# THOUGHTS ON CYBER SECURITY, DATA PRIVACY & PROTECTION AND INFORMATION TECHNOLOGY LAWS

**By CA (Dr.) Adukia Rajkumar Satyanarayan**

## NEED FOR CYBER SECURITY

Cybersecurity is the practice of protecting inter-connected systems, networks, hardware, software, data and programs from digital attacks. Cyberattacks are becoming more complex and sophisticated, and are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes. Cyber security solutions or measures consist of technological tools, processes and controls to mitigate cyber-attack risk.

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by, it became more transactional with e-business, e-commerce, e-governance and e-procurement etc.

The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber-crime.

By nature, cyberspace is a complex place to regulate because it operates in a border-less jurisdiction which when subjected to a crime or fraud have ripple effects as the victims and culprits of the crime may be located in different regions and furthermore, the after-effects of the crime may have a bearing on different countries (other than the country of the victim or the culprit) at the same time. Hence, the need for dynamic cyber security laws.

## INDIA INITIATIVES & ADMINISTRATIVE FRAMEWORK

In India, several legal, technical, and administrative policy measures have been undertaken for

addressing Cyber Security challenges in the country viz. the National Cyber Security Policy (2013), framework for enhancing Cyber Security (2013), Guidelines on Information Security Practices for Government Entities (2023), enactment of Information Technology (IT) Act, 2000 and setting-up of Indian Computer Emergency Response Team (CERT-In) for 24×7 cyber incident responses, and National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of Critical Information Infrastructure under the IT Act, 2000, Cyber Security Research & Development (R&D) and Capacity Building in Cyber Security.

**MeitY**

The Ministry of Electronics and Information Technology (MeitY) of the Government of India, is the nodal agency responsible for formulating policies related to the Information Technology (IT), cyber security and data privacy in India. It is responsible for formulation, implementation and review of national policies in the field of Information Technology, Electronics and Internet (all matters other than licensing of Internet Service Provider). The functions of the MeitY inter-alia include assistance to other departments in the promotion of E-Governance, E-Commerce, E-Medicine, E-Infrastructure, etc. and matters relating to Cyber Laws and administration of the Information Technology Act, 2000 and other IT related laws.

The National Informatics Centre (NIC) under the MeitY has assisted and set up the following portals: National Cybercrime Reporting Portal (For Citizen to report and track their Cybercrime complaints. (https://cybercrime.gov.in) and National Cyber police Portal (NCPP) – Backend portal for LEAs and financial intermediaries to process the complaints.(https://cyberpolice.nic.in)

This portal is an initiative of Government of India to facilitate victims/complainants to report cybercrime complaints online. It caters to complaints pertaining to cybercrimes only with special focus on cybercrimes against women and children. Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints. Any victim of financial cyber fraud can also dial helpline number 1930.

**National Cyber Security Policy**

National Cyber Security Policy was released in July 2013, to cater to the cyber security

requirements of Government and non-Government entities as well as large, medium & small enterprises and home users. The policy aims at facilitating creation of secured computing environment and enabling adequate trust and confidence in electronic transactions and guiding stakeholders' actions for protection of cyber space. Currently, the Government is formulating the National Cyber Security Strategy (NCSS), which is under the process of approval.

**Indian Computer Emergency Response Team (CERT-In)**

It is a statutory organization of the MeitY and the agency responsible for responding to cybersecurity incidents in India. CERT-In operates 24/7 and offers a range of services, including incident response, vulnerability assessment and penetration testing, and security audit and compliance. It also collaborates with international organizations and governments to exchange information and best practices in the field of cybersecurity. CERT-In has been designated under Section 70B of the Information Technology Act, 2000 to serve as the national agency to perform the following functions in the area of cyber security:

• Collection, analysis and dissemination of information on cyber security incidents
• Forecast and alerts of cyber security incidents
• Emergency measures for handling cyber security incidents
• Coordination of cyber security incident response activities
• Issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
• Such other functions relating to cyber security as may be prescribed.

Some important Initiatives of CERT-In are:

*i. Cert-In Cyber Security Assurance Framework* - CERT-In has created a panel of 'IT security auditing organizations' for auditing, including vulnerability assessment and penetration testing of computer systems, networks & applications of various organizations of the Government, critical infrastructure organizations and those in other sectors of Indian economy.

ii. *CERT-In Cyber Crisis Management Plan (CCMP)* – CERT-In has formulated CCMP for countering cyberattacks and cyber terrorism for implementation by all Ministries/Departments of Central Government, State Governments/UTs and organizations under their administrative control.

iii. *Cyber Swachhta Kendra (CSK) - The Botnet Cleaning and Malware Analysis Centre* - Operated by Cert-In, the CSK has been setup to provide voluntary service to companies w.re.to Botnet cleaning and malware analysis. It purports to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections.

iv. *Cyber Forensics Lab* - CERT-In is equipped with the state-of-the-art equipment and tools to carry out data retrieval, processing and analysis of the raw data extracted from the digital data storage and mobile devices using sound digital forensic techniques. The primary task of the Lab is to assist the Incident Response (IR) team of CERT-In on occurrence of a cyber-incident and extend digital forensic support to carry out further investigation.

