil Procedure Code) and arrive at a decision mostly within 4 to 6 months. An appeal against his decision can

be made to the Cyber Regulations Authority also a special mechanism created under the Act. Further appeal goes to the High Court.

Where the damage claim is in excess of Rs 5 crores, the complaint has to be made to a Civil Court of appropriate jurisdiction.

## The Takeoff:

Cyber Crimes are therefore well recognized in India and the Law Enforcement Authorities are keen on enforcing the same. Simple procedures have been introduced to approach the "Adjudicator" in every State and Union Territory for redressal of grievances coming under Civil Wrongs.

Crimes coming under "Offences" can be pursued with the Police for which a Complaint has to be made to the nearest Police Station. In some states such as

Karnataka, Cyber Crime Police Stations have been specially set up to address Cyber Crimes and complaints have to be made to them.

A Netizen should be aware that there is not only protection and remedy available to him if his rights are infringed but he also may be made accountable if he transgresses the law even innocently.

Where required Cyber Crime Complaints and Resolution Assistance Center (CCC-RAC) of Naavi.org provides information, litigation and mediation/arbitration assistance to resolve cyber disputes. (Refer www.ccc-rac.in for details)

# Chapter No 7

# Law Regarding Websites

Websites are the most important element of the Cyber World that the Netizen has to interact with. Even the first timer to the Cyber World is aware of the website of google.com or yahoo.com where he avails the e-mail services or vsnl.com or sify.com where he avails the web access services.

In this Chapter we shall briefly discuss the legal aspects of maintaining a website.

## Understanding the Website:

Website is a group pages that are accessible to a person connected to the Internet. The access is made possible by placing the pages in a "Web Server" which is a computer connected to the Internet and having a published address. The address that a

Netizen normally uses to access a website is the "Domain Name" e.g.: www.naavi.org . The technical system of Internet however uses a different address format called "IP Address". e.g.: 202.71.128.194 . The domain name is easy to remember but the machines find the number format of the IP address more convenient to function. The "Domain Name Service" or DNS enables conversion of the domain name you type on the browser into the IP address.

## Home Page:

Any website contains a group of pages. Each of this page is a file normally written in "Hyper Text Format" and expressed in htm or html extension code. Today's browsers can also open some other formats of the files such as word or pdf etc. In recent days websites are also maintained like a database

of files and when a particular page is required it is retrieved from a data base. Such pages may appear in the .asp format also. However, each page which you see on the Internet has a unique location and it is called the "URL" or "Uniform Resource Locator". Normally when you type the name of a website as the URL in the browser, you are connected to the host computer containing the relevant pages and in particular to a page called index.html by default. (Some host computers may be configured to open default.htm or index.htm by default). This therefore becomes the first page that a Netizen sees when he types the website name such as www.naavi.org Such a page is called the "Home Page" of the website.

# Hyper Links

Normally the website is structured so that the home page provides the navigational links to other pages available in the website. Such links can be placed not only to pages within the same host computer but also to outside the host computer. It can even link to another website or even a distinct file such as an image file or a document file situated anywhere else on the Internet.

Such links are provided through some reference objects in the website and are referred to as "hyperlinks".

A Website is a bundle of web pages reachable through a domain name and interconnected through hyperlinks and may also contain hyper links outside the website.

With this introduction, we shall now explore the legal aspects pertaining to the maintenance of the websites.

We have in the previous Chapter on Cyber Crimes referred to some crimes where websites were involved and they are relevant now for discussing the legal aspects regarding websites.

In India, the only law that was passed with specific reference to the Cyber World was the Information Technology Act 2000 (ITA-2000). This act however covered only aspects covering Digital Contracts and hence ignored the legal aspects covering websites in particular. We therefore have to interpret the laws regarding the websites by appropriate interpretation of the various provisions of the ITA-2000 and the laws of other countries.

ITA-2000 defines the terms such as "Electronic Record" and proceeds to define various legal provisions affecting the electronic documents. The definition of "Electronic Record" includes a webpage and hence each of the web pages represents a legally recognizable written communication. It is attributable to the person who authorized the publication. The legal liability of the webpage therefore falls on the owner of the website.

Though the web page is not normally "Digitally Signed", it is a legally recognized writing and can be proved say by third party evidence such as provided by www.ceac.in

## Accountability for Web Content

The ownership of the "Content" of a website therefore needs to be determined by a

suitable contractual arrangement. Normally website creation involves some technical work and is assigned to a website developer. The Content creator hands over the content that should appear on the website to the website designer and the website are created. Further changes on the website are also made by the content owner in similar fashion.

