CYBER LAWS AND FORENSIC 2023
(CORE 16)
B TECH SEM VIII SVNIT SURAT

SNEHAL VAKILNA

ADVOCATE

CYBER LAWYER, INVESTIGATOR AND DATA PROTECTION SPECIALIST INDIA

(M com , LLB , Sp. Cyber Laws and Sp. Cyber Crime Investigation)

OFFICE :

U-5, ORNET PALACE, AMARKUNJ SOC GHOD DOD ROAD SURAT.

CONTACT NO -+91- 9898133034

EMAIL ID: snehalvakilnain@gmail.com

Disclaimer

This Session is Strictly for Education Purpose.

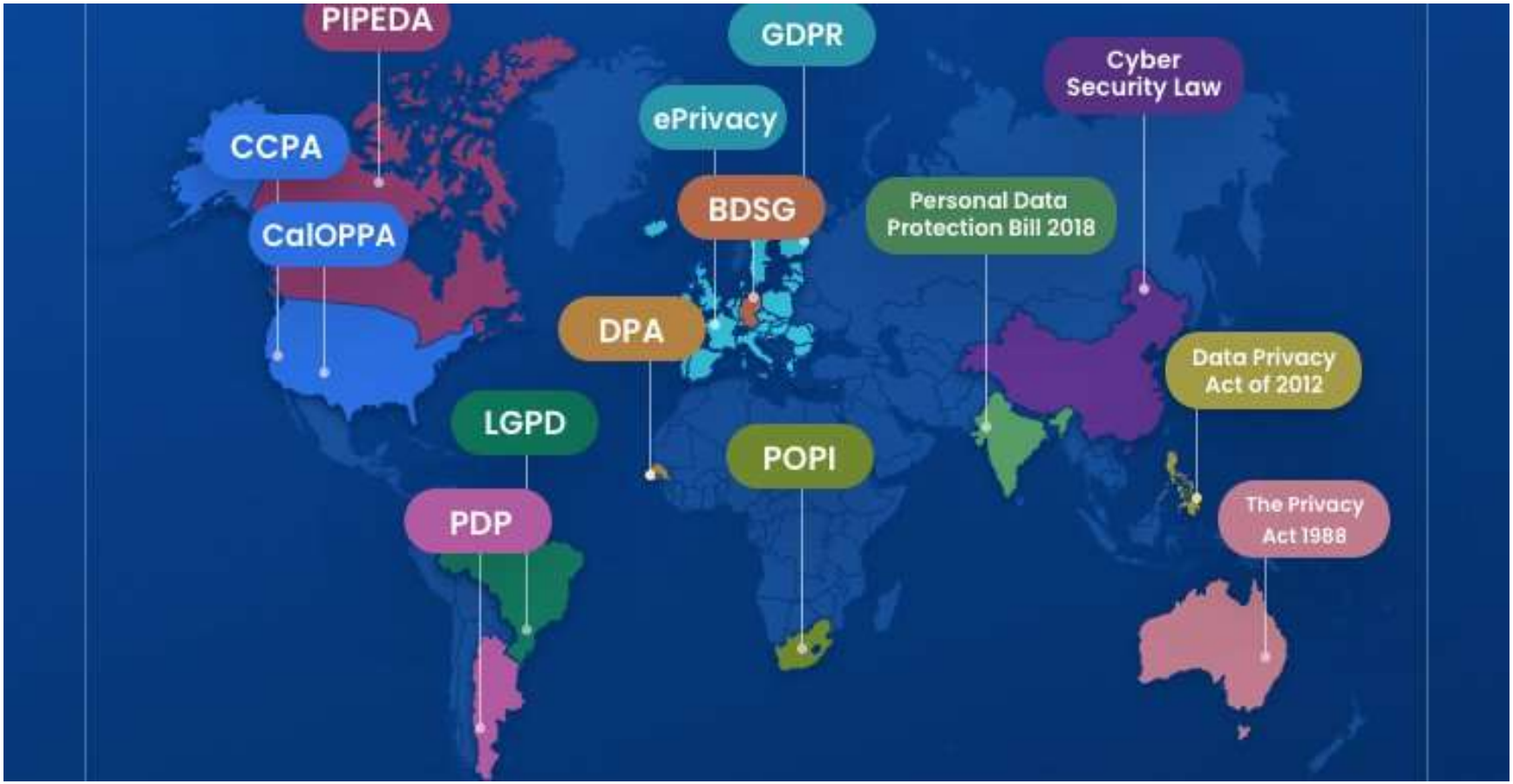
"The **JURISPRUDENCE OF CYBER LAW, CYBER SECURITY AND ELECTRONIC EVIDENCE** IS STILL *EVOLVING AND NOT EVOLVED*". (CONSTRUCTIVE LEARNING)