**Indian Cybercrime Coordination Centre**

Indian Cybercrime Coordination Centre (I4C) is an initiative of the Ministry of Home Affairs, Government of India to deal with cybercrime in the country in a coordinated and comprehensive manner. I4C focuses on tackling all the issues related to Cybercrime for the citizens, which includes improving coordination between various Law Enforcement Agencies and the stakeholders, driving change in India's overall capability to tackle Cybercrime and to improve citizen satisfaction levels.

Indian Cybercrime Coordination Centre scheme was approved on 05th October 2018. Since its roll out, it has worked towards enhancing the nation’s collective capability to tackle cybercrimes and develop effective coordination among the Law Enforcement Agencies.

**Controller of Certifying Authorities (CCA)**

CCA is a statutory Organization of the MeitY. The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under section 17 of the Information Technology Act for purposes as defined in the Act. The Office of the CCA came into existence on 1st November, 2000. It aims at promoting the growth of E-Commerce and E- Governance through the wide use of digital signatures. The Information Technology Act, 2000 facilitates acceptance of Electronic Records and Electronic Signatures through a legal framework for establishing trust in digital transactions.

The Controller of Certifying Authorities (CCA) licenses and regulates the working of Certifying Authorities (CAs). The CCA digitally signs/certifies the public keys of the CAs and the CAs issue digital signature certificates for electronic authentication of users in cyber world. CAs can be private sector companies, Government departments, public sector companies, or Non-Government Organizations (NGOs). To obtain an Electronic Signature certificate from CA, the applicant needs to undergo a verification process and to issue Digital Signature Certificates (DSC) to applicants, a Know Your Customer (KYC) of DSC applicants are carried out by CA.

**National Informatics Centre (NIC)**

National Informatics Centre (NIC) under MeitY is the technology partner of the Government of India. NIC was established in the year 1976 with the objective to provide technology-driven solutions to Central and State Governments. NIC-CERT Division is the nodal arm of National Informatics Centre (NIC) for managing the cyber security incidents. NIC-CERT acts as a single point of contact and co-ordinate with concerned stakeholders for cyber security incidents targeted at NIC Infrastructure.

**Standardization Testing and Quality Certification (STQC) Directorate**

The STQC is an attached office of the Ministry of Electronics and Information Technology, Government of India, provides quality assurance services in the area of Electronics and IT through countrywide network of laboratories and centers. In the area of IT & e-Governance, STQC provides Software Products/Systems and Process Assurance Services by conducting Testing, Training, Audit and Certifications.

**National Critical Information Infrastructure Protection Centre (NCIIPC)**

National Critical Information Infrastructure Protection Centre is an organization of the Government of India created under Section 70A of the Information Technology Act, 2000, through a gazette notification on 16 January 2014. It is designated as the National Nodal Agency for all measures to protect the nation's 'Critical Information Infrastructure'. 'Critical Information Infrastructure' is defined in Explanation to Section 70(1) of the IT Act 2000, to mean the

computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

Cybersecurity into two sectors: “Non-Critical Infrastructure (NCI),” which is regulated by CERT-In and “Critical Information Infrastructure (CII),” which is regulated by NCIIPIC.

NCIIPC is required to monitor and report national-level threats to critical information infrastructure. The critical sectors include:

- Power and energy
- Banking, financial services, and insurance
- Telecommunication and information
- Transportation
- Government
- Strategic and public enterprises

NCIIPC successfully implemented several guidelines for policy guidance, knowledge sharing, and cybersecurity awareness for organizations to conduct preemptive measures of these important sectors, especially in power and energy. The guidelines represent the first means for regulating such sectors and requiring “mandatory compliance by all responsible entities.”

**Cyber Appellate Tribunal**

Cyber Appellate Tribunal is established under section 48(1) of the Information Technology Act 2000. The Tribunal was initially known as the Cyber Regulations Appellate Tribunal (CRAT). After amendment of the IT Act 2000 in the year 2008 (which came into effect on 27.10.2009) the Tribunal is known as the Cyber Appellate Tribunal (CAT).

The Finance Act 2017 amended the Information Technology Act 2000, and renamed the Cyber Appellate Tribunal as ‘Appellate Tribunal’ and also merged the tribunal with the Telecom Disputes Settlement and Appellate Tribunal (TDSAT). TDSAT established under section 14 of the Telecom Regulatory Authority of India Act, 1997, shall, on and from the commencement of Part XIV of Chapter VI of the Finance Act, 2017 (i.e. from 26.5.2017), be the Appellate Tribunal for the purposes of the Information Technology Act 2000 and the said Appellate Tribunal shall exercise the jurisdiction, powers and authority conferred on it by or under the IT Act 2000. The Central Government shall specify, by notification the matters and places in relation to which the Appellate Tribunal may exercise jurisdiction.

