**UNIT - 3**

| **S.no.** | **Section Name** | **Summary** |
| --- | --- | --- |
| 1 | Introduction to Cyber Law | Defines cyber law, its scope, and its relation to IT, including the importance of internet regulation. |
| 2 | Importance of Cyber Law | Describes the necessity of cyber law in monitoring online activities and transactions. |
| 3 | Areas of Cyber Law | Covers fraud, copyright, defamation, harassment, stalking, trade secrets, and contracts. |
| 4 | Advantages of Cyber Law | Lists benefits like enabling e-commerce, digital signatures, e-governance and enhanced security. |
| 5 | Objectives of Cyber Law | Includes data protection, prevention of cybercrime, cybersecurity, intellectual property protection, and more. |
| 6 | The Need for Cyber Law | Explains the shift from paper to digital, and the need for legal infrastructure in cyberspace. |
| 7 | Scope of Cyber Law | Highlights e-commerce, electronic records, digital signatures, and cybercrime regulations. |
| 8 | Categories of Cybercrime | Divided into crimes against persons, property, government, and others like spamming and phishing. |
| 9 | Intellectual Property in Cyberspace | Explains copyright, trademark, and patent laws as applied to digital content and domain names. |
| 10 | Data Protection and Privacy Laws | Discusses balancing individual privacy rights and organizational data handling responsibilities. |
| 11 | Copyright Issues in Cyberspace | Covers enforcement challenges and technologies like DRM to protect digital content. |
| 12 | Data Encryption | Explains encryption techniques, importance, types (symmetric, asymmetric), and states of encryption. |
| 13 | Cryptography | Describes cryptographic techniques, features like confidentiality and integrity, and key types. |
| 14 | Applications of Cryptography | Includes secure web browsing, digital currencies, electronic signatures, and end-to-end encryption. |
| 15 | Digital Signatures | Defines digital signatures, how they work, their benefits, and their legal significance. |
| 16 | Encrypted Smart Cards | Explains smart cards as secure devices for storing sensitive data using encryption. |
| 17 | Biometrics | Discusses the use of unique physical and behavioral traits for identification and authentication. |
| 18 | Firewalls | Describes firewalls as barriers between trusted and untrusted networks, and their functions. |
| 19 | Information Security Management System (ISMS) | Outlines policies, processes, technology, and standards for managing information security. |
| 20 | Security Assurance | Covers ensuring effective security measures through risk management, training, and monitoring. |
| 21 | Security Laws in India | Includes the IT Act, National Cyber Security Policy, and sector-specific regulations. |
| 22 | International Standards | Lists ISO/IEC 27001, GDPR, NIST Cybersecurity Framework, and other global standards. |
| 23 | Security Audits | Explains compliance audits, risk assessments, penetration testing, and their types. |
| 24 | System Security Engineering Capability Maturity Model (SSE-CMM) | Describes processes and maturity levels for secure system development. |
| 25 | COBIT Framework | Explains COBIT as a framework for IT governance and management to align IT goals with business objectives. |

**Introduction to Cyber Law**

* Cyber Law, or IT Law, governs legal aspects of IT and the internet, addressing issues like information security, software, and e-commerce.
* Encompasses multiple laws such as contract, intellectual property, and privacy laws.
* Intellectual property is a core focus, especially software licensing, which is evolving globally.

**Importance of Cyber Law**

1. Regulates online transactions and monitors internet activities.
2. Ensures legal oversight for all cyberspace interactions.
3. Protects users from cybercrimes and supports a secure digital environment.

**Major Areas of Cyber Law**

1. **Fraud**: Protects against online fraud, identity theft, and financial crimes.
2. **Copyright**: Enforces intellectual property rights for digital content.
3. **Defamation**: Guards against false, harmful statements online.
4. **Harassment and Stalking**: Addresses threatening online behavior.
5. **Freedom of Speech**: Balances free expression with legal boundaries.
6. **Trade Secrets**: Secures proprietary business information.
7. **Contracts and Employment**: Regulates digital agreements and conditions.

