Cybersecurity 2024

Last Updated August 19, 2024

India

Law and Practice

Law and Practice

Close All

1. Basic National Regime

1.1 Laws

The Constitution of India guarantees the right to privacy (including the right to data security) to all citizens as part of the right to life and personal liberty under Articles 19 and 21 and as part of the freedoms guaranteed by Part III of the Constitution. This was also upheld by the Supreme Court of India (SCI) in 2017 in its landmark judgment of Justice K S Puttaswamy (Retd) and Another v Union of India and Others (2017) 10 SCC 1 (the "Privacy Judgment").

The Indian government enacted the country's first comprehensive legislation on data privacy, The Digital Personal Data Protection Act, 2023 (DPDPA) in August 2023. This was based on an increased effort to provide a legislative framework for data protection and privacy laws. However, the DPDPA is expected to be implemented and enforced in 2024. The Rules under the DPDPA are still pending with the drafting committee, however, the stakeholders are preparing themselves for the new legislation as the DPDPA provides a principal-based framework for data protection compliances.

Until the DPDPA comes into force, cybersecurity, data breach notification and incident response are governed by the Information Technology Act, 2000 (ITA) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules).

The ITA defines "cybersecurity" as "protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction".

Under the ITA, the Indian government has established the Indian Computer Emergency Response Team (CERT-In) as the national nodal agency for cybersecurity, to carry out the following functions:

- collection, analysis and dissemination of information on cyber incidents;
- forecast and alerts of cybersecurity incidents;
- emergency measures for handling cybersecurity incidents;
- co-ordination of cyber incidents response activities;
- issue of guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents; and
- such other functions relating to cybersecurity as may be prescribed.

Law and Practice Authors

Anoop Narayanan (/author/details/22611043/QW5vb3AgTmFyY

Priyanka Gupta (/author/details/226110

ANA Law Group (https://chambers.com/law firm/ana-law-group-asia-pacific-8:226110 full-service law firm based in Mumbai, with team of experienced professionals who hav broad industry knowledge and specialisatio across a wide spectrum of business areas. firm has significant experience in counselli international clients on data privacy and cybersecurity law issues in India, and regul represents clients from various industries. firm works with global clients to implemen privacy programmes, create compliant proc products, and services. It also assists international companies with carrying out transfer impact assessments, drafting and negotiating contracts with Indian counterp and preparing privacy policies for internatic companies operating in India and their Indi subsidiaries. The firm routinely advises clie issues such as permitted data processing, consent requirements, data collection, rete and disclosure, regulatory requirement compliance, transfer of sensitive personal security breaches and drafting security bre policies, on international compliance proje and on prosecutions and offences.

Compare law and practice by selecting locations and topic(s)

Select Location(s)

Search

- Australia
- Belgium

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the "CERT-In Rules") prescribe that CERT-In will be responsible for responding to cybersecurity incidents and will assist cyber-users in the country in implementing measures to reduce the risk of cybersecurity incidents. CERT-In also has powers to issue directions to service providers, intermediaries, data centres, body corporates, etc, for enhancing cybersecurity infrastructure in the country.

The CERT-In Rules mandate CERT-In to operate an incident response help desk on a 24-hour basis, including government and other public holidays. Further, it is mandatory for the service providers, intermediaries, data centres and body corporates that handle sensitive personal data (SPD) to report all cybersecurity incidents to CERT-In "as early as possible". In April 2022, a new directive modified obligations under the 2013 Cert-In Rules, including requirements to report cybersecurity incidents within six hours, syncing system clocks to the time provided by government servers, maintaining security logs in India, and storing additional customer information. CERT-In has also set up sectoral CERTs to implement cybersecurity measures at a sectoral level. The details regarding the methods and formats for reporting cybersecurity accidents, vulnerability reporting and remediation, incident response procedures and dissemination of information on cybersecurity are published on CERT-In's website and are updated from time to time.

For critical sectors, the government has set up the National Critical Information Infrastructure Protection Centre (NCIIPC) under the ITA, as the nodal agency, and has framed the NCIIPC Rules and guidelines to protect the nation's critical information infrastructure (CII) from unauthorised access, modification, use, disclosure and disruption to ensure a safe, secure and resilient information infrastructure for critical sectors in the country.

Other relevant rules framed under the ITA include:

- The SPDI Rules, which prescribe reasonable security practices and procedures to be implemented for collection and the processing of personal or sensitive personal data;
- The Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018, which prescribe security measures for protected systems, as defined under the ITA. Under the ITA, the government may notify any computer resource that affects the facility of CII to be a "protected system"; and
- The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 require intermediaries to implement reasonable security practices and procedures to secure their computer resources and information, maintaining safe harbour protections. Intermediaries are also mandated to report cybersecurity incidents to CERT-In.

The Indian Penal Code 1860 currently deals in criminal offences, including those committed in cyberspace. However, the criminal laws in India are undergoing regulatory changes in line with the new age technologies. In particular, the Indian Penal Code 1860 will be changed to Bhartiya Nyaya Sanhita 2023 (BNS), the Code of Criminal Procedure 1973 will be changed to Bhartiya Nagarik Suraksha Sanhita 2023 and the Indian Evidence Act 1872 will be changed to Bhartiya Sakshya Adinyam 2023 (BSA). The changed provisions will be made effective from July 2024. Under the BNS, continued cyber-crimes and economic offences are referred to as "organised crime". The BSA specifies that electronic records will be considered as primary records, which calls for a strong foundation to be laid to protect the data online. The BNS prescribes forging false electronic documents as an offence and lays an

☐ Chile
☐ China
☐ Denmark
☐ Germany
☐ Hungary
☑ India
☐ Israel

Select Topic(s)

Search

Law and Practice

☑ 1. Basic National Regime
☐ 1.1 Laws
☐ 1.2 Regulators
☐ 1.3 Administration and Enforcement Process
☐ 1.4 Multilateral and Subnational Issues
☐ 1.5 Information Sharing Organisations and Government Cybersecurity Assistance

Reset (/practice-guides/comparison/970/12846/20344-20345-20346-20347-20348-20349-20350-20351-20352-20353-20354) Compare

imprisonment punishment of seven years and a fine. Additionally, the Companies Act 2013, requires the companies to implement security systems to ensure that electronic records are secured from unauthorised access.

The ITA prescribes that any service provider, intermediary, data centre, body corporate or person who fails to provide the information called for by CERT-In or comply with CERT-In's direction will be punishable with imprisonment for a term which may extend to one year or a fine which may extend to INR100,000 or both.

The ITA also prescribes deterrence in terms of compensations, penalties and punishments for offences such as damage to computer systems, failure to protect data, computer-related offences, theft of computer resource or device, SPD leak, identity theft, cheating by impersonation, violation of privacy, cyberterrorism, online pornography (including child pornography), breach of confidentiality and privacy, and breach of contract.

1.2 Regulators

In addition to the Ministry of Electronics and Information Technology (MeitY) and NCIIPC, the government has established the National Security Council Secretariat (NSCS) as the central coordinating body for cybersecurity and internet governance. NSCS has developed a draft cybersecurity strategy to address the issue of security of national cyberspace, the main aim is to improve the audit quality relating to cybersecurity to aid the organisations in conducting a better review of their cybersecurity knowledge and architecture. Currently, there is no implementation date for this strategy.

The Ministry of Home Affairs has set up the Cyber and Information Security Division (C&IS) to deal with matters relating to cybersecurity, cybercrime, the National Information Security Policy & Guidelines (NISPG) and its implementation. C&IS comprises of a cybercrime wing, a cybersecurity wing, an information security wing, and a monitoring unit.

Further, the Home Ministry has established the Indian Cybercrime Co-ordination Centre (I4C) which is a nodal point in the fight against cybercrime and co-ordinates implementation of mutual legal assistance treaties (MLAT) with other countries.

The government has also set up the National Technical Research Organisation (NTRO) as a technical intelligence agency under the National Security Advisor in the Prime Minister's office. Its primary role is to develop technology capabilities in aviation and remote sensing, data gathering and processing, cybersecurity, strategic hardware and strategic monitoring. NCIIPC comes within NTRO's ambit.

The ITA mandates the central government to appoint an adjudicating officer to conduct inquiries, and adjudicate matters (ie, contravention of any of the provisions of the ITA or any rule, regulation, direction or order made thereunder, including non-compliance of CERT-In's direction), with claims for injury or damages valued up to INR50 million. Claims that exceed this amount must be filed before the competent civil court. Where more than one adjudicating officer is appointed, the ITA mandates the central government to specify the matters and places of jurisdiction of each adjudicating officer.