Some times the meaning of a content can be altered by the way it is presented...just like how news paper stories mean different from the report when you look only at the headlines. In such cases certain issues may arise on the accountability for the correctness of the report and possible defamatory consequences.

For example, look at the following sentence:

" George Bush was foolish in attacking Iraq"

This sentence may look defamatory and the content producer may be held responsible. However, if you see the sentence in greater detail, it actually reads

" George Bush was not foolish in attacking Iraq"

The word "not" was not visible to the common eye in the first sentence since the designer had given it a colour which was similar to the background color. This could have been a mistake or a consequence of the designer or the reader being colour blind to a specific contrast of colours.

One of the fundamental legal issues in maintaining a website is therefore determining the inter-se responsibilities of

the Content supplier and the designer. In a "Portal" scenario the issue may be further complicated because the content supplier may be an individual who supplies an article to the portal publisher where an editor makes some changes and submits it to the designer who puts it up on the website. In all such cases therefore there needs to be a "Contract of Content Supply, Design and Publication" which determines the legal liabilities of all the parties involved.

## Copyright

In an extension of what has been discussed in the previous paragraph, the content published on a website is a subject matter of "Copyright" which primarily belongs to the "Author". The publisher may however get some rights by virtue of the author consenting for the publishing but whether

such right is absolute or restricted depends on the contract between the publisher and the author.

If the publisher or the portal owner has not clarified the inter-se rights of the author and himself either through a separate contract or a suitable publishing of the "Terms and Conditions" on the website, there could be legal complications arising out of what happens to a published material on the website at the post publishing stage.

For example, an author may agree to let his article appear in the website of "Economictimes.com" but may not like it is reproduced in "Indiatimes.com" though both belong to the same group. He may also not like the article to be available for free reproduction or copying while the website

might not have provided such a general notice.

These issues have to be resolved if web publishing has to be free of unwarranted disputes.

## Domain Name

Domain name being the main identifier of a web site is subject to frequent disputes. Often the dispute may be with another website owner who possesses a similar domain name or with somebody who owns a trademark in the physical society which is similar to the domain name.

Normally the domain name registrations are subject to an agreement by the person registering the name with a "registrar". Such agreement provides that any dispute is subject to a "Uniform Dispute Resolution

Policy" (UDRP) prescribed by the ICANN (Internet Corporation for Assigned Names and Numbers). The UDRP normally favours those who have a "Trade Mark Right" that can be established through documentation.

Readers are advised to visit www.icann.org and www.verify4lookalikes.com for further information. Naavi.org also contains many discussions on the subject which can be perused.

## Patent

Patents are a form of "Intellectual Property Rights" (IPR) similar to Copyright and Trade Mark. It is a right that is obtained by registration with an authority for a novel idea that has some industrial use and granted to the inventor. Once a Patent is granted and registered, it gives an exclusive right to the

Patent holder to exploit the invention in the geographical location where the Patent is registered and provides him the right to sue any body else for damages if the Patent is infringed.

In the context of a website what the owners have to take care is not to infringe on other's Patents either for providing services on the website or during the process of designing of the websites. It is therefore essential that the website owner makes the web designer responsible for any patent violation regarding the tools of development. The owner himself is however responsible for the patent infringement if any in the business process adopted in providing the web service.

In view of the indiscriminate patents already issued in several parts of the world, it is not

easy to steer clear of violations whenever a person wants to do business on the net. Nevertheless this is a legal issue which could cause problems to E-Commerce sites which become popular.

## Privacy

Privacy rights of Netizens also cast some responsibilities on a website owner. Whenever a website owner provides services on a membership basis, he collects a lot of information from the members at the time of registration. According to the privacy laws that prevail in most parts of the world, only such information as is necessary for provision of the service should be collected and the information collected has to be used only for the purpose for which it is collected and should not be distributed to any body else for commercial consideration or

otherwise. It would therefore be necessary to state on the website itself the "Privacy Policy" to be adopted by the website owner to which the visitors would be bound.

The issues of Privacy, Copyright, Patent and Domain Names are not directly covered by ITA-2000. Nevertheless in view of the general legal recognition of electronic documents any other law of the country may stand extended to the Cyber world if it is not otherwise in conflict with any provisions of ITA-2000. Any website owner has to therefore keep abreast with all such laws and ensure that he is not exposing his business to the risks enumerated above.