This Session is **"AS OF THE DAY"**

"AS PER THE LAW"

to the best of my knowledge

Cyber Crimes and Legal Landscape Around the World



HISTORICAL INTERNATIONAL INTIATIVES

- **First comprehensive international effort** dealing with *the criminal law problems of computer crime* was initiated by the **Organization for Economic Co-operation and Development** (OECD)

- **United Nations (UN)Commission** on International Trade Law (UNCITRAL) formulated the UNCITRAL Model Law on **Electronic Commerce in 1996**.It is intended to facilitate the use of **modern means of communication and storage of information in trade and commerce** .

Convention on Cyber Crime

- The **Convention on Cyber crime of the *Council of Europe*** **is the** *binding international instrument on the issue of cyber crime*.

- Also Known to be **Budapest Convention on Cybercrime**

- The convention serves as a guideline for participating countries.

- It also **serves as a framework for international cooperation between** participating countries..

International & Intergovernmental Organizations

- **The Council of Europe: Action Against Cybercrime** Council of Europe's ongoing efforts to combat cyber crime, including the **Budapest Convention on Cybercrime** (drafted by the Council) and the work of the **its Monitoring Committee**.

- **International Criminal Police Organization (INTERPOL)** Its core mission is to enable law enforcement agencies in its 190 member countries to work together to combat transnational crime, including **cyber crime** and **crimes against children**.

International & Intergovernmental Organizations

- **International Telecommunications Union (ITU): Cybersecurity Activities** The ITU is a specialized agency of the United Nations that promotes the harmonization of technical standards for information and telecommunications technologies and initiates international cooperation to improve cybersecurity
- **United Nations Office of Drugs and Crime (UNODC)** UN's efforts to combat transnational crime, including cybercrime

Non-Governmental International Organizations

- **Anti-Phishing Working Group (APWG)** international industry association combats phishing and email spoofing
- **European NGO Alliance for Child Safety Online (eNACSO)** international effort for child safety online
- **International Association of Internet Hotlines (INHOPE)** combat the online distribution of child pornography and reporting illegal content.
- **Internet Watch Foundation (IWF)** identify, locate, and remove online images and videos of child sexual abuse in cooperation with law enforcement agencies worldwide.
- **RAND Corporation** is a good source for credible research and informed commentary on a wide range of topics.
- **Spamhaus** ernational non-profit organization based in London and Geneva tracks cyber threats

U.S. Federal Government Agencies

- **Department of Justice: Division of Computer Crime & Intellectual Property Section (CCIPS)** works with other federal agencies, the private sector, and foreign law enforcement agencies to prevent, investigate, and prosecute computer and intellectual property crimes.

- **Department of Homeland Security**

U.S. Federal Government Agencies

- **Department of Homeland Security**

following operate under the umbrella of the DHS—play a role in combating cyber crime:

- ✓ **Cybersecurity & Infrastructure Security Agency (CISA)** combat cybercrime is one of CISA's core responsibilities.
- ✓ **Secret Service** Secret Service's **Cyber Investigations** combat cyber fraud, the illicit use of digital assets, and other forms of transnational organized crime.
- ✓ **Immigration & Customs Enforcement (ICE)** technical support to domestic and international law enforcement agencies investigating cross-border crime.

USA

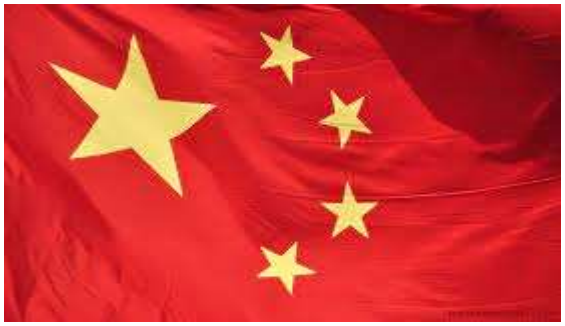
- **Global leader in laws relating** to cyber crime. **Computer Fraud and Abuse Act of 1987** *first to have computer crime laws*.
- 'No Electronic Theft' Act (1997)
- the Digital Millennium Copyright Act (1998), the
- Internet Tax Freedom Act (1998)
- Child Online Protection Act (1998)
- the Children's Internet Protection Act (2001)
- and the USA Patriot Act (2001) etc.

