CYBER LAWS

Cyber Law also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.

According to Ministry of Electronic and Information Technology, Government of India,

Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce, check cyber crimes.

Importance of Cyber Law:

1. It covers all transaction over internet.
2. It keeps eyes on all activities over internet.
3. It touches every action and every reaction in cyberspace.

Area of Cyber Law:
Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

1. **Fraud:**
   Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

2. **Copyright:**
   The internet has made copyright violations easier. In early days of online communication, copyright violations were too easy. Both companies and individuals need lawyers to bring actions to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their own creative works.

3. **Defamation:**
   Several personnel use the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's personal reputation. When people use the internet to make statements that violate civil laws that is called Defamation law.

4. **Harassment and Stalking:**
   Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.

5. **Freedom of Speech:**
   Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allow people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

6. **Trade Secrets:**
   Companies doing businesses online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance and flight search services to name a few. Cyber laws help these companies to take legal action as necessary in order to protect their trade secrets.

7. **Contracts and Employment Law:**
   Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

Some Important Sections Of Indian Cyber Laws Are as follows

Section 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 in charge of a computer, computer system or computer network, or computer resource —

1. Accesses or secures access to such computer, computer system or computer network;
2. 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;
3. Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
4. Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network;
5. Disrupts or causes disruption of any computer, computer system or computer network;
6. Denies or causes the denial of access to any person authorized 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 there under;
7. Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation to the person so affected.
8. Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

9. Steel, 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;

She/he shall be liable to pay damages by way of compensation to the person so affected.

Explanation

For the purposes of this section:

1. "**computer contaminant**" means any set of computer instructions that are designed —
    a. To modify, destroy, record, transmit data or program residing within a computer, computer system or computer network;
    b. By any means to usurp the normal operation of the computer, computer system, or computer network;
2. "**Computer data base**" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized 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;
3. "**Computer virus**" means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;
4. "**Damage**" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.
5. "**Computer source code**" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Section 65

Tampering with Computer Source Documents.

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

Explanation

For the purposes of this section, "**Computer Source Code**" means the listing of programs, Computer Commands, Design and layout and program analysis of computer resource in any form.

Section 66A

Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,-

a. Any information that is grossly offensive or has menacing character.

b. Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a 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.

She/he shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation

For the purposes of this section, terms "**Electronic mail**" and "**Electronic Mail Message**" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

Section 66B

Punishment for dishonestly receiving stolen computer resource or communication device

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.

Section 66C

Punishment for identity theft

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.

Section 66D

Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, 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.

Section 66E

Punishment for violation of privacy

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

Explanation

For the purposes of this section–

a. "**Transmit**" means to electronically send a visual image with the intent that it be viewed by a person or persons;

b. "**Capture**", with respect to an image, means to videotape, photograph, film or record by any means;

c. "**Private area**" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

d. "**Publishes**" means reproduction in the printed or electronic form and making it available for public;

e. "**Under circumstances violating privacy**" means circumstances in which a person can have a reasonable expectation that–

   i. He or she could disrobe in privacy, without being concerned that an image of his private area was being captured.

   ii. Any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Section 66F

Punishment for cyber terrorism

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 –

   a. Denying or cause the denial of access to any person authorized to access computer resource.

   b. Attempting to penetrate or access a computer resource without authorization or exceeding authorized access.

   c. 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.

B. Knowingly or intentionally penetrates or accesses a computer resource without authorization 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.

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

Section 67

Punishment for publishing or transmitting obscene material in electronic form.

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

Section 67A

Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form.

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to 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.

Exception:

This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

i. The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting,

representation or figure is in the interest of science, literature, art or learning or other objects of general concern.

ii. Which is kept or used bonafide for religious purposes.

Section 67B

Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

Whoever,

a. Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct.

b. 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.

c. 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.

d. Facilitates abusing children online.

e. Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children.

Shall be punished on first conviction with imprisonment of either description 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:

Exception:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form

i. The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern.

ii. Which is kept or used for bonafide heritage or religious purposes.

Explanation:

For the purposes of this section, "**Children**" means a person who has not completed the age of 18 years.

Section 72

Breach of confidentiality and privacy.

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