MODULE -4

History of Cyber Laws in India

The resolution of the General Assembly of United Nations dated 30th January 1997 gave birth to the Information Technology Act which leads to the adoption of Modern Law on Electronic Commerce on International Trade Law.

The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 when the new IT Ministry was formed. However it underwent some alteration with the commerce industry due to some suggestions related to e-commerce and matters about the World Trade Organization (WTO) obligations. After the bill was introduced in the Parliament, the bill was referred to the 42-member Parliamentary Standing Committee following demands and suggestions from the Members. One of the suggestions that was highly debated upon was that a cyber café owner must maintain a register to record the names and addresses of all people visiting his café and also a list of the websites that they surfed. This suggestion was made as an attempt to curb cybercrime and to facilitate speedy locating of a cyber-criminal. However, at the same time it was ridiculed, as it would invade upon a net surfer's privacy and would not be economically viable. Finally, this suggestion was dropped by the IT Ministry in its final draft.[4]

Introduction to Cyber Laws

"Internet Law" is the well-defined area of law that suggests regulations to people about the use of the internet. Categorically cyber laws are divided into criminal laws and civil laws. Any law or regulation that involves how people use computers, smartphones, the internet and other related technology is cyber law.**[3]**

The virtual world of the internet is known as cyberspace and the laws governing this area are known as Cyber Laws and all the citizens of this space come under the ambit of these laws as it carries a kind of universal jurisdiction.

Cyberlaw is important because it touches almost all aspects of transactions and activities on and involving the internet, World Wide Web and cyberspace. Cyberlaw encompasses laws relating to –

- **Cybercrimes**
- **Electronic and digital signatures**
- **Intellectual property**
- **Data protection and privacy**

CYBERLAW

Cyber law (also referred to as cyberlaw) is a term used to **describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet**.

TYPICALLY REFERRED TO AS LAWS OF THE INTERNET.

Cybercrime is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone's security and financial health.

Phishing Scams

The majority of successful cyberattacks – 91% according to a study by PhishMe – begin when curiosity, fear, or a sense of urgency entices someone to enter personal data or click on a link.

Phishing emails mimic messages from someone you know or a business that you trust. They are designed to trick people into giving up personal information or clicking on a malicious link that downloads malware. Thousands of phishing attacks are launched every day.

What you can do: Stop trusting your emails. They are not always what they seem. Security awareness and Phishing training can empower your team to defend against phishing attacks by showing the telltale signs and teaching them how to recognize targeted phishing campaigns and malicious links and encouraging them to stay away from links and attachments and go directly to websites by typing the real URL into their browser.

CYBERSQUATTING

The term cybersquatting refers to **the unauthorized registration and use of Internet domain names that are identical or similar** to trademarks, service marks, company names, or personal names

Cybersquatters are free to register any available domain names, even if such domain names significantly resemble already registered domain names.

Cybersquatters usually use a combination of legal and illicit schemes for generating profits. Such schemes may include the following elements:

(1) registering domains which include common English words with the aim to resell them in the future;

(2) registering mostly mistyped spelling of the names of popular websites;

(3) purchasing recently expired domain names;

(4) publishing derogatory remarks about a company or a person on the cybersquatted website; and

(5) monetizing the content by publishing affiliated links and encouraging users to click on them. As a result of such practices, the owner of the legitimate website may experience serious financial and reputational consequences. At present, there are four dominant cybersquatting types

Types of cybersquatting

1. typosquatting
2. identity theft
3. name jacking
4. reverse-cybersquatting

Typosquatting

Typosquatting is often referred to as 'URL hijacking,' 'a sting site,' and a 'fake URL.'

Typosquatters rely on common mistakes made by Internet users when typing a web address into a web browser. Such mistakes include misspelling (e.g., www.intrenet.com), different phrasing of a domain name (e.g., www.internets.com), other top-level domain (www.internet.net), and use of Country Code Top-Level Domain (ccTLD) (e.g., www.internet.co).

More advanced typosquatting techniques exploit visual, hardware, and sound similarities of trademarks. For example, homograph attacks rely on the visual similarity of symbols that can be confused, as well as on letters or strings that might be confused with one another, such as confusion between 'vv' and 'w' in the domain name www.bankofthewest.com (www.bankofthevvest.com).

