what is cyber laws

Date / /
Page No.

UNIT-4 CYBER LAWS

Introduction to cyber laws

Cyber laws also known as internet law or digital law refers to the legal issues surrounding the use of internet and other digital technologies. Cyber laws designed to regulate and protect the use of digital technologies, as well as to prevent and prosecute cybercrimes.

If anyone breaks a cyber laws, the action would be taken against the person on the basis of the type of cyber law he broke, where he lives, and where he broke the law.)

Scope of cyber law

1) Protecting personal data and privacy online
2) dealing with cybercrime, including hacking and identity threat
3) safeguarding itellectual property rights
4) regulating ecommerce and online contracts
5) ensuring cybersecurity and preventing cybercrimes
6) governing internet governance and regulations
7) protecting digital rights and freedom of speech online

Privacy and Freedom Issues In The Cyber World

Privacy and freedom issues in the cyber world refer to concerns about the protection of personal information and the ability to freely express oneself and access information online.

Privacy: Privacy in the cyber world means keeping personal information secure and controlling how it is used. It includes things like your name, address, financial details, and online activities. Privacy issues arise when personal information is collected, shared, or used without your permission, leading to potential risks such as identity theft or unwanted surveillance.

Freedom: Freedom in the cyber world refers to the ability to express your thoughts, access information, and use digital technologies without unnecessary restrictions or limitations. It means having the right to share your opinions, access websites and services, and engage in online activities without fear of censorship or discrimination.

Privacy Issues: Privacy issues can arise when companies or organizations collect and use your personal information without your knowledge or consent. It can also occur when your data is leaked or hacked, exposing your sensitive information to unauthorized individuals. Privacy issues may include unwanted tracking of your online behavior, targeted advertising, or the misuse of personal data by third parties.

Freedom Issues: Freedom issues can occur when there are restrictions on accessing certain websites or content, censorship of online speech, or surveillance that intrudes on people's private activities. Government control or surveillance of the internet can limit people's ability to freely express themselves or access information, stifling creativity, and hindering open communication.

Privacy issues

1) concern about personal information shared online, like contact details and financial data.
2) companies collecting user data and questions about how it is used
3) Unauthorized access or security breaches leading to exposure of personal information
4) Government surveillance and balancing security with civil liberties
5) Users wanting more control over their personal data and consent.

Freedom issues

1) Balancing intellectual property rights with the freedom to share and access information
2) content filtering or blocking
3) limited access to websites or information.
4) Cyberbullying and online harrasment, impacting to participate online.

IT Act 2000

The Information Technology Act, 2000 is the law pertaining to information technology. IT Act, 2000 was the result of passing of the IT the Bill by both the houses of Parliament. The Act is grounded on the United Nations Commission on International Trade Law (UNCITRAL). It deals with Ecommerce and cybercrimes. It is, "An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce". The Act came into force on 17.10. 2000. 17/10/2000

Features of The Information Technology Act, 2000

1. Digital signature has been replaced with electronic signature to make it a more technology neutral act.
2. It elaborates on offenses, penalties, and breaches.
3. It outlines the Justice Dispensation Systems for cyber-crimes.
4. Recognition of Digital Transactions: The Act makes electronic transactions and communications legally valid and enforceable.
5. Addressing Cybercrimes: The Act deals with various cybercrimes like unauthorized access, hacking, data theft, and sharing offensive content online. It defines these crimes and specifies the punishments for those involved.
6. Protection of Data and Privacy: The Act includes rules to protect personal information and requires organizations to implement security measures to keep individuals' data safe.
7. Electronic Governance: The Act allows government agencies to use electronic methods for communication, record-keeping, and providing services. It recognizes electronic records and documents as legally valid.

Objectives of the IT Act:

1. Recognize and make electronic transactions ~~valid and legally enforceable~~ legally valid.
2. Prevent and punish cybercrimes like hacking, unauthorized access, and data theft.
3. Protect the privacy and personal information of individuals.
4. Enable government departments to use electronic methods for communication, record-keeping, and service delivery.
5. Establish a legal framework for the use of digital signatures and certifications to ensure reliable and authentic electronic transactions.
6. Provide a specialized tribunal to handle appeals related to cyber offenses.
7. Build trust and confidence in online business transactions and promote the growth of e-commerce.

Scope of the IT Act:

1. Electronic Transactions: The Act covers all types of electronic transactions, including online shopping, contracts made online, and using digital signatures for authentication.
2. Cybercrimes: The Act deals with various cybercrimes like unauthorized access to computers, hacking, stealing personal information, spreading computer viruses, and sharing offensive or explicit content online.
3. Data Protection and Privacy: The Act includes rules for protecting personal data or information. It applies to organizations that handle sensitive personal information and provides guidelines to ensure that data is kept safe and private.

