UNIT 4

The legal framework that controls cyberspace, the internet, and the usage of technology is referred to as "cyber law," sometimes known as "internet law" or "information technology law." It covers a broad variety of legal concerns and rules pertaining to digital communication, online activities, computer systems, data security, intellectual property, and more. As our dependence on technology and the role of the internet in our daily lives has grown, the field of cyber law has evolved. It tackles the problems and issues that occur legally as a result of using computers, networks, and digital data.

Several significant issues are addressed by cyberlaw: The scope of cyber laws is vast and encompasses various aspects of technology, the internet, and electronic communication. Here are some key areas within the scope of cyber laws:

Privacy and data protection: Cyber law addresses the safeguarding of personal data and the rights of persons to privacy. It establishes rules for the gathering, holding, using, and disclosing of data as well as the security precautions that businesses must take to protect sensitive data.

Intellectual property: Cyber law deals with securing individuals' legal access to their digital works. It includes the unauthorized use or distribution of digital content as well as copyright infringement, trademark infringement, and concerns with patents.

Cybercrime: identity theft, phishing, online fraud, and other types of cybercrime are all addressed by laws in cyber law. It creates legal frameworks for the prosecution of people or organisations engaged in illicit computer network activity.

Online transactions, electronic contracts, digital signatures, and consumer protection are all governed by cyber law in the context of e-commerce. It outlines guidelines for conducting business online, accepting payments electronically, and resolving disputes.

Cybersecurity: Cyber law deals with the legal facets of cybersecurity, such as safeguarding computer networks and systems against unauthorized access, online assaults, and data breaches. It outlines organizations' responsibilities for putting security measures and protections in place to stop and address online threats.

Cyber law deals with internet governance and regulation, as well as the obligations of internet service providers (ISPs), content producers, and other entities active in cyberspace. It covers topics including freedom of speech, internet censorship, domain name conflicts, and net neutrality.

Cyber law has continual difficulties in keeping up with new advances and resolving developing legal concerns as technology continues to grow. It is essential for upholding legal rights, obligations, and safeguards in the digital era and fostering a safe and dependable online environment for people, companies, and governments.

Data protection and privacy: Cyber laws address the protection of personal data and privacy rights in the digital realm. They regulate the collection, storage, use, and disclosure of personal information by individuals, organizations, and government entities.

Internet governance and regulation: Cyber laws encompass regulations and policies governing the internet, internet service providers (ISPs), domain name registration, online content, online censorship, net neutrality, and freedom of expression in cyberspace.

Digital signatures and authentication: Cyber laws define the legal framework for the use of digital signatures and authentication methods to ensure the integrity and authenticity of electronic transactions and communications.

Cyber jurisdiction and international cooperation: Cyber laws deal with issues of jurisdiction in cyberspace and facilitate international cooperation in investigating and prosecuting cybercrimes that cross national boundaries.

Privacy and Freedom Issues in The Cyber World

The cyber world presents various privacy and freedom issues that arise from the increasing reliance on digital technologies and the internet. Here are some key concerns:

Data Privacy: With the proliferation of online services and social media platforms, personal data has become a valuable commodity. There are concerns about how personal information is collected, stored, and used by companies, governments, and other entities. Data breaches and unauthorized access to personal information can lead to identity theft, financial loss, or misuse of sensitive data.

Surveillance and Monitoring: Governments, intelligence agencies, and even private companies engage in surveillance and monitoring activities in the cyber world. Mass surveillance programs, such as bulk data collection and monitoring of online activities, raise concerns about privacy invasion and the potential for abuse of power. It can have a chilling effect on free expression and limit individuals' ability to explore ideas or dissent.

Censorship and Internet Freedom: Many countries engage in censorship and content filtering, limiting access to information and suppressing dissenting opinions. Governments may block websites, social media platforms, or specific content deemed politically or morally sensitive. This restricts freedom of speech and access to information, impeding democratic principles and stifling creativity and innovation.