In case the website owner is in E-Commerce and has a high stake, it would be necessary for him to undertake a comprehensive Cyber

Law Compliancy audit for his business and ensure compliancy at all times.

# Chapter No 8

# E-Governance

E-Governance represents an important use of Internet for the benefit of the society. As citizens of the society which is gradually transforming from a paper based society to digital society, it is necessary for us to be aware of how Internet is affecting Governance in the Country. E-Governance incorporates all the elements of business management of E-Commerce and a higher level of legal complication.

Citizens expect that their constitutional rights and human rights do not get abridged as a result of the Governance changing over from the traditional paper based system to the E-Governance system. Hence issues of Privacy, Information Security and

Constitutional responsibility become part of E-Governance.

Considering the importance of E-Governance, Readers of Cyber Law need to be introduced to the subject and this Chapter is meant to achieve this.

## The Concept of E-Governance

E-Governance is a term that is used to describe the use of IT in the functions of a Government. A finer distinction can however be made between the terms E-Government and E-Governance. Under this distinction, E-Government refers to the internal Governmental functions where IT is used. E-Governance is used where there is an interaction of the public in discharge of the responsibilities of Governance.

In the Indian context E-Governance is the common term used to describe any activity of the Government including the activities where public interaction is not there.

The Governance of the Cyber Society itself may be called "I-Governance" which covers management of the domain space issues and technology standards. For the present we shall restrict ourselves to discuss the "E-Governance" and the responsibilities of a Cyber Citizen in the process of E-Governance.

The objectives of E-Governance are Efficiency, Transparency and Convenience. Efficiency would in the form of reduced cost and better information management. Transparency of operations enables the officials to interact with the public without the intermediate touts and increases the

confidence of the public in the administration. Convenience to the public is expected in the form of easy availability of information and remote interface for payment of taxes etc.

## The Process of E-Governance:

The first step in the E-Governance process is for the Government to create "Digital Records" of the information required. Many of the Governments in the era of written records had legally defined the ways in which "Government Records" can be kept. Similarly either by practice or through administrative notifications, the means of "Application", "Tendering" etc were all paper based. The relative procedures in handling these documents were also defined in a manner suitable for handling paper documents.

With the advent of Computers as a means of efficient data base creation, storage and management, there has therefore been a need to redefine the legal provision to accommodate collection, retention and management of data in digital form.

For example, the Information Technology Act-2000 of India under Chapter 3 has provided for the legal recognition of Electronic Documents and Digital Signature in Citizen- Government interactions.

Section 6 of the Act states:

**Use of Electronic Records and Digital Signatures in Government and its agencies**

***(1) Where any law provides for***

***(a) the filing of any form, application or any other document with any office,***

***authority, body or agency owned or controlled by the appropriate Government in a particular manner;***

***(b) the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;***

***(c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government***

***(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe –***

***(a) the manner and format in which such electronic records shall be filed, created or issued;***

***(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).***

Under Section 6A, ITA 2008 has provided for legal legitimacy for the use of private sector service providers for delivering the services on behalf of the Government.

The section states:

## 6A: Delivery of Services by Service Provider

***(1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorize, by order, any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify, by notification in the Official Gazette.***

***Explanation: For the purposes of this section, service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor form or any such other body or agency which has been granted***

***permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.***

***(2) The appropriate Government may also authorize any service provider authorized under sub-section (1) to collect, retain and appropriate service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.***

***(3) Subject to the provisions of sub-section (2), the appropriate Government may authorize the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule,***

***regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.***

***(4) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:***

***Provided that the appropriate Government may specify different scale of service charges for different types of services.***

Sec 7 of the Act states as under:

**Retention of Electronic Records**

***(1) Where any law provides that documents, records or information shall be retained for any specific period, then,***

***that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, -***

***(a) the information contained therein remains accessible so as to be usable for a subsequent reference;***

***(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;***

***the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in***

***the electronic record: Provided that***

***(c) this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.***

***(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Publication of rules. regulation, etc.. in Electronic Gazette.***

Section 8 of the Act states as under:

**Publication of rules, regulation, etc, in Electronic Gazette**

***Where any law provides that any rule, regulation, order, bye-law, notification***

***or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:***

It must however be stated that the ITA-2000 has not made it mandatory for the Governments to adopt to E-Governance but left it to their discretion. This option is built in through Sec 9 which states as under.