To trick Internet users, typosquatters may also create a fake website that resembles the source by using a similar layout, color schemes, logos, and content. Typosquatters use such fake websites to (1) compel legitimate website owners to buy the cybersquatted domain names, (2) generate more web traffic, and (3) spread malware.

Identity theft

- Cybersquatters may purchase a domain which was unintentionally not renewed by the previous owner. Cybersquatters use special software applications which allow them to monitor the expiration dates of targeted domain names easily. After registering the expired domain names, cybersquatters may link them with websites which duplicate the websites of the previous domain name owners. Thus, cybersquatters will mislead the visitors of their websites into believing that they are visiting the websites of the previous domain names owners.

Name Jacking

- Name jacking refers to the registration of a domain name associated with the name of an individual, usually celebrities and well-known public figures. Name jackers benefit from web traffic related to the targeted individuals.
- In the US, personal names can have trademark protection if they acquire distinctiveness through advertising or long use and establish a secondary meaning. Personal names that do not fulfill this condition cannot not be registered as trademarks because many people within the same territory may share the same name. Hence, name jackers may fall outside the scope of the US Anticybersquatting Consumer Protection Act.

REVERSE CYBER SQUATTING

- **Reverse Domain Name Hijacking**, also known as Reverse Domain Hijacking or Reverse Cybersquatting, involves attempting to use trademark protection mechanisms, such as ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) or the Anti-cybersquatting Consumer Protection Act (ACPA), in bad faith to acquire a domain name when the owner has legitimate rights to it.[1] Reverse domain name hijacking is usually attempted by large companies that can afford expensive legal fees.

What is cyberstalking?

Cyberstalking is a crime in which someone harasses or stalks a victim using electronic or digital means, such as social media, email, instant messaging (IM), or messages posted to a discussion group or forum. Cyberstalkers take advantage of the anonymity afforded by the internet to stalk or harass their victims, sometimes without being caught, punished or even detected.

The terms *cyberstalking* and *cyberbullying* are often used interchangeably. Cyberstalking, however, is actually a form of cyberbullying, which -- along with cybersquatting and cyberterrorism -- is among the growing number of computer- and internet-related crimes, collectively referred to as *cybercrime*.

Although *cyberstalking* is a general term for online harassment, it can take many forms, including slander, defamation, false accusations, trolling and even outright threats. In many cases, especially when both the harasser and victim are individuals, the motive may be the following:

- monitor the victim's online -- and, in some cases, offline -- activities;
- track the victim's locations and follow them online or offline;
- annoy the victim;
- intimidate, frighten, control or blackmail the victim;
- reveal private information about the victim, a practice known as *doxing*; or
- gather more information about the victim to steal their identity or perpetrate other real-world crimes, like theft or harassment.

Cyberstalkers often start small. In the beginning, they may send a few strange or somewhat unpleasant messages to their intended victim. Then, later, they may brush off these messages as funny, annoying or mildly weird and ignore them without taking any action.

Over time, the messages may become systematic, sustained and repetitive and take on an increasingly intimidating or frightening tone.

Direct and indirect cyberstalking

Cyberstalking can be direct or indirect.

Perpetrators may directly email their victims or flood their inboxes with emails. Or they may harass them through IM, voicemail, texting or other forms of electronic communications. They may use technologies to surveil or follow their victims or continuously view their pages -- often without their knowledge

Sometimes, cyberstalkers may send obscene, vulgar or offensive comments, social media follower or friend requests, or even outright threats. The stalkers may either attack the victims, which may distress them, or cause them to fear for their safety and well-being. They may also attack their victims' family or friends to expand their sphere of stalking influence.

A particular type of spyware called ***stalkerware*** can run on a victim's internet-enabled digital device and collect the user's actions on these devices, including emails, text messages, photographs and keystrokes.

In other indirect attacks, perpetrators may post false or malicious information about their victims online to damage their social standing or professional reputations -- a form of *cybersmearing* -- or set up a fake social media or forum account in their victims' names to impersonate them and post online material on their behalf.