The inquiry and investigation procedure for the adjudicating officer is provided under the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003. Any decision of the adjudicating officer can be appealed before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

Under the DPDPA, the Central Government has the power to establish the Data Protection Board of India (DPB). The DPB is the primary regulatory body responsible for enforcing the legislation. Data principals are required to comply with applicable laws while exercising their rights under the Act. Breach

of the duties by data principals may result in penalties of up to INR10,000 (USD120 approximately). The maximum penalty for violation of the DPDPA's provisions by a data fiduciary is INR2.5 billion, for failure to take reasonable security safeguards to prevent a personal data breach if the non-compliance is regarded as significant by the DPB.

The DPDPA also prescribes specific penalties of INR2 billion for failure to notify the DPB and affected data principals of data breaches; and non-compliance with additional obligations while processing children's data.

Under the DPDPA, the TDSAT established under section 14 of the Telecom Regulatory Authority of India Act, 1997 adjudicates on appeals from the orders of the DPB, and the SCI is the final appellate authority for all purposes under the DPDPA.

There are various sector-specific regulators engaged in supervising their relevant intermediaries on the progress of implementation and robustness of cybersecurity frameworks. They regularly conduct cybersecurity and system audits of the intermediaries, which are reported to the relevant regulators.

Sector-Specific Regulators

Banking sector

The Reserve Bank of India (RBI) governs both public and private sector banks. The RBI's guidelines prescribe that the RBI can request an inspection at any time of any of the banks' cyber-resilience. The RBI has set up a Cyber Security and Information Technology Examination (CSITE) cell under the Department of Banking Supervision, to periodically assess the progress made by banks in the implementation of the cybersecurity framework (CSF), and other regulatory instructions and advisories through on-site examinations and off-site submissions. The RBI has an internal ombudsman scheme for commercial banks with more than ten branches as a redressal forum, and has also issued guidelines on information security, electronic banking, technology risk management and cyber frauds. CERT-In and the RBI jointly carry out a cybersecurity awareness campaign on "Beware and be aware of financial frauds" through the Digital India Platform.

RBI also issued Guidelines on Regulation of Payment Aggregators and Payment Gateways, directing payment aggregators to put in place adequate information, data security infrastructure and systems for prevention and detection of frauds, and has specifically recommended implementation of data security standards and best practices such as PCI-DSS, PA-DSS, the latest encryption standards and transport channel security. Payment aggregators must establish a mechanism for monitoring, handling and follow-up of cybersecurity incidents and breaches, and mandatorily report incidents to RBI and CERT-In.

RBI regularly conducts audits and inquiries into banks' security frameworks and imposes penalties on the banks for non-compliance with RBI's cybersecurity framework. RBI has also formulated an integrated scheme, The Reserve Bank – Integrated Ombudsman Scheme, 2021 (the "RB-IOS, 2021") to simplify the grievance redress process at RBI by enabling the customers of all regulated entities to register their complaints at one centralised reference point. Through this portal, RBI also spreads cyber-crime awareness including frauds using mobile apps/UPI/QR codes, etc.

Recently, in November 2023, the RBI issued the Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices which addresses the Regulated Entities (REs) as defined in the directions, to put in place a a Cyber Security Policy and Cyber Crisis Management Plan (CCMP). Under the directions of the Information Security Committee (ISC) under the supervision by the ITSC (Board-level IT Strategy Committee) for the management of cyber/information security. Some of the ISC's responsibilities include the development of information/cybersecurity policies and reviewing

cyber incidents. The direction lays the onus on the REs to tackle cyber attacks, which include spoofing and phishing, so that their adverse effects are mitigated. The Master Direction came into effect on 1 April 2024.

Insurance sector

The Insurance Regulatory and Development Authority (IRDA) is the nodal agency for governance and regulation of the insurance sector in India. The IRDA conducts regular on-site and off-site inspections of insurers to ensure compliance with the legal and regulatory framework. The IRDA also has guidelines on Information and Cyber Security for Insurers (IRDA Cyber Security Policy), requiring vulnerability assessment and penetration testing annually and closing any identified gaps within a month. Some other relevant guidelines issued by IRDA are: IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017; IRDAI (Maintenance of Insurance Records) Regulations, 2015; and the IRDAI (Protection of Policyholders' Interests) Regulations, 2017, which contain a number of provisions and regulations on data security. Additionally, IRDAI has recently issued guidelines to insurers on structuring cyber-insurance for individuals and identifying gaps that need to be filled. As per the guidelines, cyber-insurance should provide cover against theft of funds and identity, unauthorised online transactions, email spoofing, etc.

Telecom sector

Telecom operators in India are governed by regulations laid down by the following regulatory bodies:

- the Telecom Regulatory Authority of India (TRAI);
- the Department of Telecom (DoT);
- the TDSAT;
- the Group on Telecom and IT (GOTIT);
- the Wireless Planning Commission (WPC); and
- the Digital Communications Commission (DCC).

Further, the Unified Access Service Licence (UASL) extends information security to the telecom networks as well as to third-party operators. The regulator requires telecom operators to audit their network (internal/external) at least once a year.

TRAI has released its recommendations on cloud services in relation to creation of a regulatory framework for cloud services, and constituting an industry-led body of all cloud service providers (CSP).

DoT regularly conducts cybersecurity workshops and cyber drills for better awareness.

Securities

The Securities Exchange Board of India (SEBI) was established in 1988 and is the regulatory body for commodity and security markets in India. SEBI keeps in check the interest of investors, and market intermediaries and ensures that the issuers of securities are protected, including safeguarding their customer data, data, and transactions.

In April 2022, SEBI appointed six committee members to overlook the guidance regarding the cybersecurity initiatives for the Indian economy and advise SEBI to maintain and develop cybersecurity requirements keeping in mind the global industry standards.

SEBI has issued detailed guidelines to market infrastructure institutions (MIIs) to set up their respective Cyber Security Operation Centre (C-SOC) and to oversee their operations through dedicated security analysts. The cyber-resilience framework also extends to stockbrokers and depository participants.

SEBI works and communicates along with agencies such as the National Cyber Cyber Coordination Centre (NCSC), CERT-In, MeitY, and DoT.Health sector

The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (IMCR) impose patient confidentiality obligations on medical practitioners. The Ministry of Health and Family Welfare introduced draft legislation in 2017, known as the Digital Information Security in Healthcare Act (the "DISH Act"), to regulate the generation, collection, storage, transmission, access and use of all digital health data. The DISH Act also provides for the establishment of a National Digital Health Authority as the statutory body to enforce privacy and security measures for health data, and to regulate storage and exchange of health records.

The expert committee report and the DPDPA prescribe central government appoint the DPB to ensure compliance with the data protection laws, register data fiduciaries, conduct inquiries and adjudication of privacy complaints, issue codes of practice, monitor cross-border transfer of personal data, advise state authorities and promote awareness on data protection.

The DPDPA prescribes that the data fiduciary should appoint a Data Protection Officer who shall report to the Board of Directors or a similar governing body, and be the point of contact for the grievance redressal mechanism.

The Ministry of Health and Family Welfare had approved a Health Data Management Policy (the "HDM Policy") largely based on the DPDPA to govern data in the National Digital Health Ecosystem. The HDM Policy recognises entities such as data fiduciaries and data processors similar to the DPDPA, and establishes a consent-based data-sharing framework.

Under the DPDPA, health data can be processed by the data fiduciary as legitimate use, in case there is a medical emergency that involves a threat to life or an immediate threat to the health of a data principal or any other person or in there is a situation like an epidemic, an outbreak of a disease, or any other threat to public health.

1.3 Administration and Enforcement Process

The ITA provides for the appointment of an adjudicating officer to deal with claims of injury or damages not exceeding INR50 million. Claims exceeding this amount must be filed before the competent civil court. MeitY has appointed the Secretary of the Department of Information Technology of each Indian state or union territory as the adjudicating officer under the ITA.

A written complaint can be made to the adjudicating officer based on the location of the computer system or the computer network, together with a fee based on the damages claimed as compensation. The adjudicating officer thereafter issues a notice to the parties notifying the date and time for further proceedings and, based on the parties' evidence, decides whether to pass orders (if the respondent pleads guilty) or to carry out an investigation. If the officer is convinced that the scope of the case extends to the offence instead of contravention, and entails punishment greater than a mere financial penalty, the officer will transfer the case to the magistrate having jurisdiction.

