Cyber Security Laws & Standards

By Nilesh Ghavate

Introduction

Cybersecurity laws and standards are crucial in today's digital age to ensure the protection of sensitive information, prevent unauthorized access, and mitigate cyber threats.

Various laws and standards have been developed by governments, international organizations, and industry bodies to establish guidelines and requirements for organizations and individuals to follow.

General Data Protection Regulation (GDPR)

- Comprehensive data protection and privacy law established by the European Union (EU). It came into effect on May 25, 2018.
- The GDPR applies to all EU member states and organizations that process the personal data of EU residents, regardless of where the organizations are located.
- Its primary aim is to strengthen the protection of individuals' personal data and provide them with more control over their information in the digital age.
- It sets out strict requirements for **data protection and privacy**, including consent for data collection, the right to be forgotten, breach notification obligations, and stringent penalties for non-compliance.

Key Principles of GDPR:

1. Lawfulness, Fairness, and Transparency: inform individuals about the purposes and legal basis
2. Purpose Limitation: Data should be collected for specified, explicit, and legitimate purposes
3. Data Minimization: Minimum amount of personal data necessary for the intended purpose
4. Accuracy: Ensuring that personal data is accurate and up-to-date.
5. Storage Limitation: PD should be stored in a form that allows identification of data subjects for no longer than necessary for the intended purposes.
6. Integrity and Confidentiality: Ensure the security and confidentiality of PD
7. Accountability: Demonstrate compliance through documentation and transparency

Key Rights of Data Subjects:

1. Right to Access
2. Right to Rectification
3. Right to Erasure (Right to be Forgotten)
4. Right to Restriction of Processing
5. Right to Data Portability
6. Right to Object
7. Rights Related to Automated Decision Making and Profiling

Under the GDPR, some organizations are required to appoint a Data Protection Officer (DPO).

Enforcement and Penalties up to €20 million or 4% of their global annual turnover, whichever is higher.

California Consumer Privacy Act (CCPA):

- The CCPA is a state-level law in California, United States, that aims to enhance **privacy rights and consumer protection**.
- It grants California residents specific rights regarding the collection, use, and sale of their personal information by businesses.
- It also imposes obligations on businesses, such as providing transparency about data practices and offering opt-out mechanisms.

California Consumer Privacy Act (CCPA):

- **Applicability**: The CCPA applies to for-profit businesses that collect personal information of California residents and meet at least one of the following criteria:

  a. Have an annual gross revenue of over $25 million.

  b. Buy, sell, or share personal information of 50,000 or more consumers, households, or devices for commercial purposes.

  c. Derive 50% or more of their annual revenue from selling consumers' personal information.

CCPA Consumer Right:

a. **Right to Know:** Consumers have the right to know what personal information businesses collect, use, disclose, and sell about them. \
b. **Right to Delete:** Consumers can request businesses to delete their personal information, subject to certain exceptions.
c. **Right to Opt-Out:** Consumers have the right to opt-out of the sale of their personal information to third parties.
d. **Right to Non-Discrimination:** Businesses cannot discriminate against consumers who exercise their CCPA rights, such as denying services or charging different prices.

Health Insurance Portability and Accountability Act (HIPAA):

- HIPAA is a United States federal law that governs the security and privacy of medical records and personal health information.
- It establishes standards for the protection of sensitive healthcare data, requires safeguards for electronic health information, and sets guidelines for breach notification and patient consent.

Payment Card Industry Data Security Standard (PCI DSS):

- The PCI DSS is a set of security standards developed by major payment card brands, such as Visa, Mastercard, and American Express.
- It applies to organizations that handle payment card transactions and aims to protect cardholder data.
- The standard includes requirements for network security, encryption, access control, vulnerability management, and regular security assessments.

NIST Cybersecurity Framework

- The NIST Cybersecurity Framework is a set of guidelines and best practices developed by the U.S. National Institute of Standards and Technology.
- It provides a risk-based approach to managing and improving cybersecurity posture, offering a flexible framework that can be adapted to various industries and organizational sizes.
- The framework consists of five core functions: Identify, Protect, Detect, Respond, and Recover.

