SVKM'S NMIMS (Deemed-to-be University)
MUKESH PATEL SCHOOL OF TECHNOLOGY MANAGEMENT AND ENGINEERING
NAVI MUMBAI CAMPUS

Experiment No. 10

A.1 Aim:

1. Cyber Laws studies – Civil, Criminal and International Laws

A.2 Prerequisite:

1. Softcopy of Niranjan Reddy and Dejey Murugan book.

A.3 Outcome:

Understand various laws prevailing across various countries which may have impact on cyber forensics activities.

A.4 Theory:

Refer to ebook Practical Cyber Forensics by Niranjan Reddy Chapter 14 (Cyber Law and Cyber warfare)

Refer to ebook Cyber Forensics by Dejey Murugan Chapter 13 (Cyber Laws in India) and Chapter 14 (International Cyber Laws and Case studies)

SVKM'S NMIMS (Deemed-to-be University)
MUKESH PATEL SCHOOL OF TECHNOLOGY MANAGEMENT AND ENGINEERING
NAVI MUMBAI CAMPUS

SVKM'S NMIMS (Deemed-to-be University)
MUKESH PATEL SCHOOL OF TECHNOLOGY MANAGEMENT AND ENGINEERING
NAVI MUMBAI CAMPUS

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the portal or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no portal access available)

Roll. No. A053	Name: Nishant Baruah
Class: BTech CE	Batch: 2
Date of Experiment: 13/09/24	Date of Submission: 13/09/24
Grade:	

B.1 Task to do:

Task 1.

1. Summarize your understanding on the following laws:
    a. IT Act 2000 and IT Amamendment Act 2008
    b. Indian Penal Code 1860
    c. The Indian Evidence Act 1872
    d. The Indian Telegraph Act 1872
    e. Banker's Book of Evidence Act 1891

2. Summarize your understanding on the following laws:
    a. General Data Protection Regulation (GDPR)
    b. Personal Information Protection and Electronic Document Act
    c. Cybercrime Laws in UK
    d. Cybercrime Laws in USA

3. Analyze the gaps in Indian laws after studying the international laws.

1] Here's a summary of the mentioned laws:

a. IT Act 2000 and IT Amendment Act 2008

- **IT Act 2000**: The Information Technology (IT) Act of 2000 was enacted to provide a legal framework for e-commerce and cyber activities in India. It deals with electronic transactions, digital signatures, cybercrimes, and the regulation of internet activities. The Act recognizes electronic records and digital signatures, and it outlines penalties for cybercrimes like hacking, identity theft, and unauthorized access to computer systems.
- **IT Amendment Act 2008**: This amendment further strengthened the IT Act by addressing new forms of cybercrimes like phishing, cyber terrorism, child pornography, data protection, and privacy breaches. It introduced the concept of intermediaries (e.g., internet service providers) and their liabilities for hosting illegal content.

b. Indian Penal Code (IPC) 1860

- The IPC is the primary criminal code of India, defining various crimes and their punishments. It covers a wide range of offenses, including those against the state, individuals, property, and public tranquility. It also details punishments for crimes like theft, murder, assault, fraud, defamation, and more. The IPC applies to all individuals in India and provides a comprehensive legal framework for criminal law in the country.

c. The Indian Evidence Act 1872

- This act governs the rules and principles related to the admissibility of evidence in Indian courts. It outlines what evidence is permissible during trials, the burden of proof, and how witnesses and documents should be handled in legal proceedings. The act plays a critical role in ensuring that legal proceedings are based on valid, credible, and legally obtained evidence.

d. The Indian Telegraph Act 1885

- This act regulates the use of telegraphs and related communication systems in India. It grants the government the power to establish and regulate telegraph lines and systems. The law also allows the government to intercept communications in cases where it is necessary for national security or public safety, subject to certain legal safeguards.

e. Bankers' Books Evidence Act 1891

- This act provides a legal framework for the admissibility of bank records as evidence in courts. It allows certified copies of bank records, including ledgers, books, and other documents, to be used as evidence without physically

producing the originals in court. This law simplifies the legal process for banking transactions and financial disputes.