The first appeal from the adjudicating officer's decisions can be filed before the TDSAT, and the subsequent appeal before the High Court.

The DPDPA prescribes filing the complaint by the data principal before the DPB after the data principal has exhausted all means of redressal related to approaching the data fiduciary or the consent manager. The DPB will have the authority to impose penalties on the data fiduciary.

The maximum penalty for violation of the DPDPA's provisions by an individual is INR2.5 billion, for failure to take reasonable security safeguards to prevent a personal data breach if the non-compliance is regarded as significant by the

DPB. The DPDPA also prescribes specific penalties of INR2 billion for failure to notify the DPB and affected data principals of data breaches, and non-compliance with additional obligations when it comes to the processing of personal data of children. The penalty for breach of additional obligations on behalf of a significant data fiduciary is INR1.5 billion. The penalty for breach of duties of data principal is INR10,000. Lastly the penalty for contravention of any other provision of the DPDPA is INR500 million.

The DPDPA prescribes that the central government establish an appellate tribunal, TDSAT adjudicate on appeals from the orders of the DPB, and the SCI act as the final appellate authority for all purposes under the DPDPA.

Further, if the DPB believes that the complaint filed can be resolved by mediation, it can direct the parties to appoint a mediator through mutual agreement and to resort to mediation as a form of alternate dispute resolution.

The DPDPA also provides for a voluntary undertaking from a person. The DPB may accept the voluntary undertaking outlining such action that will be taken by the Data Fiduciary within such time as prescribed. The DPB, after varying the terms of the undertaking, with due consent of the person, shall put a bar on the proceedings as per the DPDPA.

The DPDPA also requires a valid contract when data processing is being carried out by the data processor on behalf of the data fiduciary.

However, if there is a failure to comply with the terms of the undertaking, such non-compliance will be treated as a breach as per the provisions of DPDPA, and such person shall be liable to pay a monetary penalty for the breach as per the DPDPA, after being given an opportunity to be heard.

Regarding cybersecurity and critical sectors, see **1.1 Laws** and **1.2 Regulators**.

1.4 Multilateral and Subnational Issues

India does not have state-specific cybersecurity laws or regulations. However, several state governments have taken initiatives to promote cybersecurity. For example, the Maharashtra state government launched the Cyber Safe Initiative to spread awareness regarding laws on cybercrime, bank fraud, child pornography, online gaming, cyber defamation, false information sites, etc. Further, the Karnataka government established a Centre of Excellence in Cyber Security to build awareness and facilitate innovation, standardisation, and best practices for cybersecurity.

1.5 Information Sharing Organisations and Government Cybersecurity Assistance

The following non-governmental authorities assist the Indian government in cybersecurity measures:

- the Data Security Council of India (DSCI) – a not-for-profit industry body under the National Association of Software and Services Companies (NASSCOM) that engages with governments and their agencies, regulators, industry sectors, industry associations and think tanks for policy advocacy, thought leadership, capacity-building and outreach activities;
- National Cyber Safety and Security Standards (NCSSS) – a self-governing body to protect the CII from cyber-related issues;
- the Internet and Mobile Association of India (IAMAI) – a not-for-profit industry body that addresses the issues, concerns and challenges of the Internet and mobile economy;
- the Cellular Operators Association of India (COAI) – an industry association of mobile service providers, telecom equipment, internet and broadband service providers in India, which interacts directly with ministries, policy-makers, regulators, financial institutions and technical bodies;
- the Internet Service Providers Association of India (ISPAI) – the recognised apex body of Indian ISPs worldwide; and

- the Computer Society of India (CSI) – a non-governmental organisation of professionals (software developers, scientists, academics, project managers, etc) who contribute to the government's formulation of information technology strategy and planning.

A formal memorandum of understanding (MoU) has been signed between the Central Board of Direct Taxes (CBDT) and SEBI for data exchange between the two organisations, on an automatic and regular basis. SEBI and CBDT will also exchange any information available in their respective databases, to carry out their functions under various laws.

In regard to government assistance, under the Digital India initiative, MeitY had set up the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre), operated by CERT-In, to work with internet service providers and companies to provide information and tools to users on botnet and malware threats. Similar proactive measures are deployed by sector-specific regulators from time to time.

Also, MeitY released the National Cyber Security Policy in 2013, which recommended creating a secure cyber-ecosystem, strengthening laws, and creating mechanisms for the early warning of security threats, vulnerability management and the response to security threats. The policy intended to encourage all organisations to develop information security policies integrated with their business plans and implement the policies following international best practices. This policy is expected to be updated soon.

Finally, in a one of its kind public-private partnership, MeitY launched Cyber Surakshit Bharat, a mission to strengthen the cybersecurity ecosystem in India by spreading awareness about cybercrime and undertake capacity-building for chief information security officers (CISOs) and staff across all government departments. This initiative was founded by the IT giants Microsoft, Intel, WIPRO, Redhat and Dimension Data, in alliance with CERT-In, the National Informatics Centre (NIC), NASSCOM and the FIDO Alliance, and consultancy firms Deloitte and EY.

1.6 System Characteristics

Similar to world CERTs, Cert-In is the national nodal agency for responding to computer security incidents as and when they occur. CERT-In operates on similar principles as other CERTs, such as:

- collection, analysis and dissemination of information on cyber incidents;
- forecast and alerts of cybersecurity incidents;
- emergency measures for handling cybersecurity incidents;
- co-ordination of cyber incident response activities; and
- issue of guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents; and
- such other functions relating to cybersecurity as may be prescribed.

Regarding cybersecurity incidents and critical sectors in India, please see **1.1 Laws** and **1.2 Regulators**.

The Indian cybersecurity laws follow the UK cybersecurity model. For example, the primary institutional authorities for critical information infrastructure (CII) in both jurisdictions are similar, such as the CIIPC in India and the National Cyber Security Centre in the UK. India and the UK also have similar emergency response authorities, such as CERT-In and CERT-UK.

Additionally, the UK has a central authority, the National Cyber Security Centre, that co-ordinates between the UK government and its various industry stakeholders in cybersecurity matters. The MeitY is in the process of establishing a similar authority in India, known as the National Cyber Coordination Centre (NCCC), which will be implemented by CERT-In.

However, there are certain fundamental dissimilarities in the cybersecurity regimes of India and the UK. For instance, the UK does not have a comprehensive legal framework in respect of information technology and cybersecurity, whereas India has comprehensive legislation to govern information technology and cybersecurity (the ITA). Also, in the absence of an all-inclusive cybersecurity framework, the various executive authorities in the UK function under separate laws (the Security Services Act 1989, or the Civil Contingencies Act 2004). Conversely, the central authorities for cybersecurity in India are established and operationalised under the ITA, and the various rules thereunder.

In regard to the CII, the guidelines for the protection of the national critical information infrastructure provide for security certifications by third-party agencies (government or private agencies) to protect the assets for smooth and error-free operation. The certifications must also deal with enforcing or implementing any international security standards available globally for the protection of critical assets working in the CII by respective organisations. Each CII must list the certifications needed to be implemented for the protection of their assets and the areas.

As the recent attacks on cyber infrastructure indicate increasing targeting of SCADA systems and supporting infrastructure widely used in almost all critical industrial set-ups (oil, gas, nuclear, aviation, etc), there is an increased need to implement the strategic controls recommended in the guidelines.

1.7 Key Developments

MeitY introduced a draft Bill, the DPDP Bill, on 18 November 2022, which adopts a more simplified approach to handling “personal data” in comparison to the previous versions, which were published for public consultation. The gazetted DPDPA was based on the 2022 Bill but with certain new provisions. The DPDPA allowed for the processing of personal data either collected online or offline but later digitised. The DPDPA is also applicable to data that would be processed outside India, in respect of the goods and services offered within India.

Under the DPDPA, data principal is given a broader meaning. It includes both persons with disabilities and represented by their lawful guardian. The DPDPA specifies that consent should be specific, free, unconditional, unambiguous, and informed. Withdrawal of consent should also be permitted. The Consent Manager should be managing the data principals. The scope of processing the data should be “wholly or partly” which allows for processing to be completely automated or includes a combination of manual and automated operations. However, as the DPDPA is yet to be notified by the Central Government the stakeholders have asked the MeitY to grant 12 to 24-month period so they can comply with the provisions of the DPDPA.