Penality	Imprisionment	Fine
Unauthorized Access	upto 3 years	upto ₹ 5,00,000
Hacking	upto 3 years	upto ₹ 5,00,000
Identity theft	upto 3 years	upto ₹ 1,00,000
impersonation	upto 3 years	upto ₹ 1,00,000
publishing or transmitting obscene content	upto 5 years	upto ₹ 10,00,000
Cyber fraud and financial crime	upto 3 years	upto ₹ 5,00,000
publishing false information	upto 2 years	upto ₹ 1,00,000
tampering with computer source documents	upto 3 years	upto ₹ 2,00,000
Cyber Terrorism	Life imprisonment or death	N/A
Forgery of digital signatures	upto 3 years	variable
data theft & breach	upto 3 years	variable
sending offensive message	upto 3 years	variable
cyberstalking	upto 3 years	variable
violation of copyright	variable	variable
Breach of confidentiality and privacy	upto 3 years	variable

OFFENSES

1. **Section 43:** This section deals with penalties for unauthorized access, damage, or disruption of computer systems or networks. It covers offenses such as unauthorized access to computer resources, downloading, copying, or extracting data without permission, introducing viruses, and causing damage to computer systems. It specifies the penalties for these offenses, which may include imprisonment and/or fines. ~~Penalty~~ upto 10 million

2. **Section 65:** This section pertains to tampering with computer source documents. It makes it an offense to knowingly or intentionally tamper with or manipulate computer source code, computer program, or computer system, which is intended to be used for a computer, computer program, or computer network. It carries penalties of imprisonment and/or fines. Imprisonment upto 3 years and 200000 fine or both

3. **Section 66A:** This section, deals with offensive material on internet which cause harm to any person's identity or value. Imprisonment upto 3 years + fine upyo 100000

4. **Section 67A:** This section addresses the offense of publishing or transmitting sexually explicit content in electronic form. may carry penalties of imprisonment upto 7 years and/or finesupto 1000000.

5. **Section 72:** This section pertains to the offense of breach of confidentiality and privacy. It makes it an offense for any person who has access to any material containing personal information, obtained while providing services under a lawful contract, to disclose such information without the consent of the person concerned. It carries penalties of imprisonmentypyo 2 years and/or finesupto 1 million.

E-governance

E-governance uses technology to improve government services and interacts with citizens

It allows citizens to access government services online reducing the need for physical visits

It makes government processes more efficient and transparent

It promotes citizen engagement and participations in decision-making.

Helps to reduce costs and resource allocation

It provides mobile applications and web services to reach to wider population

Goal is to create citizen centric government

Collaboration b/w government & private sector is important for e-governance

requires legal framework to protect data and privacy.

- **Legal Recognition of Electronic Records (Mentioned in Section 4 of the Act)**

  For any important point to become a law, it is needed to be written, printed, or typewritten. It can also be considered to be a law if the information is provided in an electronic form. However, the electronic form must be accessible all the time for subsequent referencing.

It means that electronic documents and records have the same value and validity as physical paper documents in legal matters

1. Equal Validity: Electronic records, like emails, digital contracts, or scanned copies, are considered just as legally valid as physical paper documents.

2. Accepted Evidence: Electronic records can be used as evidence in legal proceedings to prove facts or transactions. They are treated like any other form of evidence.

3. Digital Signatures: The Act recognizes digital signatures, which are electronic signatures that use special techniques to ensure their authenticity. They are legally recognized as equivalent to handwritten signatures on paper.

- **Legal Recognition of Signatures (Mentioned in Section 5 of the Act)**

  Most of the documents related to a person are authenticated by his or her signature. If the person can produce a digital form of his signature acceptable by the central government, then the person is legally allowed to validate the documents with the digital signature. This is the summary of the legal recognition of digital signature provision.

It means that electronic signatures have the same legal standing as handwritten signatures on paper documents.

1. Equivalent to Handwritten Signatures: Digital signatures are considered just as valid and legally binding as handwritten signatures. They serve the same purpose of verifying the authenticity and integrity of a document or agreement.

2. Authentication and Integrity: Digital signatures use advanced cryptographic techniques to securely associate an electronic signature with the person or entity signing the document. This ensures that the signature cannot be tampered with and provides assurance of the signer's identity.

3. Legal Acceptance: Digital signatures are legally accepted in various jurisdictions and can be used in legal contracts, agreements, and other official documents. They carry the same weight and validity as traditional handwritten signatures.

- **Application of Digital Signature and Electronic Records in Government and its Agencies (Mentioned in Section 6 of the Act)**

  According to this provision, if the law allows a person

  - To fill an application, form, or document related to Government authorities or related agencies,
  - To issue or grant sanction, licence, approval, or permit in a particular way,
  - To Pay or receive money in a certain manner then the person can certainly do so in an electronic form if he maintains the government-approved format.

Additionally, the manner and format of creating, issuing, and filing electronic records, and the methods of payment of fees for the same may be prescribed.