Cybercrime and Security: The interconnected nature of the cyber world makes it vulnerable to various forms of cybercrime. Malware, hacking, phishing, and online fraud can compromise personal information, financial resources, and critical infrastructure. Balancing security measures with individual privacy rights is a challenge, as robust security measures may encroach upon personal freedoms.

Digital Divide: The disparity in access to digital technologies and internet connectivity creates a digital divide, limiting opportunities for those without access. This divide can exacerbate existing social and economic inequalities, hindering individuals' ability to participate fully in the digital society and benefit from the opportunities it presents.

Ethical Implications of Emerging Technologies: Advancements in technologies like artificial intelligence (AI), biometrics, and facial recognition raise ethical concerns. The potential for misuse of these technologies, such as profiling, discrimination, or infringement on personal freedoms, highlights the need for responsible development and deployment.

Addressing these issues requires a multi-faceted approach involving legal frameworks, technological advancements, education and awareness, and the active involvement of governments, organizations, and individuals. Striking a balance between privacy, security, and freedom in the cyber world is an ongoing challenge as technology evolves and new issues emerge.

Intellectual property (IP) is a term referring to creation of the intellect (the term used in studies of the human mind) for which a monopoly (from greek word monos means single polein to sell) is assigned to designated owners by law. Some common types of intellectual property rights (IPR), in some foreign countries intellectual property rights is referred to as industrial property, copyright,

patent and trademarks, trade secrets all these cover music, literature and other artistic works, discoveries and inventions and words, phrases, symbols and designs. Intellectual Property Rights are themselves a form of property called intangible property. Although many of the legal principles governing IP and IPR have evolved over centuries, it was not until the 19th century that the term intellectual property began to be used and not until the late 20th century that it became commonplace in the majority of the world. Types of Intellectual Property The term intellectual property is usually thought of as comprising four separate legal fields: 1. Trademarks 2. Copyrights 3. Patents 4. Trade secrets

Trademarks and Service Marks: A trademark or service mark is a word, name, symbol, or device used to indicate the source, quality and ownership of a product or service. A trademark is used in the marketing is recognizable sign, design or expression which identifies products or service of a particular source from those of others. The trademark owner can be an individual, business organization, or any legal entity. A trademark may be located on a package, a label, a voucher or on the product itself. For the sake of corporate identity trademarks are also being.

Copyrights: Copyright is a form of protection provided by U.S. law to the authors of "original works of authorship" fixed in any tangible medium of expression. The manner and medium of fixation are virtually unlimited. Creative expression may be captured in words, numbers, notes, sounds, pictures, or any other graphic or symbolic media. The subject matter of copyright is extremely broad, including literary, dramatic, musical, artistic, audiovisual, and architectural works. Copyright protection is available to both published and unpublished works. Copyright protection is available for more than merely serious works of fiction or art. Marketing materials, advertising copy and cartoons are also protectable. Copyright is available for original working protectable by copyright, such as titles, names, short phrases, or lists of ingredients. Similarly,

ideas methods and processes are not protectable by copyright, although the expression of those ideas is. Copyright protection exists automatically from the time a work is created in fixed form. The owner of a copyright has the right to reproduce the work, prepare derivative works based on the original work (such as a sequel to the original), distribute copies of the work, and to perform and display the work. Violations of such rights are protectable by infringement actions. Nevertheless, some uses of copyrighted works are considered “fair use” and do not constitute infringement, such as use of an insignificant portion of a work for noncommercial purposes or parody of a copyrighted work.