2] Here's a summary of the mentioned laws:

a. General Data Protection Regulation (GDPR)

- The **GDPR** is a regulation introduced by the European Union (EU) in 2018, governing data privacy and protection. It sets strict guidelines on how organizations collect, store, process, and share personal data of individuals within the EU. The GDPR emphasizes transparency, requiring businesses to inform individuals about data usage, obtain consent, and ensure data accuracy and security. It also gives individuals rights like access, rectification, deletion (the right to be forgotten), and data portability. Non-compliance can lead to severe penalties, up to 4% of annual global turnover or €20 million, whichever is higher.

b. Personal Information Protection and Electronic Documents Act (PIPEDA)

- **PIPEDA** is a Canadian law that governs how private-sector organizations collect, use, and disclose personal information in the course of commercial activities. It applies to personal data collected from individuals across Canada. PIPEDA requires organizations to obtain consent for data collection, ensure the information is used only for the purpose it was collected, and safeguard it against misuse. Individuals have rights under PIPEDA, including the right to access and correct their personal data. It also requires organizations to be transparent about their data protection practices.

c. Cybercrime Laws in the UK

- The UK has several laws to combat cybercrime, the most notable being the **Computer Misuse Act 1990**. This act criminalizes unauthorized access to computer systems, hacking, and the distribution of malware. Offenses under this law include accessing computer systems without permission, modifying data without authorization, and impairing the operation of computers. Other relevant laws include the **Data Protection Act 2018**, which complements GDPR principles in the UK, and laws covering cyber terrorism, online harassment, and data breaches. The UK also has **RIPA** (Regulation of Investigatory Powers Act), which allows lawful interception of communications under strict circumstances.

d. Cybercrime Laws in the USA

- In the USA, cybercrime is governed by various federal and state laws. One key federal law is the **Computer Fraud and Abuse Act (CFAA)**, which criminalizes unauthorized access to computers, cyber fraud, and attacks on computer

systems. The **Electronic Communications Privacy Act (ECPA)** protects the privacy of communications over the internet, making unauthorized surveillance or interception illegal. The **USA PATRIOT Act** expanded the government's authority to investigate cyber-related threats, particularly in cases of terrorism. Additionally, the **Children's Online Privacy Protection Act (COPPA)** protects children's privacy online. Each state also has its own cybercrime statutes, dealing with issues such as identity theft, phishing, and online fraud.

Conclusion:

3] After studying international cybersecurity laws, particularly from regions like the EU, Canada, the UK, and the USA, several gaps become evident in Indian cybersecurity laws. Below is an analysis of these gaps:

1. Data Protection and Privacy

- **Absence of a comprehensive data protection law**: India lacks a comprehensive data protection law similar to the **GDPR** in the EU. While the **Information Technology (IT) Act, 2000** addresses cybersecurity and data privacy to some extent, it does not offer the robust, detailed framework for data protection like GDPR or **PIPEDA** in Canada. India has introduced the **Digital Personal Data Protection (DPDP) Bill, 2023**, but it's yet to fully enforce stringent rules comparable to GDPR, especially in terms of user rights (e.g., right to be forgotten, data portability).
- **Limited user rights**: Unlike GDPR, Indian law doesn't explicitly provide individuals with significant control over their personal data. The right to erasure, rectification, and portability is not as clearly defined as it is in GDPR or PIPEDA.
- **Weak penalties for data breaches**: Penalties in India for violations of data privacy are not as stringent as those under GDPR, which imposes fines of up to 4% of global annual turnover or €20 million, whichever is higher. Indian laws need more severe and enforceable penalties to ensure compliance from corporations.

2. Cybercrime Provisions

- **Lack of comprehensive cybercrime framework**: The **IT Act, 2000** and its amendments focus more on specific cybercrimes like hacking, identity theft, and cyber terrorism but fail to cover emerging threats such as **deepfake technology**, **ransomware attacks**, and **cryptocurrency-related crimes**. Countries like the **USA** (under CFAA and ECPA) and the **UK** (under the Computer Misuse Act) have more comprehensive frameworks for evolving cybercrimes, addressing both traditional and emerging threats.
- **Protection against surveillance and interception**: The **Indian Telegraph Act, 1885** and **Section 69 of the IT Act** allow the government to intercept communications under specific conditions. However, unlike the **ECPA in the USA** or **RIPA in the UK**, India lacks robust legal safeguards to ensure that such surveillance does not violate privacy rights. These other countries have strict procedures for lawful interception with built-in transparency mechanisms.