**Objectives of Cyber Law**

1. Safeguards personal and sensitive data.
2. Prevents cybercrimes and penalizes offenders.
3. Regulates e-commerce and digital contracts.
4. Promotes cybersecurity through secure systems and encryption.
5. Balances internet freedom with lawful constraints.

**Need for Cyber Law**

1. Addresses evolving cybercrimes and digital misconduct.
2. Enables a paperless digital economy.
3. Establishes legal frameworks for cyberspace governance.
4. Facilitates e-governance and supports global participation in cyberspace.

**Scope of Cyber Law**

1. Regulates e-commerce, electronic records, and digital signatures.
2. Defines and penalizes cybercrimes like phishing, hacking, and cyber terrorism.
3. Encompasses intellectual property protections for software and trademarks.
4. Provides data protection laws to safeguard privacy.

**Data Encryption**

* Converts plaintext into unreadable ciphertext for secure data transmission and storage.
* Types: **Symmetric** (one key) and **Asymmetric** (public/private keys).
* Applications include secure communication, digital rights management, and cloud storage.

**Cryptography**

1. Secures communication using encryption algorithms.
2. Types: Symmetric, Asymmetric, and Hash Functions.
3. Ensures confidentiality, integrity, authentication, and non-repudiation.
4. Applications: Digital currencies, secure web browsing, and electronic signatures.

**Digital Signatures**

* Used for document authentication and tamper prevention.
* Based on public key cryptography.
* Benefits include legal recognition, cost and time savings, and enhanced security.

**Biometric Technology**

* Identifies individuals using unique physical traits like fingerprints and facial recognition.
* Applications: Mobile security, identity verification, and secure financial transactions.

**Firewall**

* Protects networks by monitoring incoming and outgoing traffic.
* Types: Packet filtering, stateful inspection, and application-layer firewalls.
* Ensures secure data transfer and prevents unauthorized access.

**Information Security Management Systems (ISMS)**

1. A framework for managing sensitive company information.
2. Includes risk management, access control, and security training.
3. Compliance standards: ISO 27001, GDPR, HIPAA, PCI DSS.
4. Encourages regular audits for continuous improvement.

**Cybersecurity Laws in India**

1. **IT Act, 2000**: Governs digital signatures, cybercrimes, and data protection.
2. **IT (Amendment) Act, 2008**: Addresses hacking, data theft, and cyber terrorism.
3. **National Cyber Security Policy, 2013**: Focuses on securing critical infrastructure.
4. **RBI Guidelines**: Secures digital banking and financial systems.

**International Standards**

1. **ISO/IEC 27001**: Framework for ISMS.
2. **NIST Framework**: Risk-based approach to cybersecurity.
3. **PCI DSS**: Secures credit card transactions.
4. **GDPR**: Ensures personal data protection globally.

**Data Protection and Privacy**

* Protects individual privacy rights while allowing data controllers to operate securely.
* Aims to balance privacy with the necessity of data collection in technology.

**Copyright in Cyberspace**

1. Protects digital content like images, videos, and software.
2. Challenges include global jurisdiction, anonymity, and rapidly evolving technology.
3. Online piracy significantly affects copyright holders' revenues.

**Security Audits**

1. Assess an organization's security infrastructure and identify vulnerabilities.
2. Types: Compliance audits, penetration tests, and risk assessments.
3. Helps ensure compliance with standards and enhance overall security posture.

**System Security Engineering Capability Maturity Model (SSE-CMM)**

1. Process-oriented methodology for developing secure systems.
2. Defines processes like risk assessment, threat evaluation, and security validation.
3. Five maturity levels, from informal processes to continuous improvement.

**COBIT Framework**

1. Provides IT governance best practices.
2. Aligns IT processes with business goals.
3. Enhances communication between IT and business stakeholders.