Patents: A patent for an invention is the grant of a property right to the inventor, issued by the United States Patent and Trademark Office. Generally, the term of a new patent is 20 years from the date on which the application for the patent was filed in the United States or, in special cases, from the date an earlier related application was filed, subject to the payment of maintenance fees. U.S. patent grants are effective only within the United States, U.S. territories, and U.S. possessions. Under certain circumstances, patent term extensions or adjustments may be available. The right conferred by the patent grant is, in the language of the statute and of the grant itself, “the right to exclude others from making, using, offering for sale, or selling” the invention in the United States or “importing” the invention into the United States. What is granted is not the right to make, use, offer for sale, sell or import, but the right to exclude others from making, using, offering for sale, selling or importing the invention. Once a patent is issued, the patentee must enforce the patent without aid of the USPTO.

Trade Secrets: A trade secret consists of any valuable business information. The business secrets are not to be known by the competitor. There is no limit to the type of information that can be protected as trade secrets; For Example: Recipes, Marketing plans, financial projections, and methods of conducting business can all constitute trade secrets. There is no requirement that a trade secret be unique or complex; thus, even something as simple and nontechnical as a list of customers can qualify as a trade secret as long as it affords its owner a competitive advantage and is not common knowledge. If trade secrets were not protectable, companies would no incentive to invest time, money and effort in research and development that ultimately benefits the public. Trade secret law thus promotes the development of new methods and processes for doing business in the marketplace.

Information Technology Act, 2000

Information Technology Act, 2000

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the model law on electronic commerce

(E-commerce) to bring uniformity in the law in different countries.

Further, the General Assembly of the United Nations recommended that all countries must consider this model law before making changes to their own laws. India became the 12th country to enable cyber law after it passed the Information Technology Act, 2000.

The Information Technology Act, 2000 provides legal recognition to the transaction done via electronic exchange of data and other electronic means of communication or electronic commerce transactions.

This also involves the use of alternatives to a paper-based method of communication and information storage to facilitate the electronic filing of documents with the Government agencies.

Objectives of the Act

The objectives of the Act are as follows:

1. Grant legal recognition to all transactions done via electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication.
2. Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication
3. Facilitate the electronic filing of documents with Government agencies and also departments
4. Facilitate the electronic storage of data
5. Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions
6. Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

Non-Applicability

According to Section 1 (4) of the Information Technology Act, 2000, the Act is not applicable to the following documents:

1. Execution of Negotiable Instrument under Negotiable Instruments Act, 1881, except cheques.
2. Execution of a Power of Attorney under the Powers of Attorney Act, 1882.
3. Creation of Trust under the Indian Trust Act, 1882.
4. Execution of a Will under the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
5. Entering into a contract for the sale of conveyance of immovable property or any interest in such property.
6. Any such class of documents or transactions as may be notified by the Central Government in the Gazette.

Scope or Extent of the ACT

It extends to the whole of India

It also applies to any offence or contravention committed outside India by any person irrespective of his nationality, provided such offence or contravention involves a computer, computer system or network located in India.

Key Definitions (to be covered)

Sec. 2(1) (a)

Sec. 2(1) (b)

Sec. 2(1) (c)

Sec. 2(1) (d)

Sec. 2(1) (da)

Sec. 2(1) (g)

Sec. 2(1) (i)

Sec. 2(1) (j)

Sec. 2(1) (k)

Sec. 2(1) (l)

Sec. 2(1) (o)

Sec. 2(1) (p)

Sec. 2(1) (v)

Sec. 2(1) (w)

Sec. 2(1) (x)

Sec. 2(1) (zc)

Sec. 2(1) (zd)

Sec. 2(1) (ze)

Sec. 2(1) (h)

Sec. 2(1) (n)

Sec. 2(1) (r)

Sec. 2(1) (t)

Sec. 2(1) (za)

Sec. 2(1) (zg)

Sec. 2(1) (zh)

Digital Signature

According to Section 2(1) (p), digital signature means ‘authentication of any electronic record using an electronic method or procedure in accordance with the provisions of Section 3‘.

Further, digital signatures authenticate the source of messages like an electronic mail or a contract in electronic form.