**Sectoral Regulators**

Guidelines on Cyber Security and Information Technology by sectoral regulators like Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority of India (IRDAI) and Telecom Regulatory Authority of India (TRAI) have to be complied with. Department of Telecommunications of the Ministry of Communications also issues directions from time to time which have to be complied with.

## REGULATORY LANDSCAPE

India does not have any exclusive unitary cybersecurity law. The Information Technology (IT) Act, 2000, is the primary law governing the IT industry in India. It covers various aspects of electronic commerce, including digital signatures, cybersecurity, and data protection. India uses the IT Act 2000, a few provisions of the Bharatiya Nyaya Sanhita (earlier Indian Penal Code 1860) and the Bharatiya Sakshya Adhiniyam (earlier Indian Evidence Act 1872) and multiple other sector-specific regulations to promote cyber security standards. The Government also enacted the Digital Personal Data Protection Act, 2023 on 11$^{th}$ August 2023 but it is yet to be notified.

**Legislations having a bearing on Cyber Security and Information Technology:**

- The Information Technology (IT) Act, 2000 and the Rules and Regulations thereunder. More specifically the following Rules are important w.re.to cyber security and data privacy and protection:
    - Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009
    - The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
    - The Information Technology (Security Practices & Procedures for Protected Systems) Rules 2018 (U/s 70 of the IT Act 2000)

    - The Information Technology (Intermediary Guidelines & Digital Media Ethics Code) Rules 2021
- The Digital Personal Data Protection Act, 2023 which was enacted on 11th August 2023, but is yet to be notified
- The Telecommunications Act 2023 was notified in the official gazette on December 24, 2023, after receiving the President of India's assent. However, the whole Act has not yet come into effect. Some sections of the Act came into effect on June 26, 2024.
- The Payment and Settlement Systems Act, 2007
- The Bharatiya Nyaya Sanhita (BNS) which came into effect on July 1, 2024 and repealed and replaced the Indian Penal Code 1860
- The Bharatiya Sakshya Adhiniyam (BSA) which came into effect on July 1, 2024 and repealed and replaced the Indian Evidence Act 1872
- The Consumer Protection Act 2019 and Rules made thereunder
- The Companies Act 2013
- MeitY Order regarding online CSAM - An inter-ministerial committee was constituted by Ministry of Electronics and Information Technology(MeitY) to discuss the issues related to online child sexual abuse materials (CSAM) and its blocking in India. Based on the recommendation of the committee and the approval of Hon'ble Minister of Electronics and Information Technology, MeitY has issued an order dated. 18.04.2017 to Internet Service Providers(ISPs) to adopt and implement Internet Watch Foundation(IWF) resources on or before 31.07.2017 to prevent the distribution and transmission of Online CSAM into India.
- MeitY - Key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organizations managing ICT operations dated 11.4.2018
- MeitY - Public Procurement (preference to Make in India) Order 2019 for Cyber Security Products dated 6.12.2019 - The Government has issued Public Procurement (Preference to Make in India) Order 2017 vide the Department for Promotion of Industry and Internal Trade (DPIIT) erstwhile Department of Policy Industrial and Promotion (DIPP) Notification No. P-45021/2/2017B.E.-II dated 15.06.2017 and partially modified order no No.P-4502112/2017-PP(BE-II) was issued on 28.05.2018 to encourage 'Make in India'. In furtherance to the Public Procurement (Preference to Make in India) Order 2017

notified vide reference cited above, Ministry of Electronics and Information Technology (MeitY) notified Public Procurement (Preference to Make in India) Order No 1(10)/2017CLES dated 02.07.2018 for cyber security products. Ministry of Electronics and Information Technology (MeitY) issued revised Public Procurement (Preference to Make in India) Order 2019 for cyber security products.

- India Computer Emergency Response Team (CERT-In) Guidelines
    - Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet - No. 20(3)/2022-CERT-In dated 28th April 2022
    - Key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organizations managing ICT operations dated 14.3.2017
    - Guidelines on Information Security Practices for Government Entities
- The Reserve Bank of India (RBI) Notifications, Guidelines & Directions:
    - RBI Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators dated 30th July 2024
    - Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 - RBI/2023-24/107 DoS.CO.CSITEG/ SEC.7/ 31.01.015/2023-24 dated 7th November, 2023 – Applicable to banks and certain financial institutions, the guidelines aim to ensure the confidentiality, integrity, and availability of information.
    - RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways - RBI/DPSS/2019-20/174 DPSS.CO.PD.No.1810/02.14.008/2019-20 dated 17th March 2020
    - RBI cyber security framework in banks – RBI/2015-16/418 DBS.CO/CSITE/ BC.11/33.01.001/2015-16 dated 2.6.2016
    - Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach - RBI/2019-20/129DoS.CO/ CSITE/ BC.4083/31.01.052/2019-20 dated 31.12.2019