## Sections 6, 7 and 8 Not to Confer Right to insist document should be accepted in electronic form

***Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to***

***insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.***

Even though they are under no compulsion to go for E-Governance, several state Governments in India such as Andhra, Tamil Nadu, Karnataka and Maharashtra have already initiated measures to incorporate E-Governance in its administrative mechanism with a great degree of success. States like Madhya Pradesh and Kerala are also in the process of taking similar measures. At the

Central Government level, Ministry of Information Technology has set up a separate E-Governance Center to hasten up the process. The National Police authorities have made significant progress in imparting Cyber Law Education to the Police officers and developing an exclusive knowledge base for handling Cyber Crimes.

Some of the initiatives taken in E-Governance are to provide real time connectivity between the various offices of the Government so that "Decision making" can be speeded up and the loss of time in collecting and forwarding information between the State Capital and the District centers is brought down.

This stage of connecting the administrative centers with the Ministries is the first phase of E-Governance. However, in order to bring

the Citizens into the E-Governance network, several Government departments have thrown open the records meant for public consumption to the Citizens either through Internet or through specific E-Governance centers. As a result, several utility payments such as "Electricity" and "Tax" as well as Issue of Encumbrance Certificates" etc can be completed by the Citizen without the need to physically meet the concerned officials. This has not only made the system efficient but also reduced the scope of corruption.

## Auditing of Electronic Records

In a new section introduced by the Government under Section 7A, it is stated

> *"Where in any law for the time being in force, there is a provision for audit of documents, records or information, that*

*provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form"*

This provision would apply both for the Government segment and others where appropriate.

## Legal Issues of E-Governance:

Since Law and Order is an important aspect of Governance, Cyber Laws applicable to a particular country are drawn by the Government. It is therefore a " Self Governing Exercise" for those who are responsible for the regulation.

In India, while most of the laws are created and managed by the Ministry of Law and Justice, Cyber laws were an exception and

were created by the Ministry of Information Technology.

Even in the US, initially, Internet was in the hands of the Defense Department. It then moved into the domain of the Commerce department. In view of the visions of these departments being different from the vision of the Department of Justice and Law, , the process of making Cyber Laws has to circumvent many complications. Naturally, the final outcome could be less than optimum since it has to accommodate diverse interests. In the process, "Law" as it finally emerges may fail to be in consonance with the requirements of the "Citizens". It may be more keeping in view the requirements of "Officialdom" than those of the Citizens. The biggest responsibility of

Citizens is therefore to make the laws as "Citizen Centric" as practically possible.

Thus the first responsibility of a Cyber Citizen is to participate in the process of making of the Cyber Laws and contribute towards its formation in a manner that will take care of the interests of the majority of the society. Then the Cyber Laws will be "Citizen Centric".

Some of the specific legal issues concerning E-Governance are, "Citizen's Identity", "Electronic Voting", "Data Security", "Digital Divide", "National Security" etc.

## Citizen's Identity:

In any form of interaction over the Computer, it will be necessary to carry an appropriate digital identity. The best form of such identification is through a "Digital

Certificate" issued by an appropriate authority. Digital Certificate takes care of "Authentication" as well as "Data Integrity" for documents. Other authentication methods such as "Finger Print ","Iris Print" And "Signature on a written pad" can also be used in Citizen identity . They may not however be capable of "Protecting Data Integrity during Communication".

## Electronic Voting

Digital Certificates of higher class which are issued after physical verification of the identity of a person, can be effectively used for creating "Voting Identity" of citizens. If this can be translated into a voting system in elections, the cost of elections and therefore the attendant corruption can be brought down.

While the feasibility of politicians accepting this mode of voting is remote, particularly after the recent controversies in the American presidential elections, it is likely that the "Corporate sector" may soon accept voting in shareholder's meetings through digital signatures.

The Governments will be accepting filing of Income Tax and other statutory returns through Internet if the identity of the persons can be properly established through digital signatures.

In case Digital Certificates are embedded with information such as "Age" and "Credit Information", Digital Certificates can be used as a means of establishing the "Credit Rating" of individuals.