On 5 March 2024, MeitY released a notification for project proposals for Research & Development in Cyber Security where a proposal could be submitted by research professionals/scientists/ engineers/ academicians highlighting technology developments and prototype models on brief areas such as:

- recovery of deleted or overwritten data,
- preserving privacy and digital forensic investigations,
- Privacy and accidental leakage prevention and,
- Next-generation hashing, encryption and applications in network security and Zero Trust, Privacy and security in cloud and networks.

On 20 March 2024, MeitY’s notification confirmed that a Fact Check Unit has been notified by the Central Government under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which governs privacy policies published by the intermediaries.

On 12 February 2024, MeitY notified a cyber security roadmap that suggests work on dark web forensics, social media analytics tools, deepfake detection tools, and real-time fraud detection tools in the next five years.

The February 2024 IoT Security roadmap suggested that in the next five years, AI-enabled privacy and data protection systems would be introduced.

In April 2022, CERT-In issued a new directive modifying obligations under the 2013 Cert-In Rules, including requirements to report cybersecurity incidents within six hours, syncing system clocks to the time provided by government servers, maintaining security logs in India, and storing additional customer information. This is applicable to all service providers, intermediaries, data centres, body corporate, virtual private server (VPS) providers, cloud service providers, VPN service providers, virtual asset service providers, virtual asset exchange providers, custodian wallet providers and government organisations. Individual citizens are not covered by these directions.

MeitY notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022 replacing the Information Technology (Intermediaries guidelines) Rules, 2021. The amendments have come into effect immediately, and have introduced significant obligations on intermediary platforms including prompt resolution of grievances, and acting as a protector of fundamental rights. It also provides for the constitution of the Grievance Appellate Committees to address appeals from decisions of an intermediary's Grievance Officer.

In October 2022, IRDAI introduced an improved cybersecurity framework focused on the insurers' security concerns, which aims to encourage insurance firms to establish and maintain a robust risk assessment plan, improve mitigation methods of internal and external threats, prevent ransomware attacks and other types of fraud, and implement a strong and robust business continuity.

RBI through a notification has mandated that no entity in the card transaction/payment chain, other than the card issuers and/or card networks, shall store Card-on-File (CoF) data, and any such data stored previously shall be purged.

The Department of Science and Technology issued guidelines for acquiring and producing geospatial data and geospatial data services including maps. Under these guidelines, there is no restriction, and no requirement of any approval, clearance, license, etc, on the collection, generation, preparation, dissemination, storage, publication, updating and/or digitisation of geospatial data and maps within the territory of India, subject to certain restrictions. The guidelines also restrict foreign entities from creating and/or owning, or hosting geospatial data other than the prescribed threshold values.

The Bureau of Indian Standards issued standards for data privacy assurance, the IS 17428. The standard seeks to provide a privacy assurance framework for organisations to establish, implement, maintain and continually improve their data privacy management system.

The Competition Commission of India (CCI), India's antitrust regulator, initiated an investigation against WhatsApp, Inc. and Facebook, Inc. (now Meta Platforms, Inc.) assessing the impact of WhatsApp's update requiring the users to agree to data sharing with Facebook to continue using the WhatsApp. CCI noted that WhatsApp's unilateral terms violated the users' voluntary agreement and appeared to be unfair and unreasonable for its users. Meta and WhatsApp filed petitions before the Delhi High Court and, thereafter, in the Supreme Court requesting that CCI's proceedings and the final order must be halted, but the Supreme Court dismissed these petitions in October 2022.

1.8 Significant Pending Changes, Hot Topics and Issues

The Indian government is working towards updating its National Cybersecurity

Strategy in order to improve its position in cyberspace. The updated National Cybersecurity Policy may be issued this year.

The validity of the Cert-In Directions has been challenged by several entities across Indian courts alleging that certain provisions of the Cert-In Directions are ultra vires. Reportedly, one of the provisions challenged includes collection of details like name, IP address, address, contact information, and the purpose of using VPN and keeping it for five years even after the user's relationship with the VPN service provider has ended. Although the Cert-In Directions are currently in force, the court's approach on the pending cases will be noteworthy.

India continued to witness a tremendous increase in cybercrime and data breach incidents in 2022. India's cyber-attacks on government agencies rose, more than doubling to 13.7% in 2022 from 6.3% in 2021, which is reportedly attributed to significant increase in "hacktivist" activity. Cert-In witnessed more than 1 million cyber-attacks reported in India by November 2022. AIIMS, widely regarded as India's foremost government hospital, was hit by a ransomware attack on 23 November 2022. The incident marked one of the most high-profile data breaches targeting a government-backed entity in the country, compromising the records of nearly 30–40 million patients including high-profile political personalities.

Further, Oil India Limited's headquarters witnessed a massive ransomware attack which led to the shutting down of its computer and IT systems. The attackers had demanded a USD7.5 million ransom. Also, the New CapraRAT Android Malware targeted the Indian government and military personnel. This exponential rise may deepen concerns about potential cybersecurity risks as well as new kinds of data security breaches.

The government will soon be releasing the draft e-commerce policy that proposes to set up an e-commerce regulator with broad powers over e-commerce entities and platforms. The draft policy contains proposals on sharing source codes, algorithms and other data with the government, use of non-personal data of consumers, anti-piracy, cross-border data transfers, etc. This is an important development and it will be interesting to monitor the final policy in view of the provisions under the pending DPDP Bill, and, thereafter, the policy's feasibility and enforceability.

The Jan Vishwas (Amendment of Provisions) Bill 2023 was received the President's assent in August 2023. It will come into effect as soon as the Central Government notifies it in the official gazette. The provisions that have been amended are Sections 33, 44, 67 C, 68, 69 B, 70 B, 72, and 72A of the ITA. Under Section 69B, the intermediaries not providing the government with technical assistance are now liable for an imprisonment for one year with an INR10 million maximum fine. Similarly, the above amended provisions either reduce or remove the imprisonment and increase the fine amount instead.

Also, the penalty under Section 70B was increased to INR10 million, which is a hundred times the previous amount of INR100,000, and a maximum imprisonment for up to one year.

2. Key Laws and Regulators at National and Subnational Levels

2.1 Key Laws

The ITA and the IT rules are applicable for the protection of data, computer systems and infrastructures in India until the DPDPA is notified. The ITA protects data, which is defined as "a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer

network, and may be in any form (including computer print-outs, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer".

The ITA protects data and computer systems, including computers, computer resources and computer networks from unauthorised access, downloads, and extraction of data, database and information, computer contaminant or virus, damage, disruption, denial of access by authorised persons, theft, concealment, destruction and alteration of computer source code, etc. The ITA also provides compensations, penalties and punishments in respect of offences related to the aforesaid activities.

The SPDI Rules prescribe protection of personal information and SPD. The SPDI Rules define personal information as "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". Further, the SPDI Rules recognise the following as SPD:

- password;
- financial information, such as bank account, credit card or debit card, or other payment instrument details;
- physical, physiological and mental health condition;
- sexual orientation;
- medical records and history;
- biometric information;
- any detail relating to the above as provided to a body corporate for providing service; and
- any of the information received from a body corporate in respect of the above, for processing, stored or processed under lawful contract or otherwise.

The DPDPA

Under the DPDPA, the processing of personal data can only happen by way of consent of the data principal. A notice must be provided to the data principal before seeking consent. The notice should contain details about the personal data to be collected, the purpose of processing, as well as how the data principal may withdraw its consent, avail the grievance redressal mechanism, and make a complaint to the DPB.

The DPDPA prescribes that the consent obtained from the data principal must be free, specific, informed, unconditional, and unambiguous with clear affirmative action, and shall signify an agreement to the processing of the subject's personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose

Consent need not be sought for legitimate uses which include processing for:

specified purposes for which the data principal has voluntarily shared personal information without objecting to such processing;

- for purposes of employment;
- for responding to medical emergencies;
- for performing any function under law or the State providing any service or benefit to the data principal;
- for compliance with any judgment or order issued under any law; and
- for taking measures to ensure safety during breakdown of public order, etc.

The CERT-In Rules require mandatory reporting of all cybersecurity incidents to the CERT-In at the earliest and in a prescribed format. Cert-In's new directive mandates the reporting of a cybersecurity incident within six hours. The CERT-In is the central authority for reporting cyber incidents, analysing

trends and patterns in intruder activities, determining the scope, priority and threat of a cyber incident and developing preventive strategies against cybersecurity incidents.