ISO/IEC 27001

- ISO/IEC 27001 is an international standard for information security management systems (ISMS).
- It provides a systematic approach to managing sensitive information, encompassing risk assessment, security controls implementation, and ongoing monitoring and improvement.
- Compliance with this standard demonstrates an organization's commitment to maintaining the confidentiality, integrity, and availability of information.

Computer Fraud and Abuse Act (CFAA)

- The CFAA is a U.S. federal law that criminalizes various computer-related activities, such as unauthorized access to computer systems, stealing information, and causing damage to computer networks.
- It establishes penalties for cybercrime offenses and serves as a legal tool for prosecuting individuals involved in hacking, identity theft, and other cyber-related offenses.

Information Technology Act, 2000 (IT Act):

- The IT Act is the primary legislation governing cyber security in India. It defines various cyber offenses and their penalties, such as unauthorized access, hacking, identity theft, and spreading of computer viruses.
- The act also provides legal recognition for electronic documents and digital signatures, enabling secure electronic transactions.

India's Digital revolution and Global advancements have made our current regulatory landscape old and dated…

Information Technology Act, 2000 (IT Act):

1. **IT Act 2000** is 22 years old and was created in the **early days of internet**.
2. Provisioned for **nascent IT ecosystem in 2000 pre-Digital India** in the absence of modern internet-based service such as e-Commerce, social media platforms
3. **Limited mandate**- legal recognition of electronic records, transactions and electronic signatures over the electronic medium
4. **Internet, Devices and Information Technology** have empowered citizens. However, these have also created challenges in the form of **user harm**; ambiguity in **user rights**; **security**; **women & child safety;** organised information wars, radicalisation and circulation of **hate speech**; **misinformation** and **fake news**; **unfair trade practices**, etc.

The Indian Computer Emergency Response Team (CERT-In):

- CERT-In is the **national nodal agency** for responding to cybersecurity incidents in India.
- It operates under the provisions of the IT Act and is responsible for **collecting, analyzing, and disseminating information on cybersecurity threats and vulnerabilities**.
- CERT-In also provides **incident response** services, issues **alerts and advisories**, and promotes cybersecurity **awareness**.

National Cyber Security Policy, 2013:

- The National Cyber Security Policy aims to **protect** the country's **information infrastructure** and **strengthen cybersecurity capabilities**.
- The goal of this policy is to guarantee safe and reliable cyberspace for individuals, organizations, and the government.
- This Policy aims to protect the information infrastructure in cyberspace, reduce vulnerabilities, develop capabilities to prevent and respond to cyber threats, and minimize damage from cyber incidents through a combination of institutional structures, processes, technology, and cooperation. Also promoting research and development in cybersecurity,

Critical Information Infrastructure Protection (CIIP):

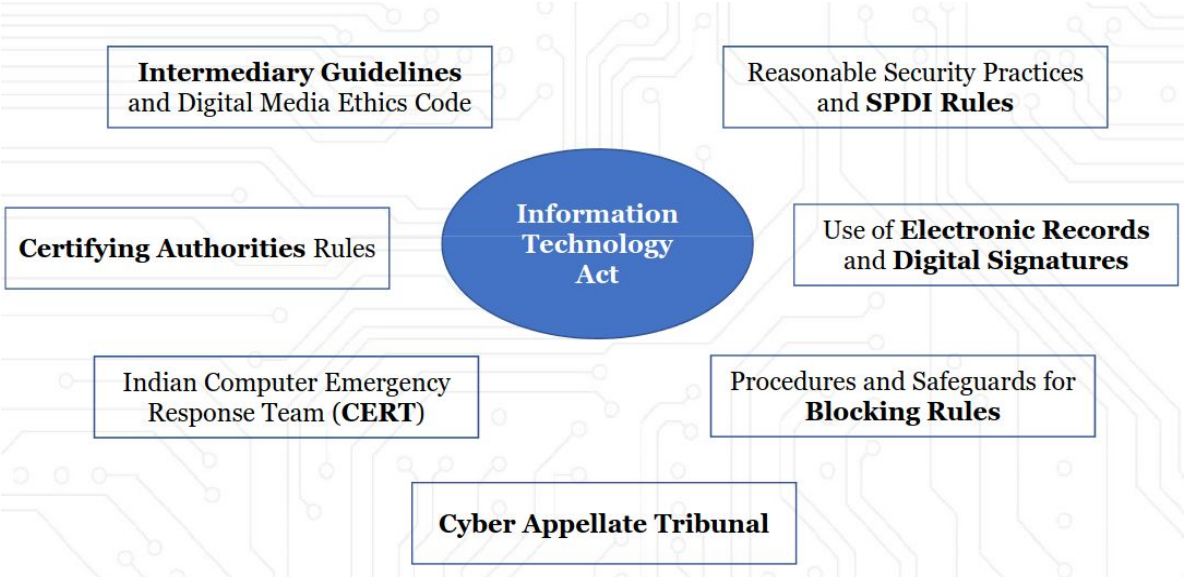
- The CIIP guidelines were introduced by the Indian government to secure critical information infrastructure in sectors such as power, finance, telecommunications, and transportation.