## Digital Divide

Yet another concern in E-Governance is the need to avoid a "Digital Divide" being created in the community by virtue of the dependence of the Government on E-Governance. Due to either the difficulty of language or due to lack of financial standing, it is possible that the benefits of IT may not reach all sections of the society equally. As a result the gulf between the "Digital haves" and "Digital Have nots" may enlarge. If this aspect is lost sight off, it is likely to result in creating a section of "Disgruntled population" which can turn hostile and create a law and order problem in the society.

Thus the aspect of "E-Governance" throws up many challenges to the administrators and if a harmonious society has to be maintained, the sensitive issues mentioned above need to be addressed properly. The best way to

address such issues is for the Citizens to use the power of the Net in a positive manner by creating :"Similar Interest Virtual Groups" for exchange of ideas and networking of resources. It is such bodies of Netizens which will ultimately guide the legislators to form "Credible Laws" and assist law enforcers to be fair in their dealing with common men. More informed persons in the public can come together to provide services such as the "Computer Emergency Response Teams" to tackle security problems on the Internet.

Many of the legal responsibilities that are forced on the Government arise due to the lack of "Cyber Law Awareness" in the community. If therefore, the public can enhance their awareness of Cyber laws many of the problems associated with protecting an

ignorant community can be solved more easily. For example, it is more difficult to tackle the problem of “Stray Cattles” on a high way rather than “Stray Persons” on the highway. It is the responsibility of all “Netizens” to increase their knowledge levels to such levels that they donot become “Net Cattles” instead of “Netizens” needing impractical legal provisions to protect what cannot be protected.

# Chapter No 9

# Cyber Law Compliance

In the business environment, it is necessary for the users to recognize that non compliance of Cyber Laws could result in

a) A Legal liability on the firm

b) Inability of the firm to pursue legal remedies in the event of its assets being lost due to an illegal activity of an outsider.

Cyber Law Compliance is therefore suggested as a " Prudent Business Principle" . This should be considered mandatory in the sense that "Non Compliance" may tantamount to "Negligence" or "Lack of Due Diligence" as required by law.

ITA-2000 has specified that when Cyber Crimes occur in Corporate Networks, the

officials in charge of business including the CEO could be held responsible unless such a person besides being ignorant of the crime is able to establish that he had excercised "Due Diligence". Similar expectation is placed on "Intermediaries" such as ISPs or Cyber Cafes.

Even the general law expects persons who by being negligent to their responsibilities cause damage to the society should be punished. Thus negligent handling of explosives during transit could result in penalty for the owner for an accident though the accident was caused by the driver. The "Bhopal Gas Leak" Case in India is a classic example of "Vicarious responsibility" in an industrial environment where "negligence" in taking sufficient care of the assets by the owner could be considered

enough reason for the owner to be held liable for losses caused though indirectly.

It is therefore considered that any owner of an Information Asset is expected to exercise due care in the handling of the information asset failing which he would be liable to third parties for damages. Hence, if A virus spreads from the Computer of Mr A and causes damage to Mr B and if it is held that Mr A had not taken due care to protect his computer against virus, then he would be held responsible to compensate Mr B.

Cyber Law Compliance therefore represents the action that an Information Asset owner is expected to take so that he does not cause damage to the society by reason of him being the owner of the Information Asset.

# What is the Concept of CyLawCom?

CyLawCom is the set of pre-emptive actions that an Information Asset owner initiates either voluntarily or otherwise to cover against the risk arising out of non compliance of Cyber Laws.

The actual actions initiated vary depending on the type of the Information Asset and the nature of the Information Asset owner.

CyLawCom applies to an individual who uses a shared Computer either in the office or in a Cyber Café or a single computer owner or organizations which own several computers. It applies to a Cyber Café or a Web Portal or a Software Development Company or a BPO.

# CyLawCom Certification

Examination of the CyLawCom measures initiated by an Information Asset owner and grading the measures against certain accepted standards is the process of CyLawCom Certification.

Like any other certification process, the value of the Certification depends on the strengths of the Certifier and the individuals who actual do the assessment namely, the CyLawCom Examiners.

CyLawCom Certification is complimentary to other security certifications such as BS7799/ISO 27001 or Quality certifications such as Six Sigma or CMM.