In indirect cyberstalking attacks, perpetrators may damage the victim's device. They may do this by infecting it with ransomware to lock their files and then forcing them to pay a ransom for unlocking them. Or they may install a virus or keystroke logger that monitors the victim's digital behavior and/or steals data from the device.

Protection of CopyRight in Cyber Space

- In India, Copyright exists in source code of a computer program. Computer software is protected as literary work and so are computer databases as per Section 2(o) of Copyright Act, 1957. Thus, an original database is also protected by copyright.

In India 'copyright' means the exclusive right subject to the provisions of the law to do or authorise the doing of act in respect of work or any substantial part of work.

(a) In the case of literary, dramatic or musical work not being a computer programme to reproduce the work in any material form including the storing of it in any medium by electronic means, to issue copies, to perform the work in the public, to make any cinematograph film, or sound recording, to make any translation or to make any adaptation[14].

(b) In the case of computer programme to—

(i) do any of the acts specified in clause(a); and

(ii) sell or give on commercial rental or offer for sale or for commercial rental any copy of the computer programme.

- According to Section 14 of the Copyright Act, 1957
- an author of a work has the sole and exclusive right to enjoy and exploit several rights conferred by the Act for literary , dramatic, musical or artistic work, cinematographic film and sound recording.
- Rights mentioned under Section 14 include the right to reproduce the work, to issue its copies, perform or communicate work in public[4, make adaptations, translations, selling or rental rights in respect of different categories of work. Term of copyright in published literary , dramatic, musical and artistic works is lifetime of author and sixty years from beginning of calendar year next following year in which author dies. Same is the case of cinematographic film and sound recording .

Copy Right Infringement

- Where copyright is infringed, owner of copyright is entitled to sue for remedies including injunction, damages, profit of accounts and delivery up of infringing goods[7].
- Section 51 states copyright in a work is considered infringed when a person without a license from owner or registrar of copyrights or contravening conditions of a license does anything the exclusive right to do which is the right of the owner as per the Act or permits for profit a place to be used for communication of work to public where such communication constitutes infringement of copyright in the work unless he was not aware and had no reasonable ground to believe such communication will be infringement of copyright.

- It also amounts to an infringement where a person makes for sale or hire or displays or offers for sale , or distributes for trade or to prejudicially affect the owner of copyright or by way of trade exhibit in public or import into India infringing copies of work(excluding one copy for personal use of importer).
- As registration is not compulsory , suits for infringement can be filed even if plaintiff has secured no registration of the work Civil remedies available to owner of copyright are also available to exclusive licensee.Electronic contracts are considered legally valid in most jurisdictions such as India and electronic licensing or assignment is also legally valid.

- On second and subsequent conviction imprisonment is for a term not less than one year but which may extend to three years and fine which will not be less than one lac but may extend to 2 lacs. Punishment may be reduced if infringements are not made for commercial gain

Fair Dealing as a Defense

Section 52(a) provides for exceptions to infringement termed as " Fair dealing"

Fair dealing with literary , dramatic , musicasl or artistic work (not being a computer program) for purpose of private use, including research , criticism, review, and as per Section 52 (b) for purpose of reporting current events in a newspaper, magazine, or similar periodical, or by broadcasting or cinematographic film or by means of photographs

As per Section 62 of Copyright Act, a suit or civil proceeding will be filed for infringement of copyright in district court having jurisdiction to hear the case.

The jurisdiction under CPC will include place of residence where plaintiff resides or carries on business or personally works for gain. Section 63 of the Copyright Act provides the punishment for offence of copyright infringement.

Any person who knowingly infringes or abets the infringement of the copyright in a work or any other right conferred by the Act is punishable with imprisonment for a term which shall not be less than six months but which may extend to three years and fine which shall not be less than Rs. 50,000 but may extend to 2 lacs.