CHINA

In **China**, the major relevant laws are

- **The Computer Information Network and Internet Security, Regulations on Computer Software Protection (2002)** AND

- the **Criminal Law** of the **People's Republic of China (1979)** as revised in 1997



United Arab Emirates

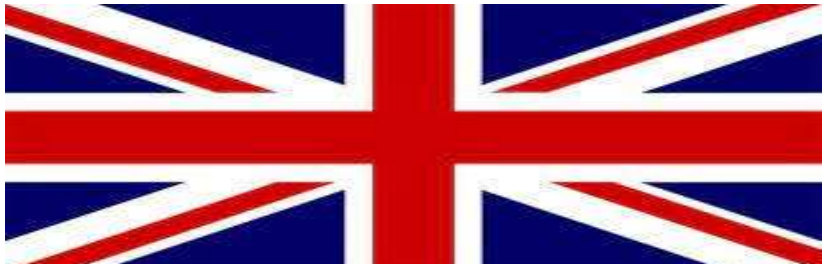
- In United Arab Emirates (UAE), the relevant law for cyber crime is **The Federal Law No. 2 of 2006** Combating Information Technology Crimes

- For electronic commerce, the relevant law is **The Law No. 2 of 2002 of the Emirate of Dubai Electronic Transactions and Commerce Law**

United Kingdom

In the **United Kingdom** the relevant laws for cyber crime are

- the Forgery and Counterfeiting Act (1981)
- Computer Misuse Act (1990)
- Data Protection Act (1998)
- Terrorism Act (2000)
- Regulation of Investigatory Powers Act (2000)



United Kingdom

- Anti-terrorism, Crime and Security Act (2001)
- Fraud Act (2006).

For electronic commerce, the relevant laws are the

- Electronic Communications Act (2000) and
- the Electronic Signatures Regulations (2002).

Australia:

- In **Australia** the relevant law for cyber crime is the
- Cybercrime Act (2001) and the
- Revised Criminal Code Act (1995)

For electronic commerce, the relevant law is the

- Electronic Transactions Act 1999.
- The Commonwealth's Privacy Act (1988).

Australia

- **Australia's Privacy Principles** (APP) is a collection of **13 principles guiding the handling of personal information**. It is chargeable offense to look at private or classified material.

Canada:

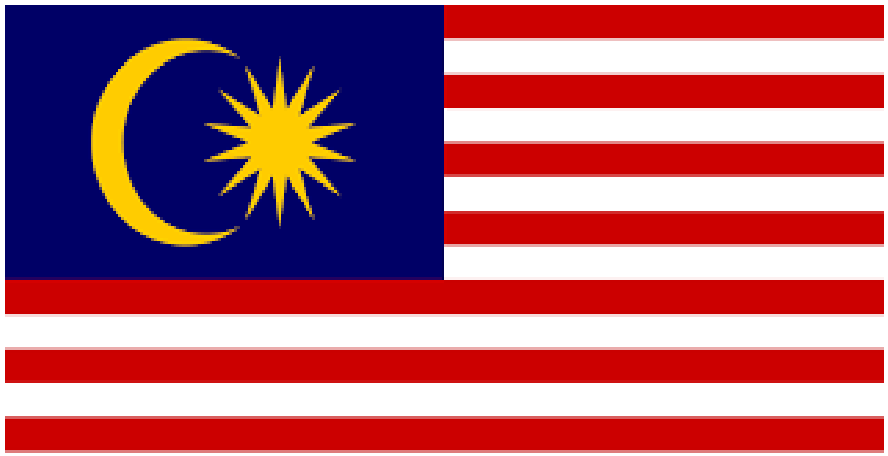
- In **Canada**, the relevant law for cyber crime is the **Criminal Code as amended to include computer crimes**. For electronic commerce, the relevant law is the **Electronic Transactions Act (2001).**

Canada

- **Canada's Personal Information Protection and Electronic Data Act (PIPEDA)** governs how you can collect, store, and use information about users online in the course of commercial activity.
- According to the act, you must make information regarding your privacy policies publicly available to customers

Malaysia:

- In **Malaysia**, the relevant law for cyber crime is the **Computer Crimes Act (1997)**.
- For electronic commerce, the relevant law is the **Digital Signatures Act** (1997).
- Malaysia's **Personal Data Protection Act 2010** protects any personal data collected in Malaysia from being misused



Singapore:

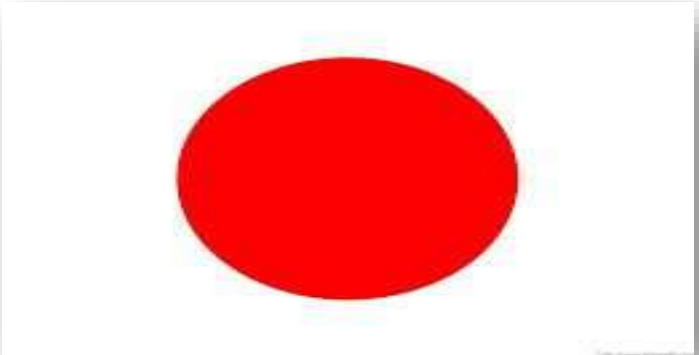
- In **Singapore** the relevant law for cyber crime is the **Computer Misuse Act**.
- For electronic commerce, the relevant law is the **Electronic Transactions Act (1998).**

Singapore:

- In Singapore, personal data is protected under the **Personal Data Protection Act**.
- According to the act, you may only collect personal data only **with the consent** of the individual, and the individual must be informed of the **purpose** for the data collection.

Japan:

- **Japan** the relevant laws for cyber crime are the Unauthorized Computer Access Law (Law No. 128 of 1999) and
- the Online Dating Site Regulating Act (June 2008).
- In Japan, the **Personal Information Protection Act** protects the rights of individuals in regard to their personal data.

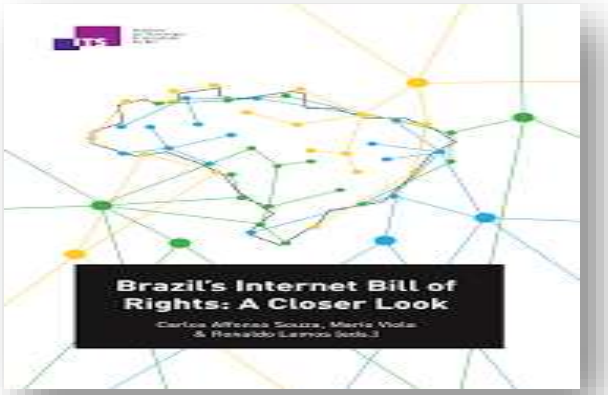


Argentina

- **Cybersecurity is not a highly regulated area in Argentina**
- **<u>Argentina's Personal Data Protection Act of 2000</u>** applies to any individual person or legal entity within the territory of Argentina. (Personal data includes any kind of information that relates to individuals, except for basic information such as name, occupation, date of birth, and address).

Brazil:

- Brazil passed the **Brazilian Internet Act** in 2014 which deals with policies on the collection, maintenance, treatment and use of personal data on the Internet.



Colombia:

- **Colombia's Regulatory Decree 338 for digital security governance**
- **Colombia's Regulatory Decree 1377** states that you must **inform users of the purpose their data will be used for, and you can't use the data for any other purpose without obtaining consent**.

Ireland:

- Ireland is shielded under multi-layers of **laws** and **regulations** relating to **Cybersecurity**.
- **Privacy of personal data is regulated by the Data Protection Act 1988, including a 2003 amendment.**
- There's also the **e Privacy Regulations 2011 (S.I. 336 of 2011)**, which deals with **electronic communication.**

South Africa:

- **South Africa's Cyber Crime Act 2021 partially implemented**
- **<u>Electronic Communications and Transactions Act</u>** applies to any personal data collected through electronic transactions, such as through a website.

European union

- EU is governed by multiple **Cyber Security Act**
- But the recent development **General Data Protection Regulation** implemented from 25 May 2018.
- GDPR is a regulation in EU law on data protection and privacy issues for European Citizen.

General Data Protection Regulation

We have to ensure that data of EU citizens are primarily protected.

It shall apply to any individual, company, data processor outside EU

who is he dealing, handling or processing

the personal data of EU Citizen

General Data Protection Regulation

- EU citizen visiting India, Staying in hotels and Shopping with his credit cards.
- If you don't comply fine

  4 percent of total global turnover in last preceding financial year

  or 20 Million Euros.

India

- In India Law Governing Cyber Space is **Indian Information Technology Act (As amended 2008)**
- **Right to Privacy** had been given Constitutional Privilege and is now a **Fundamental Right**.
- **Digital Personal Data Protection Bill 2022 had been drafted** and can be can be Implemented soon.