**UNIT - 4**

| **Section No.** | **Section Name** |
| --- | --- |
| 43 | Penalty and compensation for damage to computer resource |
| 65 | Tampering with Computer Source Documents |
| 66 | Computer-Related Offenses |
| 66A | Punishment for Sending Offensive Messages through Communication Service |
| 66B | Punishment for Dishonestly Receiving Stolen Computer Resource or communication device |
| 66C | Punishment for Identity Theft |
| 66D | Punishment for Cheating by Personation by using computer resource |
| 66E | Punishment for Violation of Privacy |
| 66F | Punishment for Cyber Terrorism |
| 67 | Punishment for publishing or transmitting obscene material in electronic form |
| 67A | Punishment for publishing or transmitting of material **containing** sexually explicit act, etc. in electronic form |
| 67B | Punishment for publishing or transmitting of material **depicting** children in sexually explicit act, etc. in electronic form |
| 67C | Preservation and Retention of Information by Intermediaries |
| 68 | Power of Controller to Give Directions |
| 69 | Powers to issue directions for interception or monitoring or decryption of any information through any computer resource |
| 69A | Power to Issue Directions for Blocking Public Access of any information through any computer resource |
| 69B | Power to authorize to monitor and collect traffic data or information through any computer resource |
| 70 | Protected Systems |
| 70A | National Nodal Agency |
| 70B | Indian Computer Emergency Response Team (CERT-In) to serve as national agency for incident response |
| 71 | Penalty for Misrepresentation |
| 72 | Breach of Confidentiality and Privacy |
| 72A | Punishment for Disclosure of Information in Breach of Lawful Contract |
| 73 | Penalty for Publishing False Electronic Signature Certificates |
| 74 | Publication for Fraudulent Purpose |
| 75 | Act to Apply for Offense or Contraventions committed Outside India |
| 76 | Confiscation |
| 77 | Compensation, Penalties, or Confiscation Not to Interfere with other Punishment |
| 77A | Compounding of Offenses |
| 77B | Offenses with Three Years Imprisonment to be Cognizable |
| 78 | Power to Investigate Offenses |

**Introduction to Cyber Law**

* Cyber Law governs the legal aspects of cyberspace, including the internet, digital information, e-commerce, and IT security.
* Combines contract law, intellectual property law, privacy law, and data protection law.
* Aims to protect individuals and organizations from cybercrimes, ensuring secure digital environments.
* Covers fraud, defamation, intellectual property protection, trade secrets, and online harassment.

**Importance and Objectives of Cyber Law**

1. **Legal Oversight**: Monitors internet activities, regulates e-commerce, and ensures secure digital transactions.
2. **Data Protection**: Safeguards sensitive personal and business data.
3. **Cybercrime Prevention**: Addresses hacking, identity theft, and online fraud.
4. **Global Uniformity**: Promotes international consistency in cyber regulations.
5. **E-Governance Enablement**: Supports digital infrastructure and paperless governance.

**Major Areas of Cyber Law**

1. **Fraud Prevention**: Protects users from identity and financial theft.
2. **Copyright Protection**: Safeguards intellectual property in the digital space.
3. **Harassment and Stalking**: Criminalizes threatening online behavior.
4. **Trade Secrets**: Protects proprietary business information.
5. **Cybersecurity**: Ensures safe online interactions through encryption and secure systems.

**Information Technology Act, 2000**

**Background**

* Inspired by the UN Model Law on Electronic Commerce (1997).
* Drafted in 1998, passed by Indian Parliament in May 2000, and came into effect on October 17, 2000.
* Provides a legal framework for digital records, signatures, and e-commerce.

**Key Objectives**

1. Legal recognition of digital transactions.
2. Facilitation of secure e-governance.
3. Addressing cybercrimes with defined penalties.
4. Regulation of Certifying Authorities (CAs) for digital signatures.
5. Ensuring data protection and cybersecurity.