The ITA, the NCIIPC Rules and guidelines prescribe protection of India's CII from unauthorised access, modification, use, disclosure and disruption, and ensure a safe, secure and resilient information infrastructure for critical sectors. The NCIIPC, as the nodal agency under the NCIIPC Rules, essentially protects and delivers advices aimed at reducing vulnerabilities of CII against cyberterrorism, cyberwarfare and other threats.

The National Cyber Security Policy, 2013 aims to create a cybersecurity framework, leading to specific actions and programmes to enhance the security posture of India's cyberspace. The Cyber Security Policy prescribes various objectives, which include the following:

- to create a secure cyber-ecosystem in the country, generate adequate trust and confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy;
- to create an assurance framework for the design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology and people);
- to strengthen the regulatory framework for ensuring a secure cyberspace ecosystem;
- to enhance and create national and sectoral level 24x7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions;
- to enhance the protection and resilience of the CII by operating NCIIPC, and mandating security practices related to the design, acquisition, development, use and operation of information resources;
- to enable protection of information while in process, handling, storage and transit so as to safeguard privacy of citizens' data and for reducing economic losses due to cybercrime or data theft; and
- to enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

The government is working towards updating its National Cybersecurity Strategy in order to improve its position in cyberspace.

The Payment and Settlement Systems Act, 2007, mandates all information received by the RBI from a payment system and system provider to be confidential, subject to certain safeguarding interests, such as protection of:

- the integrity, effectiveness and security of the payment system;
- the interest of banking or monetary policy;
- the operation of the payment systems generally; or
- in the public interest.

The Companies (Management and Administration) Rules, 2014, mandate adequate cybersecurity in respect of an electronic voting system, which is used by members of a company to exercise their right to vote at general meetings.

2.2 Regulators

As India currently does not have a specific DPB, cybersecurity issues are adjudicated by an adjudicating officer appointed under the ITA, having the powers of a civil court.

2.3 Over-Arching Cybersecurity Agency

At present, there is no over-arching cybersecurity agency for India similar to ENISA. However, in addition to Cert-In and NCIIPC, the government has established the National Security Council Secretariat as the central co-ordinating body for cybersecurity and internet governance.

As part of the government's Digital India (https://digitalindia.gov.in/) initiative, MeitY has set up Cyber Swachhta Kendra as a botnet cleaning and malware analysis centre. The Ministry of Home Affairs has set up a Cyber and Information Security Division (C&IS) to deal with matters relating to cybersecurity, cybercrime, National Information Security Policy & Guidelines (NISPG) and its implementation. C&IS comprises of a cybercrime wing, cybersecurity wing, information security wing, and a monitoring unit.

Further, the Home Ministry has established the Indian Cybercrime Co-ordination Centre (I4C), which is a nodal point in the fight against cybercrime and co-ordinates implementation of Mutual Legal Assistance Treaties (MLAT) with other countries. The government has also set up the National Technical Research Organisation (NTRO) as a technical intelligence agency under the National Security Advisor in the Prime Minister's office. The primary role is to develop technology capabilities in aviation and remote sensing, data gathering and processing cybersecurity, strategic hardware and strategic monitoring. NCIIPC comes within NTRO's ambit.

The Ministry of External Affairs has set up a New Emerging and Strategic Technologies Division (NEST) to engage in technology diplomacy and deal with the foreign policy and international legal aspects of new and emerging technologies.

2.4 Data Protection Authorities or Privacy Regulators

The DPB is the central data privacy authority as per the provisions of the DPDPA. The DPB is currently in the process of being set up. The DPDPA specifies that before a matter reaches the Data Protection Officer (DPO), it should be heard by the data fiduciary or the consent manager. A consent manger is a person who is registered with the DPB and serves as a point of contact for the data principal. If the individual is aggrieved by the decision of the DPO, then he/she can approach the appellate tribunal for appeal.

The maximum penalty for violation of the DPDPA's provisions by an individual is INR2.5 billion, for failure to take reasonable security safeguards to prevent the personal data breach if the non-compliance is regarded as significant by the DPB. The DPDPA also prescribes specific penalties of INR2 billion for the failure to notify the DPB and affected data principals of data breaches; as well as non-compliance with additional obligations while processing children's data. The penalty for the breach of additional obligations on behalf of a significant data fiduciary is INR1.5 billion. The penalty for breach of the duties of a data principal is INR10,000, and the penalty for any other provision of the DPDPA is INR500million.

2.5 Financial or Other Sectoral Regulators

The RBI is the nodal banking and financial sector regulator in India. The sub-CERT for the banking and finance sector is the Institute for Development and Research in Banking Technology (IDRBT), which is an autonomous centre for development and research in banking technology set up by the RBI. The IDRBT owns the Indian Financial Network (INFINET), which is the communication backbone for the banking and finance sector in India.

The RBI's Regulations, and Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds (the "RBI Cyber Security Guidelines") provide detailed guidance on information technology governance for banks in India. The RBI has also issued guidelines on CSF in

banks, prescribing banking companies to have an adaptive incident response, management and recovery framework to deal with adverse incidents and disruptions.

The Information Technology Framework for the NBFC Sector was set up in 2017, focusing on IT policy, IT governance information and cybersecurity.

The Finance Minister has proposed to establish a CERT-Fin, which will act as an umbrella CERT for the finance sector. The RBI will be the lead regulator, until such CERT-Fin is set up.

SEBI has also issued guidelines on Cyber Security and Cyber Resilience for Stock Exchanges, Clearing Corporation and Depositories. Further, the IRDA has issued guidelines on Information and Cyber Security for Insurers, for cybersecurity protection of information in relation to policyholders.

NITI Aayog (the government's policy think-tank) released a draft framework on Data Empowerment and Protection Architecture (DEPA) in consultation with industry regulators, banks and fintech entities, to set up a mechanism for secure consent-based data sharing in the fintech sector. This would empower individuals with control over their personal data. Individuals will be able to share their financial data across banks, insurers, lenders, mutual fund houses, investors, tax collectors, and pension funds in a secure manner. DEPA is also proposed to be introduced for other sectors, such as the health and telecom sectors.

In the insurance sector, IRDI has issued the Guidelines on Information and Cyber Security for Insurers (the "Insurance Cyber Guidelines") under which the insurers must put in place adequate measures to ensure that cybersecurity issues are addressed. Insurers are also mandated to appoint a chief information security officer (CISO), formulate a cyber crisis management plan and conduct audits. In the telecommunications sector, the Department of Telecommunication (DOT) has prescribed the licence conditions and cybersecurity obligations on the licensee entity under the unified licence.

2.6 Other Relevant Regulators and Agencies

There are CERTs established under the Ministry of Power to mitigate cybersecurity threats in power systems, and four sub-CERTs for transmission, thermal, hydro and distribution to coordinate with power utilities. The amended Intermediaries Guidelines of 2022 under the ITA impose various obligations on the intermediaries including reporting cyber incidents to the CERT-In.

3. Key Frameworks

3.1 De Jure or De Facto Standards

The SPDI Rules prescribe reasonable security practices that should be supplemented by documented information security programmes and policies. One such security standard prescribed is the International Standard on Information Technology Security Techniques and Information Security Management System Requirements, such as the ISO 27001, and the use of codes of best practices created by self-regulatory bodies. Sectoral regulators and nodal agencies also prescribe security measures. RBI has prescribed baseline cybersecurity and resilience requirements for banks, in sync with global security standards. It also mandates banks to follow the ISO/IEC 27001 and ISO/IEC 27002 standards. A similar framework is applicable to non-banking finance companies. SEBI requires stock exchanges, depositories and clearing corporations to follow standards such as ISO/IEC 27001, ISO/IEC 27002 and COBIT 5.

3.2 Consensus or Commonly Applied Framework

There is no consensus or commonly applied framework for reasonable security, and the regulators have recommended a sector-wise framework based on various factors, including risk-based elements. CERT-In operates on the aspects of “identifying” the cybersecurity risks and the incidents, “containment” of the cyber breach incident and minimising damage, “eradication” of the cause of incident and “recovery” to restore normal operations. Under the ITA, reasonable security practices and procedures include the security practices that are designed to protect any information from unauthorised access, damage, use, modification, disclosure or impairment, and are specified in a contractual agreement, or any law or as prescribed by the central government.

The SPDI Rules prescribe the following criteria to comply with the “reasonable security” practices and procedures:

- entities must implement the security practices and standards; and
- there must be a comprehensive documented information security programme and policies, containing managerial, technical, operational and physical security control measures, that are commensurate with the information assets being protected and the nature of business.