- RBI Master Directions on Digital Payment Security Controls 2021 - RBI/2020-21/74 DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21 dated 18th February, 2021
- RBI Digital Lending Guidelines 2022 - RBI/2022-23/111 DOR.CRE.REC.66/ 21.07.001/2022-23 dated 2nd September 2022

- Securities and Exchange Board of India (SEBI) Guidelines
  - Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs) dated 20th August 2024
  - SEBI had issued Cybersecurity and Cyber resilience framework for Market Infrastructure Institutions (MIIs) in 2015. Subsequently, SEBI had issued other Cybersecurity and Cyber resilience frameworks in line with MIIs circular of 2015 for following Regulated Entities (Res): Stock Brokers and Depository Participants, Mutual Funds (MFs)/ Asset Management Companies (AMCs), KYC Registration Agencies (KRAs), Qualified Registrar to an Issue and Share Transfer Agents (QRTAs), Portfolio Managers.
  - Further, SEBI has also issued various advisories to REs, from time to time, on Cybersecurity best practices.
  - The CSCRF aims to provide standards and guidelines for strengthening cyber resilience and maintaining robust cybersecurity of SEBI REs. This framework shall supersede existing SEBI cybersecurity circulars/ guidelines/ advisories/ letters and shall be applicable to the following REs:
  - Alternative Investment Funds (AIFs)
  - Bankers to an Issue (BTI) and Self-Certified Syndicate Banks (SCSBs)
  - Clearing Corporations
  - Collective Investment Schemes (CIS)
  - Credit Rating Agencies (CRAs)
  - Custodians
  - Debenture Trustees (DTs)
  - Depositories
  - Designated Depository Participants (DDPs)
  - Depository Participants through Depositories

- Investment Advisors (IAs)/ Research Analysts (RAs)
- KYC Registration Agencies (KRAs)
- Merchant Bankers (MBs)
- Mutual Funds (MFs)/ Asset Management Companies (AMCs)
- Portfolio Managers
- Registrar to an Issue and Share Transfer Agents (RTAs)
- Stock Brokers through Exchanges
- Stock Exchanges
- Venture Capital Funds (VCFs)

- Department of Telecommunications (DoT), Ministry of Communications
  - Telecom Regulatory Authority of India (TRAI) is a statutory body under DoT
  - There are license conditions imposed by DoT for grant of license, which lay down requirement of implementation of measures
  - DoT mainly issues the directions from time to time with respect to cyber security
  - DoT has issued 'Best Practices – Cyber Security' dated 8th July 2020
  - DoT has issued 'Unsafe Practices to be avoided at Workplace' dated 9th September 2020
  - The Telecommunications Act 2023 which was enacted on 24th December, 2023, and of which few sections have been made effective, provides Measures for protection of users under section 28(2) of the Act.
- Insurance Regulatory and Development Authority of India (IRDAI)
  - IRDAI has released the "Information and Cyber Security Guidelines, 2023" – Ref No. IRDAI/GA&HR/GDL/MISC/88/04/2023 dated 24th April 2023
  - Applicability of guidelines - All insurers including Foreign Re-Insurance Branches (FRBs), Insurance intermediaries regulated by the IRDAI viz. covering Brokers, Corporate Agents, Web Aggregators, TPAs, IMFs, Insurance Repositories, ISNP, Corporate Surveyors, MISPs, CSCs and Insurance Information Bureau of India (IIB) shall adhere to the guidelines.
  - Mission of the guidelines - Ensuring the security of all Organization's information assets through implementation of up-to-date security mechanisms for prevention

and monitoring of threats; governance of information security related activities and awareness of all employees

    - Insurance companies have to appoint a Chief Information Security Officer (CISO), who will be responsible inter alia for providing advice and for setting out the Information and Cyber Security Policy (ICSP)
- Pension Fund Regulatory and Development Authority (PFRDA)
    - PFRDA Circular PFRDA/2022/14/I&CS/02 dated 15.6.2022 - Re: Cyber Security Directions & FAQs issued by CERT-In
- General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) is a regulation introduced by the European Union (EU) to protect the privacy and personal data of its citizens. It applies to all organizations that process personal data of EU citizens, irrespective of their location.

## INFORMATION TECHNOLOGY LAW IN INDIA

The Information Technology Act, 2000 received Presidential Assent on 9th June, 2009 and was notified on October 17th, 2000.

The United Nations General Assembly by resolution A/RES/51/162, dated the 30 January 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This is referred to as the UNCITRAL Model Law on E-Commerce. The said resolution recommended inter alia that all States give favorable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information. The Ministry of Commerce Government of India created the first draft of the legislation following the UN termed as "E Commerce Act 1998". After the formation of a separate ministry of Information Technology, the draft was taken over by the new ministry which re-drafted the legislation as "Information Technology Bill 1999". This draft was placed in the Parliament in December 1999 and passed in May 2000. After the assent of the President on

June 9, 2000, the act was finally notified with effect from October 17, 2000 vide notification number G.S.R 788(E).