3. Lack of a Regulatory Framework for Critical Infrastructure

- **Inadequate protection for critical infrastructure**: Indian laws lack a specialized framework to protect critical infrastructure like energy, healthcare, and finance against cyberattacks. The **USA** has the **Critical Infrastructure Protection (CIP) standards** and the **National Institute of Standards and Technology (NIST)** cybersecurity framework, which provide detailed regulations and guidelines for protecting key infrastructures. India's cybersecurity frameworks, managed by **CERT-In**, are not as robust in this area.

4. Lack of Clear Guidelines for Intermediaries

- **Inconsistent intermediary liability**: The role and responsibility of intermediaries (such as ISPs, social media platforms) in managing illegal content or cybercrimes are not as clearly defined in Indian laws as they are in international laws. The **IT Rules, 2021** introduced more regulations for intermediaries, but they do not fully match the clarity and scope seen in the **Digital Millennium Copyright Act (DMCA)** in the USA or the **GDPR**'s intermediary provisions in the EU.

5. Cybersecurity Regulations for Emerging Technologies

- **Insufficient regulation for AI, IoT, and Blockchain**: Indian laws do not yet have specific regulations for emerging technologies such as **Artificial Intelligence (AI)**, **Internet of Things (IoT)**, **blockchain**, and **cryptocurrencies**. Internationally, regions like the **EU** and **USA** have started addressing these through targeted regulations (e.g., EU's **AI Act**, US **blockchain regulations**). India's framework is still catching up with these evolving technologies, leaving gaps in areas like data collection from IoT devices and legal accountability in AI-based systems.

6. Cyber Forensics and Evidence Collection

- **Outdated legal mechanisms for evidence collection**: Indian laws governing cyber forensics and the collection of digital evidence are outdated compared to those in the UK or USA. The **Indian Evidence Act, 1872**, while recognizing digital evidence, lacks modern amendments to deal with cloud-based evidence, cross-border data, and encryption issues, whereas **PIPEDA** in Canada and US laws have clear provisions for dealing with such complexities.

7. Coordination with Global Cybersecurity Standards

- **Lack of harmonization with international standards**: India's cybersecurity standards are not fully aligned with international standards like **ISO/IEC 27001** (information security management) or **NIST** cybersecurity frameworks. This lack of harmonization makes it difficult for Indian organizations to integrate with global best practices, and it can create challenges in international trade or cross-border collaborations.

8. Cybersecurity Training and Awareness

- **Need for enhanced training and awareness programs**: Countries like the **UK** and the **USA** have invested significantly in national cybersecurity awareness programs for businesses and citizens. India needs more structured initiatives at both the corporate and grassroots levels to improve awareness of cybersecurity threats, defenses, and best practices.

Recommendations to Address Gaps

1. **Enforce Comprehensive Data Protection Law**: Implement and enforce a data protection law akin to **GDPR**, offering stronger individual rights and penalties.
2. **Broaden Cybercrime Legislation**: Update the **IT Act** to include emerging threats like ransomware, deepfakes, and crypto-related crimes.
3. **Develop Critical Infrastructure Protection Standards**: Implement regulations for the cybersecurity of critical infrastructure akin to the **USA's NIST** framework.
4. **Clarify Intermediary Liability**: Strengthen laws governing intermediary platforms, ensuring they adhere to content moderation and cybersecurity protocols.
5. **Regulate Emerging Technologies**: Introduce regulations for **AI, IoT**, and **blockchain** to address data privacy, accountability, and security issues.
6. **Enhance Cyber Forensics Framework**: Modernize the **Indian Evidence Act** to address digital forensics, encryption, and cross-border data sharing challenges.
7. **Align with International Standards**: Promote harmonization of Indian cybersecurity laws with international standards like **ISO** and **NIST** to foster global cooperation.
8. **Promote Cybersecurity Awareness**: Develop national-level programs to train businesses, individuals, and government personnel on modern cybersecurity threats and best practices.