3.3 Legal Requirements and Specific Required Security Practices

Written Information Security Plans or Programmes

The SPDI Rules prescribe that corporate bodies have a comprehensive documented information security programme and security policies containing managerial, technical, operational and physical security measures.

Incident Response Plans

There is no statutory requirement under the cybersecurity laws to maintain an incident response plan. The Protected System Rules prescribe that central and state governments implement a cyber crisis management plan for rapid identification, information exchange, swift response, and remedial actions to recover from malicious cyber-related incidents in the critical sectors.

The RBI requires banks to have a written incident response programme and cybersecurity policy to handle cyberthreats, and a cyber crisis management plan addressing detection, response, recovery and containment. The RBI requires mandatory reporting of cyber breach incidents within two to six hours of the incident. The IRDA requires insurers to have an incident response plan.

Appointment of Chief Information Security Officer or Equivalent

The NCIIPC guidelines recommend that all CIIs have an information security department headed by a CISO. The RBI’s Cyber Security Guidelines mandate the appointment of a chief information security officer (CISO), along with a security steering committee in public/private sector banks, who must report any incident directly to the bank’s head of risk management. The IRDA also requires the appointment of a CISO to implement a cybersecurity framework. The SPDI Rules provide for the appointment of a grievance officer to redress the information provider’s grievances. Cert-In’s new directives require the service providers, intermediaries, data centres, corporate bodies and government organisations to designate a “Point of Contact” to interface with CERT-In.

Involvement of Board of Directors or Equivalent

The RBI and IRDA guidelines require the involvement of the board of directors to approve cybersecurity policies and cyber crisis management plans and take overall responsibility for the information security governance framework.

Conducting Internal Risk Assessments, Vulnerability Scanning, Penetration Tests

The SPDI Rules do not prescribe conducting internal risk assessments,

vulnerability scanning, penetration tests, etc. The RBI mandates banks to have periodical vulnerability assessment and penetration testing exercises for all critical systems. The IRDA also has a cybersecurity policy that recognises the need for testing programmes, vulnerability assessments and penetration tests.

For instance, in October 2022, IRDAI introduced an improved cybersecurity framework focused on the insurers' security concerns, which aims to encourage insurance firms to establish and maintain a robust risk assessment plan, improve mitigation methods of internal and external threats, prevent ransomware attacks and other types of fraud, and implement robust business continuity.

Further, the DPDPA requires the significant fiduciaries to undertake measures including data protection impact assessment and periodic audits. The "Data Protection Impact Assessment" is defined as a process comprising description, purpose, assessment of harm, measures for managing the risk of harm, and such other matters concerning the processing of personal data, as may be prescribed. Unlike the previous versions, this law does not provide any details on how to carry out the assessment, which would be notified by the government in due course.

Multi-factor Authentication, Anti-phishing Measures, Ransomware, Threat Intelligence

The RBI has issued guidelines for banks to implement two-factor/multi-factor authentication to protect the customer account data and transaction details' confidentiality, and to combat cyber-attacks by phishing, keylogging (ie, keyboard capturing or the action of recording the keys struck on a keyboard), spyware/malware, etc, that are targeted at banks and their customers.

Besides this, organisations such as DSCI issue periodic advisories on data breaches, recommendations to avoid data breaches, and strengthening security measures. For instance, DSCI issued guidance on Targeted Phishing Campaign by Malicious Actors, anticipating a large-scale phishing attack against Indian organisations, targeting small, medium and large enterprises. DSCI also provided information on mitigation measures.

Insider Threat Programmes

There are no insider threat programmes or standards under the current Indian cybersecurity framework.

Vendor and Service Provider Due Diligence, Oversight and Monitoring

The SPDI Rules do not have any provisions for vendor/service provider due diligence or monitoring. The IRDA, TRAI and RBI respective sectoral guidelines on outsourcing and cloud services guide companies and banks to carry out due diligence, audits and regular monitoring of vendors and service providers.

Use of Cloud, Outsourcing, Offshoring

The MeitY guidelines for government use of cloud services prescribe that the service providers must store the data within India. If the data is located in one or more discrete sites in foreign countries, the conditions for data location must be mentioned in an agreement with the service providers. The telecom regulations prohibit telecom companies from transferring customer account information outside India. RBI proposes to issue guidelines to operators and participants to ensure that a code of conduct is adhered to in the outsourcing process. TRAI has recommended the creation of a regulatory framework for cloud services, including establishing the first industry-led body of all cloud service providers.

Payment of Ransomware

Currently, there are no regulations restricting the payment of ransomware. However, legal experts have been advising companies against making ransomware payments, as the remittance is likely to trigger implications under the foreign exchange and money laundering laws.

Secure Software Development or Patching

There are no specific regulations in this regard. However, the guidelines provide that information security must be considered at all stages of an information asset – including software development, hardware, life cycle which typically includes planning and design, acquisition and implementation, patching, maintenance and support, and disposal –to minimise exposure to vulnerabilities.

Responsible Disclosure of Software Vulnerabilities

There is no mandate. However, it is possible for individuals and organisations to voluntarily report any cybersecurity incident relating to information or vulnerabilities to CERT-In and seek requisite support and technical assistance to recover from them.

Training

The SPDI Rules do not prescribe any training requirements. CERT-In prescribes stakeholders and other entities to conduct training on technical know-how; RBI and IRDA also prescribe regular training and security awareness to human resources on cybersecurity policies and programmes.

3.4 Key Multinational Relationships

Key multinational relationships are as follows.

- India–US cyber-relationship (signed on 30 August 2016, valid for five years): India and the US have signed a memorandum of understanding (MoU) to co-operate on cybersecurity mechanisms and information sharing.
- India–Israel on cybersecurity (signed 15 January 2018): India and Israel have signed an MoU to develop, promote and expand co-operation in the field of human resources development (HRD) through platforms such as training programmes and skills development.
- India–UK on cybersecurity (signed 20 May 2016): the CERT-In and CERT-UK have signed an MoU to promote co-operation for exchange of knowledge and experience in detection, resolution and prevention of security-related incidents.
- India–Brazil on cybersecurity (signed 25 January 2020): India has signed 15 MoUs with Brazil on 25 January 2020 in respect of various issues, including co-operation in cybersecurity, and addressing information and communication technologies-related issues.
- Japan's Ministry of Internal Affairs and Communications signed an MoU with the Ministry of Communications of India (January 2021) regarding information and communications, and more particularly agreed to co-operate in areas including cybersecurity.
- India has also signed MoUs with Australia, Bangladesh, Indonesia, Kenya, Portugal, Serbia, the UAE, Vietnam, France, Malaysia, Mauritius, Morocco, Qatar and Singapore on cybersecurity co-operation.
- India has signed mutual legal assistance treaties (MLAT) with nearly 35 countries for cross-border co-operation in respect of access to data in different countries.

4. Key Affirmative Security Requirements

4.1 Personal Data

The SPDI Rules require all body corporates to implement reasonable security practices and standards, as well as to document their security programmes and policies. Similarly, the RBI requires banks to classify data based on

business complexity and risk levels, and the sensitivity criteria of a bank. The IRDA cybersecurity policy also provides that systems must be classified under different categories based on their criticality and severity.

4.2 Material Business Data and Material Non-public Information

There is no specific security requirement provision in respect of material business data and material non-public information.

4.3 Critical Infrastructure, Networks, Systems and Software

The National Critical Information Infrastructure Protection Centre (NCIIPC) is the nodal agency for the protection of the Critical Information Infrastructure (CII), networks and systems in the country. The NCIIPC guidelines recommend that cybersecurity breach incidents must be reported to the NCIIPC. The NCIIPC regularly advises on reducing vulnerabilities of the CII, and against cyberterrorism, cyberwarfare and other threats.

The NCIIPC guidelines prescribe the development of audit and certification agencies for the protection of the CII. The NCIIPC also exchanges cyber incidents and other information relating to attacks and vulnerabilities with CERT-In and concerned cybersecurity organisations in India.

4.4 Denial of Service Attacks

There are no specific provisions relating to security requirements to prevent denial of service (DoS) attacks, under the ITA or the SPDI Rules. The NCIIPC guidelines and the sectoral cybersecurity guidelines prescribe preventive and corrective measures to address DoS attacks and similar attacks on systems. Further, the NCIIPC regularly advises on vulnerabilities based on the latest DoS attack incidents, which can be accessed on its website (https://nciipc.gov.in/).

4.5 Internet of Things (IoT), Software, Supply Chain, Other Data or Systems

There are no specific security provisions for other data or systems under the current cybersecurity regime.