- These guidelines outline the roles and responsibilities of stakeholders, risk assessment methodologies, incident response mechanisms, and cybersecurity measures to be implemented by organizations operating critical infrastructure.

Reserve Bank of India (RBI) Guidelines

- The RBI, as the central banking institution in India, has issued guidelines and regulations to ensure cybersecurity in the banking and financial sectors.
- These guidelines cover aspects such as technology risk management, information security, cyber incident reporting, and cybersecurity audits for banks, payment system operators, and other financial institutions.

Current Regulatory Landscape (India)

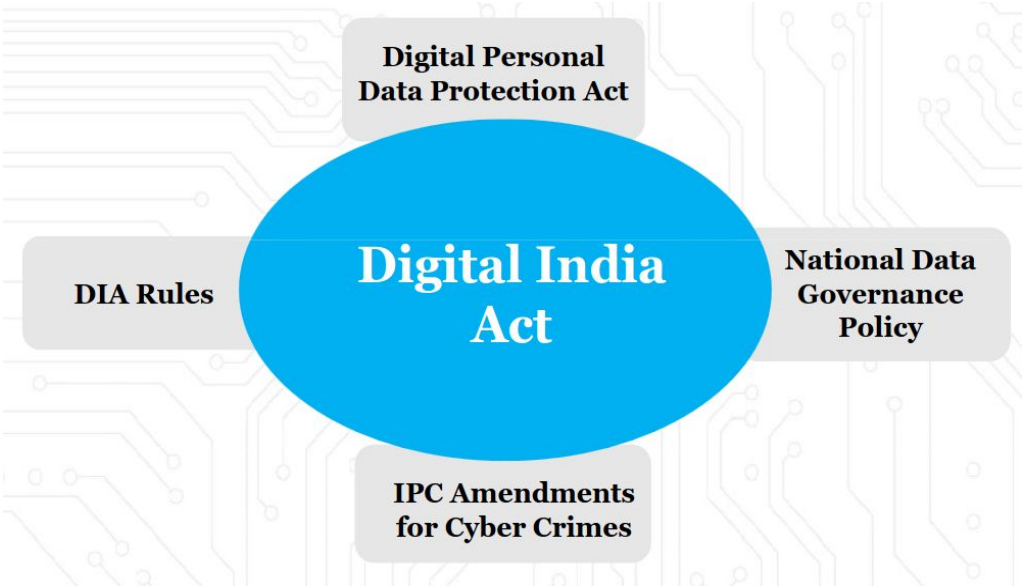


Source: https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

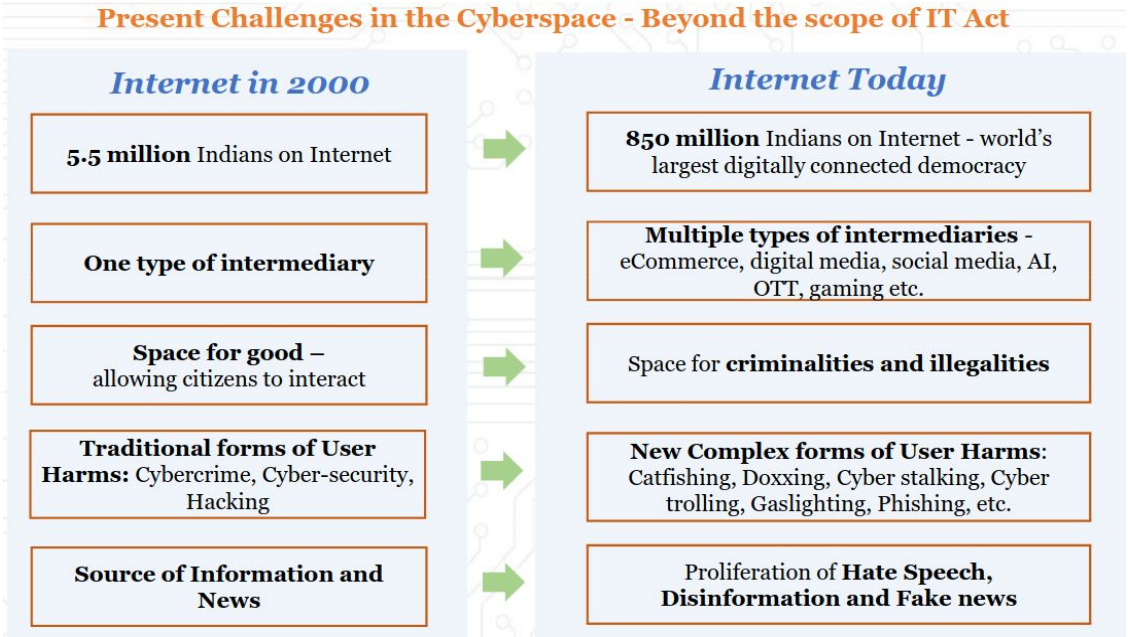
Objectives of Global Standard Cyber Laws

- Ensure Indian Internet is **Open, Safe & Trusted and Accountable**
- Accelerate the growth of **innovation and technology ecosystem**
- Manage the **complexities of internet** and **rapid expansion of the types of intermediaries**
- Create a framework for **accelerating digitalization of Government** and to strengthen democracy and governance (G2C)
- **Protect citizens' rights**
- Address **emerging technologies and risks**
- Being **Future-proof** and **Future-ready**

Framework of Global Standard Cyber Laws



Internet in 2000 vs Internet today



Goals of Digital India Act 2023 - Draft

The new law should evolve through rules that can be updated, and address the tenets of Digital India

- Open Internet
- Online Safety and Trust
- Accountability and Quality of Service
- Adjudicatory mechanism
- New Technologies

Open Internet

- An Open Internet should have

  (a) Choice;
  (b) Competition;
  (c) Online diversity
  (d) Fair market access, and
  (e) Ease of Doing Business and Ease of Compliance for Startups
- **Fair trade practices**, prevention of concentration of market power and gatekeeping, distortions through regulation of dominant Ad-tech platforms, App stores etc., promoting start-up India via **non-discriminatory** access to digital services and **interoperable platforms**.
- **Safeguard innovation** to enable emerging technologies like AI/ML, Web 3.0, Autonomous systems/ Robotics, IoT/ Distributed Ledger/ Blockchain, Quantum Computing, Virtual Reality/Augmented Reality, Real-time language translators, Natural-language processing, etc.
- **Promotion of Digital Governance** ease access to government & other public utility services, **delivery of public services through online and mobile platforms** in a simple, accessible, interoperable and citizen friendly manner.
- May need to update provisions in the **Competition Act, 2002**