Though the security certifications such as BS7799 do address some part of the Law Compliance, the weightage provided in the

assessment today is insufficient to adequately protect the asset owner. The ISO 27001 standard however goes a step further and provides that Legal Compliance and Evidence Management Systems need to be audited as a part of the certification process. Additionally, the requirements of SOX compliance, SAS 70 audit applicable to BPOs and India's SEBI guideline on Corporate Governance under Clause 49, RBI's regulations on monitoring of Cooperative Banks etc indicate that the Directors are liable to provide a certificate on "Internal Controls" which inter alia includes how the legal risks are being monitored. These developments have brought a focus on Legal Compliance in business environment. When the business environment becomes electronic environment, the legal compliance

becomes Cyber Law Compliance or CyLawCom.

CyLawCom certification focuses solely on the legal compliance aspect and hence stands apart from other certifications.

Though CyLawCom Certification is presently the pioneering concept promoted by Cyber Law College, it is expected that it will in due course find a place as an accepted Information Security practice. Its utility will be felt more when the system of Information Asset Insurance comes into use and the Insurer would expect the owner to take adequate legal measures so as to enable the insurer to step into the owner's shoes and recover the settled money through legal action against those who caused the loss to the owner of the insured asset.

## What are the essentials of an Audit?

An Audit is a standard process by which the expected behaviour of a person or an organization is systematically analysed and documented. The results may be presented in comparision with a bench mark if available.

A " Standard Audit" should therefore have

a) An Accepted Bench mark

b) Systematic Process of Observation

c) Systematic Process of Presentation

## Scope of CyLawCom Audit.

Cyber Law Audit is an audit of an environment against the known standards of compliance expected in the society. Since law compliance cannot be an exact science, there is bound to be some subjectivity in the

setting of standards and the evaluation of the environment.

As the Cyber Regulation regime becomes mature, there would be several judicial pronouncements that become standards through precedence and establish reliable bench marks. Until such time, bench marks will be "Moving Targets" and the "Certification Process" will necessarily be subject to periodical upgradation.

The scope of CyLawCom audit obviously varies from organization to organization. A rough indication of the expectations in an environment such as presently prevailing in India could be expressed as follows.

a) Total Compliance of Information Technology Act 2000

b) Compliance of the principles of the Uniform Dispute Resolution Policy in respect of the Domain Names.

c) Compliance of the Privacy Laws as per the European Union Guidelines which have become a de-facto standard

d) Compliance of the CanSpam Act which is the defacto standard for anti spam law

e) Compliance of the Indian Copyright Act and the Digital Millennium Copyright Act of USA which is the defacto standard for Copyright Compliance in the Cyber Space

f) Compliance of the Patent Regulations in India and USA

g) Compliance of the specific laws of countries with which the asset user has a business relationship

h) Compliance of other non cyber laws such as the Indian Penal Code which apply to the use of Electronic documents and are therefore relevant to the Information Asset user.

## Advantages of CyLawCom Audit

The CyLawCom Audit enables the management to discharge its primary responsibility of "Taking Steps to be Aware of the Possible Risks".

It also enables the organization to engage experts in the field to provide an insight into the unknown risks to which the organization and its stake holders are exposed.

It enables the management to take such steps as may be necessary to mitigate the risks so that either the risks are eliminated fully or provide a reasonable legal protection in the event of a loss occurring to the information assets of the Company.

# About the Author

**Na.Vijayashankar (Naavi),** MSc., CAIIB, CIIF, AIMADM
Techno Legal Information Security Consultant

Naavi is Techno Legal Information Security Consultant based in Bangalore. He is a pioneer in the field of Cyber Laws in India and the founder of www.naavi.org, a premier Cyber Law Portal in India. He is also the founder of www.cyberlawcollege.com, a dedicated virtual education center for Cyber Laws.

Naavi is the author of the first book on Cyber Laws in India titled "Cyber Laws for Every Netizen in India" released in December 1999. Since then he has released the first E-Book on the subject, "Cyber Laws, ITA 2000 and Beyond", as well as other print books

"Cyber Laws Demystified", "Cyber Law Compliance, Corporate Mantra for the Digital Era". He has also released a book in Kannada titled "Antarjaala AparadhagaLu".

Naavi has pioneered the concept of "Techno Legal Information Security" and also introduced for the first time in India the concept of a Three dimensional Information security approach adding the "Behavioral Science Approach" to Techno Legal aspects of Information Security" and presented a "Theory of IS Motivation". Naavi has also pioneered many innovative Cyber Law related services such as the Cyber Evidence Archival Center, Look-Alike domain name dispute resolution service etc.

Naavi can be contacted at naavi@vsnl.com.