4.6 Ransomware/Extortion

Currently, there are no regulations restricting payment of ransomware. However, legal experts have been advising companies against making payments for ransomware, as the remittance is likely to trigger implications under the foreign exchange and money laundering laws.

According to the new CERT-In directive, any cyber security incident must be notified to Cert-In within six hours of its occurrence. Further, any information/documents or other assistance sought by Cert-In in assessing the cybersecurity incident must be promptly provided. According to Section 44(b) of the ITA, if anyone fails to provide the information as requested by CERT, they may be subject to a fine of up to INR5,000 for each day of default. Additionally, non-compliance with CERT's demand for documents/information can result in up to one year's imprisonment and/or a fine of INR100,000.

5. Data Breach or Cybersecurity Event Reporting and Notification

5.1 Definition of Data Security Incident, Breach or Cybersecurity Event

The CERT-In Rules define a cyber-incident as "any real or suspected adverse event that is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing the confidentiality integrity, or availability, of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorisation; or threatens public safety, undermines public confidence, have a negative impact on the national economy, or diminishes the security posture of the nation".

The CERT-In Rules also define cybersecurity incident as “any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, and information without authorisation”.

A cybersecurity breach is also defined under the CERT-In Rules as “unauthorised acquisition or unauthorised use by a person as well as an entity of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource”.

Cybersecurity incidents prescribed under the CERT-In Rules must be reported, including:

- targeted scanning/probing of critical networks/system;
- compromise of critical systems/information;
- unauthorised access of IT systems/data;
- defacement of a website or intrusion into a website and unauthorised changes, such as inserting malicious code, links to external websites, etc;
- malicious code attacks, such as the spreading of viruses, worms, Trojans, botnets and spyware;
- attacks on servers, such as databases, email and DNS and network devices, such as routers;
- identity theft, spoofing and phishing attacks;
- denial of service (DoS) and distributed denial of service (DDoS) attacks;
- attacks on critical infrastructure, SCADA systems and wireless networks; and
- attacks on applications, such as e-governance, e-commerce.

The DPDPA defines personal data breach as "any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data".

As per the provisions of the DPDPA, a data fiduciary, in case of a personal data breach, must inform the DPB as well as the affected data principal about such breach.

The DPDPA mentions that the data fiduciary should only retain personal data in case to comply with any law in force. Other functions of the data fiduciary should include:

- erasure of personal data in case consent is withdrawn by the data principal or after the fulfilment of specified purpose; and
- causing the data processor to erase data that was made available by the data fiduciary for processing

The DPDPA also emphasises reporting of all breaches, regardless of their impact on the data principal or the sensitivity of such breaches. Non-compliance in this regard shall attract a penalty of up to INR 2 billion.

5.2 Data Elements Covered

The data to be provided while incident reporting includes the sector details, location of the system, date and time of the occurrence, criticality, affected system/network, symptoms observed, and the relevant technical information such as type of incident, number of hosts affected, security systems deployed and actions to mitigate the damage. The DPDPA also defines personal data meaning “any data about an individual who is identifiable by or concerning such data.”

5.3 Systems Covered

The ITA covers computer systems, and networks, resources, data and database.

5.4 Security Requirements for Medical Devices

Currently, there are no specific cybersecurity guidelines for medical devices, and the SPDI Rules and the NCIIPC guidelines apply. These include classifying data based on criticality, preparing a documented cybersecurity programme and appointing a CISO.

5.5 Security Requirements for Industrial Control Systems (and SCADA)

There is no specific cybersecurity framework and the security requirements under the SPDI Rules and CERT-In Rules apply to industrial control systems.

5.6 Security Requirements for IoT

There is no specific statutory provision that applies to security requirements for the internet of things (IoT). The data privacy principles under the SPDI Rules are applicable. However, MeitY's draft IoT Policy, 2015 (yet to be approved), proposes to appoint a nodal organisation for formalising privacy and security standards and create a national expert committee for developing and adopting IoT standards in the country.

Further, TechSagar – India's cyber-tech repository, supported by the National Cyber Security Co-ordinator and managed by DSCI – is a platform for discovering India's cyber-tech capabilities. It lists the business and research capabilities of various entities from the IT industry, start-ups, academia and R&D institutes. Currently, about 180–190 capability definitions of IoT are listed on the TechSagar platform. TechSagar acknowledges the presence of 700+ companies, 125+ Academia, 20+ R&D centres and approximately 250 researchers that are active in the IoT space in India.

Also, NASSCOM, MeitY and ERNET have designed an IoT Centre of Excellence (CoE) to help Indian IoT start-ups create market-leading products. This CoE is India's largest deep-tech innovation ecosystem.

5.7 Requirements for Secure Software Development

There are no such statutory requirements.

5.8 Reporting Triggers

Incidents specified under the CERT-In Rules must be reported to CERT-In within six hours in the prescribed format. Data breaches in certain specific sectors such as finance, insurance and securities must be reported to the respective regulators. Cybersecurity incidents must be reported to the CISO.

There is no statutory requirement to report a cybersecurity incident to other companies or organisations. Contractually, a body corporate may require the vendor or service provider to promptly report any incident to the company.

As per the provisions of the DPDPA, a data fiduciary, in case of a personal data breach, must inform the DPB as well as the affected data principal regarding such breach. It also emphasises reporting of all breaches, regardless of their impact on the data principal or the sensitivity of such breach. Non-compliance shall attract a penalty of up to INR2 billion.

5.9 "Risk of Harm" Thresholds or Standards

There are no "risk of harm" thresholds or standards under the current privacy regime. The DP Bill prohibits processing of such information that could cause harm or significant harm to the data principals.

The DPDPA prohibits the processing of personal data which is likely to cause a detriment to the well-being of a child. Also, behavioral monitoring and tracking of children or targeted advertisements made for children are also prohibited under the DPDPA.

6. Ability to Monitor Networks for Cybersecurity

6.1 Cybersecurity Defensive Measures

The relevant laws in India that govern network monitoring and cybersecurity defensive measures are:

- the DPDPA;
- the ITA;
- the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (the "Interception Rules");
- the SPDI Rules;
- the CERT-In Rules and the new directives issued thereunder in April 2022;
- the NCIIPC Rules; and
- the Sectoral Cyber Security Framework Policies.

The ITA provides a legal framework to address hacking and security breaches of IT infrastructure and prescribes penalties for negligently handling SPD. Furthermore, to the extent that the data intercepted and monitored by a body corporate includes the SPD of its customers or employees, the body corporate must comply with the SPDI Rules.

The Interception Rules prescribe that no person shall carry out any interception, monitoring or decryption of any information generated, transmitted, received or stored in any computer resource, unless authorised by India's central or state governments. There is a lack of clarity on whether a company's interception and monitoring of its internal servers will conflict with the above restriction.

. In the "Privacy Judgment" and the expert committee report, the courts have ruled that monitoring of employee communications and employee surveillance must be handled carefully and recommends maintaining a balance between an employee's privacy and the employer's legitimate need to safeguard the company's interest, until the new privacy law is enforced.

The sectoral cybersecurity policies for banks, insurance companies, telecom companies and CII permit body corporates, including banks, to monitor the secure status of each system and network, mobile and home-working procedures, and critical systems. These may include third-party providers. The UASL obliges telecom companies to monitor all intrusions, attacks and fraudulent activity on its technical facilities and report to the DoT.

Cert-In's directives require a body corporate to report a cybersecurity incident within six hours to Cert-In. Further, the bodies corporate must appoint a point of contact to coordinate with Cert-In. Also, all bodies corporate handling Indian residents'/citizens' data or a computer, computer system, computer network located in India, must promptly provide any necessary information demanded by Cert-In to analyse a cyber-breach incident reported to Cert-In. All service providers, intermediaries, data centres, bodies corporate and government organisations must enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days within India. Also, the virtual asset service providers, virtual asset exchange providers and custodian wallet providers must maintain all information obtained as part of Know Your Customer (KYC) and records of financial transactions for five years.

MEITY has constituted four committees to promote artificial intelligence (AI) initiatives and developing a policy framework around it. The committees have submitted their first reports on platforms and data on AI; leveraging AI for identifying national missions in key sectors; mapping technological capabilities; key policy enablers required across sectors; and on cybersecurity, safety, legal and ethical issues.

6.2 Intersection of Cybersecurity and Privacy or Data Protection

The intersection of cybersecurity and privacy is an important point of discussion, more so due to increasing unauthorised data access through cyber-attacks, third-party data sharing and data compromises. Existing privacy laws and cybersecurity laws include data breach notification requirements.