Open Internet

Online Safety and Trust

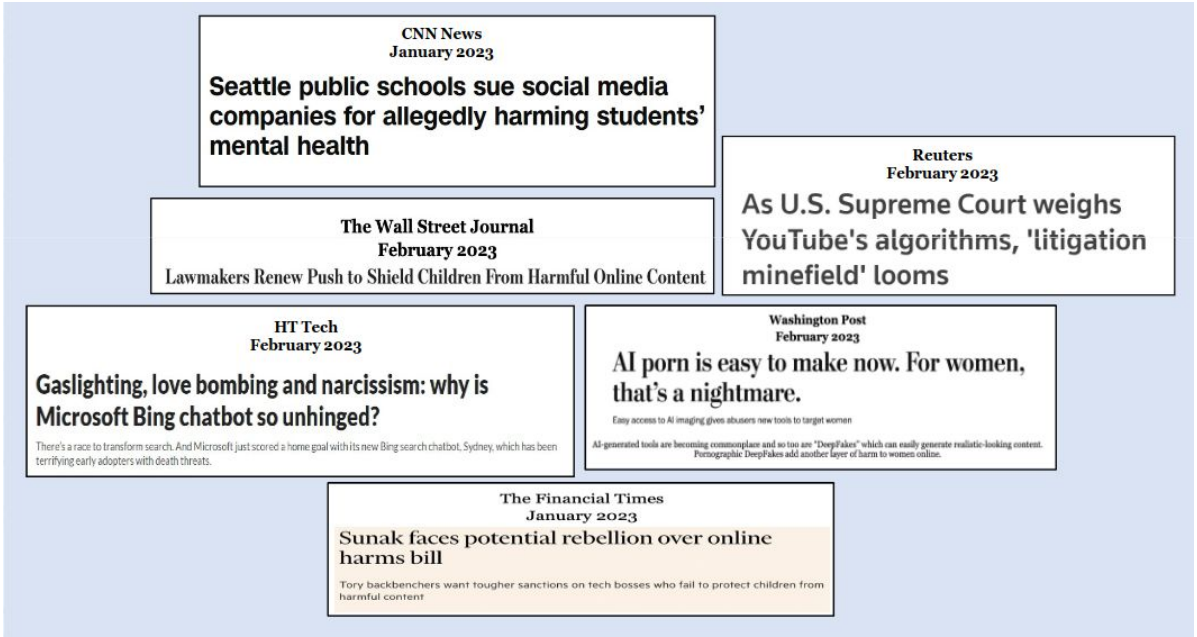
- **Adjudicating User Harm** against revenge porn, cyber-flashing, dark web, women and children, defamation, cyber-bullying, doxing, salami slicing, etc.
- **Age-gating** by **regulating addictive tech** and protect **minors' data**, safety and privacy of children on social media platforms, gaming and betting apps; **Mandatory 'do not track'** requirement to avoid children as data subjects for ad targeting, etc.
- **Digital user rights** including **Right to be forgotten**, Right to secured electronic means, **Right to redressal,** Right to digital inheritance**, Right against discrimination**, Rights against automated decision making, etc.
- **Discretionary moderation of fake news** by social media platforms should be critically examined and regulated under the **Constitutional rights of freedom of speech & expression**.

Online Safety and Trust

- **Definition and Regulation of hi-risk AI systems** through legal, institutional quality testing framework to examine regulatory models, algorithmic accountability, zero-day threat & vulnerability assessment, examine AI based ad-targeting, content moderation etc.
- **Privacy invasive devices** such as spy camera glasses, wearable tech should be mandated under stringent regulation before market entry with strict KYC requirements for retail sales with appropriate criminal law **strict KYC requirements** for retail sales with appropriate criminal law sanctions.
- **Secure Cyberspace** by empowering agencies like **CERT-In** for cyber resilience; strengthening the penalty framework for non-compliance, advisories on the information & data security practices, etc.
- **Content Monetisation Rules** for platform-generated and user-generated content

Online Safety and Trust

User harm, taking various forms - Particularly unique to the internet



Online Safety and Trust

Weaponization of disinformation in the name of Free Speech

Online Safety and Trust

Intermediaries have started acting upon harmful content, but that's not enough !

56 lakh videos (30% of which are from India) Removed

- **Top 3 reasons for channel suspension**: Spam, misleading; Nudity or sexual and Child Safety
- **Top 3 reasons for video removal**: Child Safety, Violent content, nudity or sexual

**July to Sept 2022*

- **Acted upon content:** 322 crore on Facebook and 52 crore on Instagram
- **Top 3 reasons for acting**: Spam, Fake accounts and Adult Nudity & Sexual Activity

**Oct to Dec 2022*

Whatsapp: 97.2 lakh Indian accounts banned

- Accounts are banned when abuse is detected either on the basis of user complain, or through Whatsapp's own tools and resources

**Oct to Dec 2022*

Accountable Internet

- **Adjudicatory and Appellate Mechanisms** for accountable and responsive digital operators; updated intermediary framework; Obligations on significant digital operators through classification/ mandates; **Algorithmic transparency and periodic risk assessments** by digital entities
- Accountability for upholding Constitutional rights of the citizens, esp. Article 14, 19 & 21; Ethical use of AI based tools to protect rights or choices of users;
- **Dedicated inquiry agency** and a specialised Dispute resolution/ adjudication framework.
- **Disclosure Norms** for data collected by Data Intermediaries, collecting data above a certain threshold.
- **Standards for ownership** of anonymized personal data collected by Data Intermediaries

Case Study 1: Inadequate Data Protection at ShopSmart Retailers

Scenario: ShopSmart Retailers is a chain of stores operating across India, offering a wide range of products to consumers. The company maintains a customer database that includes personal data such as names, contact details, and purchase history.