The IT Act, 2000 consists of thirteen Chapters divided into 90 sections [Sections 91, 92, 93 and 94 of the principal Act were omitted by the Information Technology (Amendment) Act 2008 and has 2 schedules. [Schedule III and IV of the Principal Act were omitted by the Information Technology (Amendment) Act 2008].

The comprehensive legal framework of the IT Act, 2000 provides for:

i. Enabling regime for legal recognition of – E-Commerce, E-Governance, Electronic Records & transactions, E-Signature

ii. Controller of Certifying Authority (CCA)

iii. Adjudication and Appellate mechanism for cyber contraventions

iv. Cyber Crimes with criminal punishment/ penalties provided (vis-à-vis physical crimes under IPC). These include- effective deterrence provisions (Sections 43, 43A, 65, 66, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 70, 72 & 72A) in terms of compensation/ penalty and punishment to deal with cybercrimes.

v. Internet-enabled businesses ('intermediaries') including Social media platforms and mobile applications

vi. Cyber Security through institutional framework of CERT-In, NCIIPC. It covers- Collection and sharing of information related to cyber incidents (Sections 69B & 70B) for effective proactive/reactive actions by CERT-In and investigative actions by law enforcement agencies; Protection of critical information infrastructure (Section 70A)

vii. Blocking of information from public access under section 69A and the rules thereunder in specific conditions, only in the interest of (i) sovereignty and integrity of India, (ii) defence of India, (iii) security of the State, (iv) friendly relations with foreign States
or (v) public order or (vi) for preventing incitement to the commission of any cognizable offence relating to above.

viii. Privacy & security of data related issues (section 43A) (limited to Sensitive Personal Information) and Breach of lawful contract (section 72A)

ix. Takedown / removal of any information appearing on intermediary platforms which are

violative of any law for the time being in force by the appropriate Government or its agency under section 79(3)(b).

Some Important Rules and Regulations under the Information Technology Act 2000 are:

- The Information Technology (Certifying Authority) Regulations 2001
- Information Technology (Certifying Authorities) Rules, 2000.
- Information Technology (Procedures and Safeguards for Interception, Monitoring or Decryption of Information) Rules, 2009.
- Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009
- Cyber Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009
- Cyber Appellate Tribunal (Procedure for Investigation of Misbehavior or Incapacity of Chairperson and Members) Rules, 2009
- Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009
- Information Technology (Guidelines for Cyber Cafe Rules) Rules, 2011
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- The Information Technology (Electronic Service Delivery) Rules, 2011.
- Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013
- Cyber Appellate Tribunal (Powers and Functions of the Chairperson) Rules, 2016.
- The Information Security Practices and Procedures for Protected System Rules, 2018
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Major Provisions in the Information Technology Act 2000

*1. Intermediaries*

- Definition of 'intermediary' has been modified and a new definition has been inserted for "intermediary". "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes"
- As per the amendments in various sections now intermediaries are made more responsible and liable towards their acts. New Section 67C asks intermediaries to preserve and retain certain records for a stated period. New Section 69B is also quite stringent to intermediaries, whereby intermediary has to provide technical assistance and extend all facilities to agency appointed by Government to monitor and collect traffic data or information
- Section 79 of the old Act which exempted intermediaries has been modified to the effect that an intermediary shall not be liable for any third party information data or communication link made available or hosted by him if; (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; (b) the intermediary does not initiate the transmission or select the receiver of the transmission and select or modify the information contained in the transmission; (c) the intermediary observes due diligence while discharging his duties.
- However, section 79 will not apply to an intermediary if the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act or upon receiving actual knowledge or on being notified that any information, data or communication link residing in or connected to a computer resource controlled by it is being used to commit an unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

- Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction of CERT-In, India's nodal agency for cyber security, shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one crore rupees or with both.
- The Ministry of Electronics and Information Technology (MeitY) has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 on 25th February, 2021.

*2. Indian Computer Emergency Response Team (http://www.cert-in.org.in)*

- With the passage of Information Technology (Amendment) Act 2008, Indian Computer Emergency Response Team (CERT-In) has been designated as Nodal agency for coordinating all matters related to cyber security and emergency response. It is now assigned with the task of oversight of the Indian cyber space for enhancing cyber protection, enabling security compliance and assurance in Government and critical sectors and facilitating early warning & response as well as information sharing and cooperation.
- CERT-In is appointed by the Government under section 70B of the Act, with a Director General and other prescribed officers and employees and it shall perform the following functions in the area of cyber security:
    - collection, analysis and dissemination of information on cyber incidents;
    - forecast and alerts of cyber security incidents;
    - emergency measures for handling cyber security incidents;
    - coordination of cyber incidents response activities;
    - issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
    - such other functions relating to cyber security as may be prescribed.
- It will perform its functions in the prescribed manner and in this regard, may call for information and give direction to the service providers, intermediaries, data centres, body

corporate and any other person. Any person who fails to provide the information called for or comply with the direction issued shall be punishable with imprisonment or fine or with both.