However, these breach notification requirements function directly at the intersection of security and privacy. Data protection requires protecting against unauthorised data access, regardless of how it occurs, while simultaneously securing sharing of data.

The SPDI Rules mandate compliance with reasonable security practices and procedures by documenting information security programme and information security policies, and adhering to security standards, such as ISO270001, or government-approved codes of best practices. Despite the statutory mandate, various cybersecurity breaches have led to the exposure of personal data and SPD (as discussed in 8.4 Significant Private Litigation).

A larger concern that remains is about people who are impacted by such cyber-attacks. In the absence of any statutory provision to notify the impacted persons and assess their loss, the reporting mechanism does not provide any direct benefits or remedies to the impacted persons. Hopefully, the notification of the DPDPA Bill containing stringent fines will bring some respite to the situation.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information

The breach must be reported to CERT-In. As per the provisions of the DPDPA, a data fiduciary, in case of a personal data breach, must inform the DPB as well as the affected data principal about such breach.

7.2 Voluntary Information Sharing Opportunities

As per the provisions of the DPDPA, a data fiduciary, in case of a personal data breach, must intimate the DPB as well as the affected data principal about such breach.

8. Significant Cybersecurity and Data Breach Regulatory Enforcement and Litigation

8.1 Regulatory Enforcement or Litigation

Please refer to **8.4 Significant Private Litigation**.

8.2 Significant Audits, Investigations or Penalties

Please refer to **1.2 Regulators**.

8.3 Applicable Legal Standards

There are no applicable legal standards. Instances of cybersecurity breach are adjudicated on a case-by-case basis.

8.4 Significant Private Litigation

India saw a rising trend of writ petitions filed across various High Courts seeking the right to be forgotten and the right to erasure. A world-renowned doctor in the case of Dr. Ishwarprasad Gilda v Union of India & Others, was charged under the provisions of the Indian Penal Code for causing death by negligence, cheating, and impersonation of a public servant. The doctor was accused of procuring medicines from abroad and administering them to the patients in India. The doctor was arrested in April 1999 and received bail in May 1999. In 2023 the doctor approached the Delhi High Court for "right to be forgotten", asking for all news and journal articles to be erased against him as they were causing a grave injury to his reputation.

As the ITA and the SPDI Rules do not expressly mention the "right to be forgotten", the court relied on Article 21 of the Constitution of India, which includes the Right to Privacy, and the court recognized the right to be forgotten and the held that individuals have the right to silence past events in their lives which are no longer in occurrence. This right allows the individual to

get videos, information, and photographs of themselves deleted from the internet records. The court allowed for an affidavit to be filed that allowed de-indexing so the concerned URLs do not appear in the search results.

In general, in the petitions that involved family matters including matrimony, divorce, custody of a child, etc., the court had allowed the right to privacy and directed the removal of aggrieved persons' details from online records.

In another landmark case, Balu Gopalakrishnan v State of Kerala and Ors (Kerela High Court) W.P. (C). Temp No. 84 of 2020, which involved the collection and transfer of citizens' personal data for COVID-19 tracking purposes by the Government of Kerala to a US-based data analysis company, the Kerala High Court had restricted the government from sharing citizens' sensitive personal data, unless the data was anonymised. The court had also recognised the importance of the data subjects' informed consent before collecting their personal data and laid down the safeguards to ensure the confidentiality of the data collected.

ITAIndia continued to witness a tremendous increase in cybercrime and data breach incidents in 2022 and 2023. India's cyber-attacks on government agencies rose by approximately 15% since 2022. In 2023, there were cyber-attacks on 36 government websites in India. In just the first half of the year around 429,000 cyber-attacks occurred in financial institutions. AIIMS, widely regarded as India's foremost government hospital, was hit by a ransomware attack on 23 November 2022. The incident marked one of the most high-profile data breaches targeting a government-backed entity in the country, compromising the records of nearly 3–4 million patients including high-profile political personalities.

Further, Oil India Limited's headquarters witnessed a massive ransomware attack which led to the shutting down of its computer and IT systems. The attackers had demanded a USD7.5 million ransom. Also, the New CapraRAT Android Malware targeted the Indian government and military personnel.

8.5 Class Actions

Other than under the Companies Act, India does not have any laws enabling class action lawsuits. Under the Companies Act, shareholders or depositors can collectively approach the National Company Law Tribunal for redress where, for example, a company's affairs are not managed in its best interests.

9. Cybersecurity Governance, Assessment and Resiliency

9.1 Corporate Governance Requirements

Under the SPDI Rules, a body corporate that has sensitive personal data is required to employ reasonable security practices to protect the stored data. Furthermore, companies must ensure that electronic records and security systems are protected against unauthorised access and tampering, in accordance with the Companies (Management and Administration) Rules 2014, which was created under the Companies Act, 2013. In case of any information security breach, such corporations are required to show to the authorities that the prescribed security control measures have been implemented. Any lapse on the part of such bodies corporate shall attract charges under Section 43A of the ITA and they will be required to compensate all those affected as a result of such breach.

India's Whistle Blowers Protection Act, 2011 (the "Whistle Blower Act") establishes a mechanism to receive complaints relating to allegations of corruption or wilful misuse of power against any public servant and to provide adequate safeguards against the victimisation of a whistle-blower. However, a major shortfall is that a whistle-blower must disclose their identity in the complaint.

Further, the Companies Act 2013 mandates certain publicly listed companies to establish a vigil mechanism and an exclusive hotline for directors and employees to report their genuine concerns about unethical behaviour or misconduct, actual or suspended frauds, and violations of the code of conduct.

Additionally, SEBI's Listing Agreement's Clause 49 under the Principles of Corporate Governance requires that companies establish a whistle-blower policy to safeguard the identity of an employee who reports instances to the management.

10. Due Diligence

10.1 Processes and Issues

There is no prescribed procedure for conducting diligence in corporate transactions in relation to cybersecurity. The companies normally demand the target company's cybersecurity policy and framework, the annual audit reports on cybersecurity measures, and details of any past breaches and reporting in that regard.

10.2 Public Disclosure

There is no specific legal provision requiring mandatory disclosure of cybersecurity risk profile or experience.

11. Insurance, Artificial Intelligence and Other Cybersecurity Issues

11.1 Further Considerations Regarding Cybersecurity Regulation

A massive increase in cybersecurity incidents was witnessed in 2023, especially on government entities, and the majority were reportedly attacking political decisions and policies. Cert-In had exercised its powers and had issued directives in April 2022 mandating all bodies corporate to report any cybersecurity incident within six hours, and imposing certain other cumbersome obligations on the bodies corporate.

The surge in e-commerce and digital payments in 2023 will be consistent across the country. This exponential rise may deepen concerns about potential cybersecurity risks for consumers and businesses, as well as new kinds of data security breaches. Additionally, with increase in digitisation including digital payments, and remote working becoming the norm, such risks may continue until combined efforts are taken by the stakeholders, users and the government.

RBI, in co-ordination with CERT-In, has issued over ten advisories to supervised entities on various cyberthreats and best practices to be adopted. Additionally, a series of video conferences were conducted regarding cybersecurity preparedness and broad cyber/IT threats to sensitise the supervised entities.

India is set to notify the DPDPA and gives wide powers to the federal government to prescribe detailed rules.

There is already higher awareness and focus on data privacy and cybersecurity. The government and other organisations have been working on developing policies and frameworks in respect of machine learning and AI for cybersecurity solutions, anomaly detection and response, and IoT infrastructure for automation and efficiency, specifically for the CII. Governments and corporations will have to further secure the cloud-based model and the data stored in the cloud. Concepts such as blockchain to prevent data theft may also be in demand.

ITA

On the other hand, India is facing a shortage of cybersecurity skills in the workplace. Certain authorities, such as CERT-In and RBI, have been proactively conducting skill-development activities and encouraging greater awareness to deal with the increase in cyber incidents.

Some regulatory developments are anticipated. The National Cyber Security Strategy 2020 is a long-awaited policy initiative of the government and is expected to bring in stronger security standards and priority allocation after it is notified.

ANA Law Group

7th Floor, Keshava
Bandra Kurla Complex
Bandra East
Mumbai - 400 051
India

+91 22 6112 8484

+91 22 6112 8485

mailbox@anaassociates.com
(mailto:mailbox@anaassociates.com)
www.anaassociates.com
(http://www.anaassociates.com)