**Key Features of the IT Act**

1. **Electronic Transactions**: Recognizes digital records and signatures as legally valid.
2. **Certifying Authorities**: Supervises and licenses entities that issue Digital Signature Certificates.
3. **Cybercrimes**: Defines and penalizes offenses like hacking, data theft, and identity fraud.
4. **Jurisdiction**: Covers offenses affecting Indian systems, even if committed outside India.
5. **Amendments (2008)**: Expanded scope to include privacy violations, child protection, and cyber terrorism.

**Important Sections of the IT Act**

**Electronic Records and Authentication**

1. **Section 3**: Digital signatures authenticate electronic records.
2. **Section 4**: Electronic records are legally equivalent to paper-based records.
3. **Section 5**: Legal recognition of electronic signatures.

**Cyber Offenses**

1. **Section 43**: Penalty for unauthorized access or data theft.
2. **Section 65**: Punishment for tampering with computer source documents.
3. **Section 66**: Covers fraudulent or dishonest computer-related activities.
4. **Section 66A**: Penalized offensive electronic messages (repealed in 2015).
5. **Sections 66B to 66F**:
   * Dishonest receipt of stolen assets.
   * Identity theft (66C) and impersonation (66D).
   * Violation of privacy (66E).
   * Cyber terrorism threatening national security (66F).

**Obscene Content and Child Protection**

1. **Section 67**: Punishment for publishing obscene material online.
2. **Section 67A**: Addresses sexually explicit acts in electronic form.
3. **Section 67B**: Prohibits child pornography and related activities.

**Cybersecurity Provisions**

1. **Section 69**: Government powers to intercept, monitor, and decrypt data for national security.
2. **Section 70**: Declares critical information infrastructure as protected systems.
3. **Section 70A**: National nodal agency for critical infrastructure protection.
4. **Section 70B**: CERT-In serves as the national cybersecurity incident response team.

**Regulation of Certifying Authorities**

1. Certifying Authorities (CAs) issue Digital Signature Certificates.
2. Controller of Certifying Authorities supervises CAs and enforces compliance.
3. Licenses are issued based on prescribed qualifications, infrastructure, and practices.
4. Recognizes foreign Certifying Authorities for global interoperability.

**Duties of Subscribers and Intermediaries**

**Subscribers:**

1. Safeguard private keys and notify authorities if compromised.
2. Verify the accuracy of Digital Signature Certificates.
3. Accept responsibility for secure electronic transactions.

**Intermediaries:**

1. Retain specified information for a prescribed period.
2. Assist in investigations and monitoring as required by authorities.
3. Ensure compliance with cybersecurity guidelines.

**Amendments and Future Developments**

**2008 Amendment:**

* Introduced Sections 66A to 66F for advanced cybercrimes.
* Added provisions for child protection, privacy, and monitoring.

**Proposed Digital India Act:**

* Aims to replace the IT Act with regulations on privacy, social media oversight, and emerging technologies like AI and IoT.

**Offenses and Penalties**

1. **Section 72**: Breach of confidentiality and privacy.
2. **Section 73**: Publishing false Digital Signature Certificates.
3. **Section 74**: Fraudulent creation or use of Digital Signature Certificates.
4. **Corporate Liability**: Companies are liable for negligent handling of sensitive personal data (Section 43A).

**Special Provisions**

1. **Jurisdiction (Section 75)**: Covers offenses involving Indian systems, irrespective of offender location.
2. **Confiscation (Section 76)**: Devices used in contraventions may be confiscated.
3. **Enforcement**:
   * Compounding of offenses punishable with imprisonment up to 3 years (Section 77A).
   * Only police officers above Inspector rank can investigate offenses (Section 78).

**Conclusion**

The **IT Act, 2000** and its amendments provide a robust legal framework for regulating digital activities, addressing cybercrimes, and ensuring cybersecurity. Its evolution reflects the growing complexities of cyberspace, with the proposed **Digital India Act** aiming to address new challenges and technologies comprehensively.