The three important features of digital features are:

1. Authentication – They authenticate the source of messages. Since the ownership of a digital certificate is bound to a specific user, the signature shows that the user sent it.
2. Integrity – Sometimes, the sender and receiver of a message need an assurance that the message was not altered during transmission. A digital certificate provides this feature.
3. Non-Repudiation – A sender cannot deny sending a message which has a digital signature.

Authentication of Electronic record

Section 3

Section 3 of the Information technology Act, 2000 provides certain provisions for the authentication of electronic records. The provisions are:

- Subject to the provisions of this section, any subscriber can affix his digital signature and hence authenticate an electronic record.

- An asymmetric crypto system and hash function envelop and transform the initial electronic record into another record which affects the authentication of the record.
- Also, any person in possession of the public key can verify the electronic record.
- Further, every subscriber has a private key and a public key which are unique to him and constitute a functioning key pair.

Read the Process and creation of Digital Signature (Rule 4 and Rule 5)

Electronic Signature (Section 3A)

Electronic Signature has been defined under Section 2(1)(ta) of the Information Technology Act, 2000. Electronic Signature means the authentication of any electronic record by a subscriber by means of the electronic technique as specified under the Second Schedule and also includes a digital signature.

Read the Difference between Digital Signature and Electronic Signature – Chapter 26 (Sushma Arora) or Chapter 25 (Dr. Rajni Jagota)

Electronic Governance (Section 4 -10)

- **Meaning of E- Governance**
- **Provisions-**

1. Legal recognition of electronic records – Section 4
2. Legal recognition of digital signatures – Section 5
3. Use of electronic records and digital signatures in the Government and also its agencies – Section 6
4. Delivery of services by service provider - Section 6 A
5. Retention of electronic records – Section 7
6. Audit of documents, records or information maintained in electronic form - Section 7A
7. Publication in Electronic Gazette – Section 8
8. Section 6,7 and 8 Not to confer right to insist on the acceptance of documents in the electronic form – Section 9
9. Central Government's power to make rules pertaining to digital signatures – Section 10
10. Validity of contracts formed through Electronic means – Section 10A

Attribution, Acknowledgement and dispatch of Electronic Records (Sec. 11-16)

Sec. 11 Attribution of electronic records.-An electronic record shall be attributed to the originator,-

(a) if it was sent by the originator himself;
(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
(c) by an information system programmed by or on behalf of the originator to operate automatically.

Sec. 12 Acknowledgement of receipt. –

(1) Where the originator has not agreed that the acknowledgement of receipt of electronic record be given in a particular form or by a particular method, an acknowledgement may be given by-
(a) any communication by the addressee, automated or otherwise; or
(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgement of such electronic record by him, then, unless acknowledgement has been so received, the electronic record shall be deemed to have been never sent by the originator.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then, the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgement

must be received by him and if no acknowledgement is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

Sec. 13. **Time and place of despatch and receipt of electronic record.-**

(1)Time of Dispatch- Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(2) Time of Receipt- Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:-

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,-
(i) Receipt occurs at the time when the electronic record enters the designated computer resource; or
(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;
(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Place of Dispatch- Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) Place of Receipt- The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

(5) Place of Business- For the purposes of this section,-

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;
(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
(c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

Sec. 14. **Secure electronic record**.-Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Sec. 15 Secure electronic signature. -An electronic signature shall be deemed to be a secure electronic signature if-
(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation. -In case of digital signature, the "signature creation data" means the private key of the subscriber.]

Sec. 16 Security procedures and practices. -The Central Government may, for the purposes of sections 14 and 15, prescribe the security procedures and practices: Provided that in prescribing such security procedures and practices, the Central Government shall have regard

to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.] "16. Security procedure. -The Central Government shall, for the purposes of this Act, prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including-
(a) the nature of the transaction;
(b) the level of sophistication of the parties with reference to their technological capacity;
(c) the volume of similar transactions engaged in by other parties;
(d) the availability of alternatives offered to but rejected by any party;
(e) the cost of alternative procedures; and
(f) the procedures in general use for similar types of transactions or communications."