*3. National Security Purpose*

- In view of the increasing threat of terrorism in the country, the new amendments include an amended section 69 giving power to the state to issue directions for interception or monitoring of decryption of any information through any computer resource.
- Further, sections 69A and 69B, two new sections, grant power to the state to issue directions for blocking for public access of any information through any computer resource and to authorize to monitor and collect traffic data or information through any computer resource for cyber security.
- Section 69A has been introduced to enable blocking of websites by the central government. Where the Government or any of its officers specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource. The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed. The Government has prescribed the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009
- Section 69B provides powers to central government to collect traffic data from any computer resource. It could be either in transit or in storage. The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted,

received or stored in any computer resource. The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed. The Government has prescribed the Information Technology (Procedures and Safeguards for Interception, Monitoring or Decryption of Information) Rules, 2009.

*4. Certifying Authorities*

- The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users in cyber world. The Controller of Certifying Authorities (CCA) licenses and regulates the working of Certifying Authorities (CAs). The CCA established the Root Certifying Authority (RCAI) of India under section 18(b) of the IT Act to digitally sign/certify the public keys of Certifying Authorities (CA) in the country, and the CAs issue digital signature certificates for electronic authentication of users in cyber world. CAs can be private sector companies, Government departments, public sector companies, or Non-Government Organizations (NGOs).
- To obtain an Electronic Signature certificate from CA, the applicant needs to undergo a verification process and to issue Digital Signature Certificates (DSC) to applicants, a Know Your Customer (KYC) of DSC applicants are carried out by CA.
- The CCA acts as repository of all digital signature certificates and CAs need to get Licence from the Controller to issue digital signature certificates
- The Information Technology (Certifying Authorities) Rules, 2000 prescribe the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA.
- One of the most important compliance under this Rule is that the Certifying Authority should get its operations audited annually by an auditor and such audit shall include:
  (i) security policy and planning;
  (ii) physical security;
  (iii) technology evaluation;
  (iv) Certifying Authority's services administration;
  (v) relevant Certification Practice Statement;

(vi) compliance to relevant Certification Practice Statement;

(vii) contracts/agreements;

(viii) regulations prescribed by the Controller;

(ix) policy requirements of Certifying Authorities Rules, 2000.

The Certifying Authority should also conduct half yearly audit of the Security policy, physical security and planning of its operations and a quarterly audit of its repository.

- Information Technology (Certifying Authority) Regulations, 2001 came into force on 9 July 2001. They provide terms and conditions of licence to issue Digital Signature Certificate and technical standards and procedures to be followed by a Certifying Authority in carrying out its functions.

*5. Offences and Damages, Compensation and Penalties*

- There are Various types of computer crimes defined and stringent penalties provided under the Act
- Section 43. Penalty and compensation for damage to computer, computer system, etc.
- Section 43A. Compensation for failure to protect data
- Section 44. Penalty for failure to furnish information, return, etc.
- Section 45. Residuary Penalty
- Section 65. Tampering with computer source documents.
- Section 66. Computer related offences.
- Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device.
- Section 66C. Punishment for identity theft.
- Section 66D. Punishment for cheating by personation by using computer resource.
- Section 66E. Punishment for violation of privacy.
- Section 66F. Punishment for cyber terrorism.
- Section 67. Punishment for publishing or transmitting obscene material in electronic form.
- Section 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

- Section 67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.
- Section 67C. Preservation and retention of information by intermediaries.
- Section 68. Power of Controller to give directions.
- Section 69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.
- Section 69A. Power to issue directions for blocking for public access of any information through any computer resource.
- Section 69B. Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.
- Section 71. Penalty for misrepresentation.
- Section 72. Penalty for Breach of confidentiality and privacy.
- Section 72A. Punishment for disclosure of information in breach of lawful contract.
- Section 73. Penalty for publishing electronic signature Certificate false in certain particulars.
- Section 74. Publication for fraudulent purpose.
- Section 75. Act to apply for offence or contravention committed outside India.
- Section 76. Confiscation.
- Section 77. Compensation, penalties or confiscation not to interfere with other punishment.
- Section 77A. Compounding of offences.
- Section 77B. Offences with three years' imprisonment to be bailable.
- Section 78. Power to investigate offences.
- Section 84B. Punishment for abetment of offences.
- Section 84C. Punishment for attempt to commit offences.
- Section 85. Offences by Companies
- The amendments introduced to the Information Technology Act, 2000, notified through the Jan Vishwas (Amendment of Provisions) Act, 2023, came into effect on 30th November, 2023 through which five offences have been decriminalized, while penalties for two others have been increased.