Incident Details: A cyber attack targeted ShopSmart Retailers' database, resulting in unauthorized access to customers' personal data. The attackers stole customer information, including credit card details and transaction history.

Violations ???

Information Technology Act, 2000 (IT Act) Violation:

- **Inadequate Data Security:** ShopSmart Retailers failed to implement appropriate security measures to safeguard its customer database. The lack of proper data protection measures violates the IT Act, which requires organizations to maintain reasonable security practices and procedures to protect sensitive data.
- **Delayed Reporting of Cyber Incident:** The company did not promptly report the data breach to the Indian Computer Emergency Response Team (CERT-In), as mandated by the IT Act. The delay in reporting the incident violates the act's requirement for timely incident reporting.
- **Insufficient Consent and Data Usage Notice**: ShopSmart Retailers did not obtain explicit consent from customers for data processing and did not provide adequate notice about the purposes and extent of data collection and usage, violating the IT Act's requirements for consent and disclosure.

Penalty

Under the PDP Bill, organizations may face fines of up to 2% of their annual global turnover or INR 15 crore (150 million rupees), whichever is higher, for violations related to data processing and consent.

Impact on Business due to irregularities

1. Financial Losses
2. Legal Consequences
3. Reputational Damage
4. Loss of Customer Confidence
5. Regulatory Scrutiny
6. Brand Image Impact
7. Loss of Competitive Advantage
8. Business Disruption

Case Study:

Scenario: TechConnect Solutions is a software development company based in Europe that offers a range of IT solutions to its clients. The company maintains a large database of customer information, including names, addresses, email IDs, and preferences. Recently, an incident occurred where TechConnect Solutions shared customer data with a third-party vendor without obtaining proper consent, resulting in a potential violation of the General Data Protection Regulation (GDPR).

Incident Details: TechConnect Solutions entered into a partnership with a third-party vendor to enhance its customer support services. In the process, the company shared customer data with the vendor, including personal details and customer interaction history, to improve service quality. However, TechConnect Solutions failed to inform its customers about the data sharing or seek explicit consent for sharing their personal information with the vendor.

Upon discovering the incident, concerned customers expressed their dissatisfaction and concerns about the unauthorized data sharing, and a data protection authority was alerted to investigate the matter.

Violations ???

General Data Protection Regulation (GDPR) Violations:

- **Lack of Lawful Basis for Data Sharing:** TechConnect Solutions violated the GDPR's principles of lawful processing by sharing customer data with the third-party vendor without obtaining explicit consent or establishing another lawful basis for the data transfer.
- **Insufficient Notice and Transparency:** The company failed to provide customers with transparent information about the purpose and extent of data sharing with the third-party vendor, violating the GDPR's requirements for clear and concise data processing notices.
- **Unauthorized Data Transfer to Third Countries:** Some of the third-party vendors receiving the personal data were located outside the EU. TechConnect Solutions did not implement appropriate safeguards, such as standard contractual clauses, for such data transfers, violating GDPR's provisions on cross-border data transfers.
- **Failure to Comply with Data Subject Rights:** When clients requested information about their data and objected to data sharing, TechConnect Solutions did not respond adequately. This violates GDPR's provisions on data subject rights, including the right to access and object to data processing.

Penalty

Penalties: Based on the severity of the violations, TechConnect Solutions could face significant penalties under the GDPR:

- Fines: The company may be subject to fines of up to **4% of its global annual revenue or €20 million**, whichever is higher, for the most serious violations.
- Regulatory Investigations: Supervisory authorities may initiate investigations into TechConnect Solutions' data processing practices, leading to further scrutiny and potential enforcement actions.

Impact on Business

1. Financial Penalties
2. Reputational Damage
3. Legal Liabilities
4. Loss of Clients and Business Opportunities
5. Regulatory Oversight