Linking,Hyperlinking and Framing

- A link takes a user from one website to another by clicking on a link or image. ...
- Framing is **the process of allowing a user to view the contents of one website while it is framed by information from another site**, similar to the "picture-in-picture" feature offered on some televisions.
- Framing is **a method of splitting one window into two or more screens**. A web page can be inserted into a frame, and that portion of the screen will remain static as a user moves through other web pages

Under the law, copyright in a work shall be deemed to be infringed—

(a) when any person, without a license granted by the owner of the copyright or the Registrar of Copyrights under this Act, or in contravention of the conditions of a license so granted or of any condition imposed by a competent authority under this Act—
  (i) does anything, the exclusive right to do which is by this Act conferred upon the owner of the copyright;
  (ii) permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement of copyright in the work, unless he was not aware and had no reasonable ground for believing that such communication to the public would be an infringement of copyright; or

(b) when any person—
  (i) makes for sale or hire, or sells or lets for hire, or by way of trade displays or offers for sale or hire; or
  (ii) distributes either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright; or
  (iii) by way of trade exhibits in public; or
  (iv) Imports into India[29]. …

- Is hyperlinking legal?

Hyperlinks **are lawful** - unless you use them unlawfully.

LIABILITY OF NETWORK SERVICE PROVIDERS IN CYBERSPACE

- The Indian ITAct,2000 stipulates that Network service providers are not liable in certain cases, for any third party information or data made available by an ISP, if it proves that the offence was committed without his knowledge, or that he had exercised all due diligence to prevent the commissioning of such offence

- A ‘network service provider’ means any person who provides access to information service in electronic form. For example: Internet service provider, cellular mobile services, customer access services, mobile satellite services etc. It essentially performs two tasks-to provide access to the network and to act as intermediary between an originator and addressee with respect to any particular electronic message.

- The position on ISP liability in India is the same as prevailing in other countries.
- However, with the enforcement of the IT Amendment Bill 2008, certain additional grounds will be added whereby an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him if the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or the intermediary does not initiate the transmission, select the receiver of the transmission, and select or modify the information contained in the transmission and the intermediary observes due diligence while discharging his duties under the Act .
- The amended Section 79 of the IT Act (yet to be enforced) provides that intermediaries will be held liable if the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act; or upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Protection of Patents in India

The term 'patent' refers to a grant of some privilege, property or authority made by the government or the sovereign of the country to one or more individuals. The instrument by which such a grant is made by the government is known as patent. A patent is a form of intellectual property rights in, among other things, a new and useful device, design or process. In India, under the law, a patent is a—

- right granted by the government;
- to exclude others;
- from engaging in activities such as making, using, importing, offering to sell or selling an invention.

In India, the law relating to patents came on the Statute Book as The Patents Act, 1970. Patent, under the Act, is granted by the Controller to the inventor for a period of twenty years. It is exclusive right to make use, exercise and vend his invention. The Patents (Amendment Act) 2005, defines: 'patent means a patent for any invention granted under this Act'[42]. The Patent's Act grants to the inventor substantive rights and secures to him the valuable monetary right which he can enforce for his own advantage either by using it himself or conveying the privileges to others. He receives something tangible, something which has present existing value, which protects him from some competition, and is the source of gain and profit.

Patent as a form of Intellectual Property

An invention is the creation of intellect applied to capital and labour, to produce something new and useful. Such creation becomes the exclusive property of the inventor on the grant of patent. The patentee's exclusive proprietary right over the invention is an intellectual property right. The owner's of the 'patent', that is the, patentee is entitled to deal with his such property in the same manner as owner of any movable property deals with his property. This means that the patentee can sell the whole or part of his property (patent). He can also grant license to other(s). Such sale and license of assignment of patented property naturally has to be for valuable consideration, acceptable mutually.

Under Section 66C of the IT (Amendment) Act, 2008 any person who fraudulently or dishonestly makes use of the electronic signature, password for 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 one lakh rupees.

Under this Section the offender requires *mens rea*, because the offence can be committed by fraudulently or dishonestly making use of electronic signature, password or unique identification feature. The offence in the section is cognizable because the offence can be committed by fraudulently or dishonestly making use of electronic signature, password or unique identification feature. The offence in the section is cognizable as well as bailable under section 77B of the IT Act.

Under Section 66D of the IT (Amendment) Act, 2008 any person who by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to a fine which may extend to one lakh rupees.