- Any police officer, not below the rank of Inspector, or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under the Information Technology Act 2000. Where the arrest is made by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station. The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of section 80 of the IT Act 2000, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

*6. Critical Information Infrastructure and protected system.*

- 'Critical Information Infrastructure' means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.
- 'Protected System' means any computer, computer system or computer network of any organization as notified under section 70 of the IT Act, in the official gazette by appropriate Government.
- The Government may, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system. The Government may authorize persons to access these notified protected systems. Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of section 70 of the IT Act 2000, shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.
- The Central Government has prescribed the information security practices and procedures for such protected system viz. the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018.

**Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018.**

The Government notified the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 (Protected System Rules) on 22nd May, 2018. Under Rule 3 of the Protected System Rules, the organization having "Protected System" shall constitute an Information Security Steering Committee (IISC) under the chairmanship of Chief Executive Officer/Managing Director/Secretary of the organization. The IISC shall be the apex body in the organization w.re.to protected system. The organization having Protected System shall plan, establish, implement, operate, monitor, review, maintain and continually improve Information Security Management System (ISMS) of the Protected System; and shall nominate an officer as Chief Information Security Officer (CISO) with roles and responsibilities as per latest "Guidelines for Protection of Critical Information Infrastructure" and "Roles and Responsibilities of Chief Information Security Officers (CISOs) of Critical Sectors in India" released by National Critical Information Infrastructure Protection Centre (NCIIPC). The CISO shall establish a process in consultation with NCIIPC, for timely communication of cyber incidents on "Protected System" to the said NCIIPC.

**Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021)**

In order to ensure an open, safe & trusted internet and accountability of intermediaries including the social media intermediaries to users, Ministry of Electronics and Information Technology (MeitY) has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021) on 25th February, 2021.
These Rules prescribe the due diligence to be followed by all intermediaries as well as the additional due diligence to be followed by significant social media intermediaries.
The Rules also provide guidelines to be followed by publishers of news & current affairs and also online curated content providers. These Rules supersede the earlier notified Information Technology (Intermediaries Guidelines) Rules, 2011.

**The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules)**

The Information Technology Act 2000 and the SPDI Rules aim to govern how Indian entities and organizations process sensitive info, data protection, data retention, and collection of personal data and other sensitive information. Some sectors like banking, insurance, telecom, and healthcare, also include data privacy provisions as part of their separate statutes. The provisions of the Rules are explained in detail later under data privacy and protection.

## PRIVACY AND DATA PROTECTION

Data is information. The information may be raw, in organized or in unorganized form – whatever form it may be in, the information needs to be protected. With the advent of high-tech instruments and software, data is collected, worked upon and distributed which makes it subject to exchanging hands through various channels. Legal and political issues make it imperative for the data to be securely protected. Privacy concerns exist wherever personally identifiable information or other sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues.

Major sources of information which are compromised and are most prone to breaches are:

- Healthcare records
- Criminal justice investigations and proceedings
- Financial institutions and transactions
- Biological traits, such as genetic material
- Residence and geographic records
- Social media profiles and information
- Location-based services
- Web surfing behavior or user preferences using persistent cookies

The challenge for regulators is to frame mechanisms wherein it is possible to utilize data while simultaneously protecting an individual's privacy preferences and their personally identifiable

information. Hence, the laws and regulations related to Privacy and Data Protection are constantly changing, as lawmakers endeavor strict and diligent compliance with data privacy and security regulations.

**Regulatory Mechanism for Data Protection**

Data protection has emerged as an important reaction to the development of information technology. On August 11th 2023, the Indian Government enacted the Digital Personal Data Protection Act, 2023 (DPDP Act) by publishing it in the Official Gazette. The DPDP Act, when effective (as per dates to be notified), will govern the personal data processing activities of a broad range of organizations that operate in the Indian market.

The DPDP Act will replace the current data protection laws encapsulated under the Information Technology Act (IT Act) 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("SPDI Rules").

**Highlights of the Digital Personal Data Protection Act 2023**

Receiving Presidential assent on 11th August 2013 and being published in the Official Gazette of India on 12th August 2023, India's data protection law viz. The Digital Personal Data Protection Act 2023, came into force. Different dates may be appointed for the enforcement of the different provisions of this Act, thus notification of sections of the Act for implementation is awaited.

The following are some of the main highlights of the Act:

- The Act has been laid down to provide for the processing of digital personal data
- It will apply to the processing of digital personal data within India where such personal data is collected in digital form, or in non-digital form and digitized subsequently. It will also apply to processing of digital personal data outside India, if such processing is in connection with offering goods or services within India.
- It will not apply to personal data processed by individuals for any personal or domestic purpose and personal data that is publicly available
- The Act allows transfer of personal data outside India, except to countries restricted by the central government through notification.
- The Act introduces terms like Data Fiduciary, Data Principal, Data Processor, Data Protection Officer and defines the same.

- Data Fiduciaries, being persons who process data, have been mandated certain obligations w.re.to digital personal data in the Act and may process data in accordance with the provisions of the Act and that too for lawful purpose.
- Processing of personal data is permissible only for a lawful purpose and that too only after obtaining consent of the Data Principal or processing may be done for legitimate purposes.
- Data Principal, that is, the person to whom the personal data relates has certain rights and duties as laid down in the Act
- Data Protection Board of India will be established as the regulatory body to adjudicate on non-compliance with the provisions of the Act.
- Substantial financial penalties extending up to Rs.250 crores have been prescribed for breaches of provisions of this Act

**The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules, 2011 ("SPDI Rules")**

The rules provide guidelines for the collection, use and storage of sensitive personal data or information by body corporate. Section 43A of the IT Act 2000 provides for the right of individual regarding protection of sensitive personal data or information and also compensation to be paid to the affected users in case of unauthorized access of information and leakage of sensitive personal information. Section 72A of the IT Act 2000 provides for punishment for disclosure of information in breach of the lawful contract.

***Personal Information and Sensitive Personal Data or Information***

What constitutes as 'personal information' and 'sensitive personal data or information' is explained in the SPD Rules 2011. As per Rule 2(i), 'Personal information' means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. Rule 3 of the SPD Rules 2011, further states that sensitive personal data or information will comprise of information relating to various aspects like password; financial information; physical, physiological and mental health condition; sexual orientation; medical records and history; Biometric information etc. Information that is freely available or accessible

in public domain or furnished under the Right to Information Act, 2005 or any other law shall not be regarded as sensitive personal data or information.

***Privacy Policy***

Under Rule 4 of the SPD Rules 2011, the body corporate or any person who is acting on its behalf is under obligation to provide a policy for privacy and disclosure of information and publish such policy on its website. When the body corporate collects, receives, possess, stores, deals or handle information of provider of information, it shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract.

The Privacy Policy of the body corporate should provide information on the following matters —

(i) Clear and easily accessible statements of its practices and policies;

(ii) type of personal or sensitive personal data or information collected by it

(iii) purpose of collection and usage of such information;

(iv) rules for disclosure of information including sensitive personal data or information

(v) reasonable security practices and procedures

***Collection of Personal Data or Information***

The information collected from a person shall be used for the purpose for which it has been collected and the body corporate holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force (Rule 5(4) and 5(5) of SPD Rules 2011). It is also under obligation to keep the information secure.

The body corporate or any person on its behalf shall before collection of personal information, shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage. Additionally, while collecting such information it shall ensure that the person concerned is having the knowledge of the following:

(a) the fact that the information is being collected;

(b) the purpose for which the information is being collected;

(c) the intended recipients of the information; and

(d) the name and address of —(i) the agency that is collecting the information; and (ii) the agency that will retain the information

Under Rule 5(2) of the SPD Rules 2011, the body corporate is not allowed to collect sensitive personal data or information unless it complies with the following:

(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and

(b) the collection of the sensitive personal data or information is considered necessary for that purpose.

Prior to the collection of information including sensitive personal data or information, an option has to be given to the provider of the information that he need not provide the data or information which is sought to be collected and he may (in writing) while availing the services or otherwise, withdraw his consent given earlier.

A Grievance Officer shall be appointed by the body corporate (and his name and contact details shall be published on its website), to address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. The Grievance Officer shall redress the grievances within one month from the date of receipt of grievance.

***Disclosure of Sensitive Personal Data or Information***

Disclosure of sensitive personal data or information by body corporate to any third party (except Government Agencies mandated under the law) shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation. (Rule 6 of SPD Rules 2011)

The body corporate shall not publish the sensitive personal data or information and the third party receiving the sensitive personal data or information from body corporate, shall not disclose it further.

Under Rule 7 of the SPD Rules 2011, it is possible for the body corporate to transfer sensitive personal data or information to any other body corporate or person in India or another country

that ensures the same level of data protection that is adhered to by the body corporate itself. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

Under section 72A of the Information Technology Act, 2000, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract shall be liable to penalty which may extend to twenty-five lakh rupees. However, under sections 69 and 69A of the IT Act, 2000, the Government or any of its officer specially authorized by the Government, if satisfied that it is necessary or expedient so to do in the interest of sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, for reasons to be recorded in writing, by order, can direct any agency of the Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource and block for access to the public any information generated, transmitted, received, stored or hosted in any computer resource. Under section 69B the Central Government also has power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

***Security Practices and Procedures***

A body corporate shall implement security practices and standards (for e.g. like the international Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques - Information Security Management System - Requirements") which have a comprehensive documented information security programme and information security policy that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.

Any industry association or an entity formed by such an association, whose members are self-regulating and follow their own codes of practice for data protection rather than the IS/ISO/IEC codes of best practices for data protection, shall get its codes of best practices duly approved and notified by the Central Government for effective implementation. Whatever code out of the

above two is followed, such standard or codes of best practices should be certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government.

The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertakes significant upgradation of its process and computer resource. (Rule 8(4) of SPD Rules 2011)