Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

# Data Protection & Cybersecurity

Second Edition

**India**
ANA Law Group

2019

chambers.com

# Law and Practice

*Contributed by ANA Law Group*

## Contents

**ANA Law Group** is a full-service law firm based in Mumbai, with a team of experienced professionals who have broad industry knowledge and specialisation across a wide spectrum of laws. It has significant experience in counselling international clients on issues related to data protection and privacy in India, and regularly represents clients from industries such as banking and insurance, online gaming, finance, luxury goods, consumer goods, healthcare, payroll-processing, pharmaceuticals, telecommunications and internet service-providers, credit research and employee screening. The firm also assists international companies with global privacy law involving Indian projects, the drafting and negotiating of contracts with Indian counterparts, and the preparation of data protection and privacy policies for international companies operating in India and their Indian subsidiaries. More specifically, it advises clients on permitted data processing, consent requirements, data collection, retention and disclosure, complying with the regulatory requirements, transfers of sensitive personal data within and outside India; on security breaches and drafting security breach policies; on international compliance projects; and on prosecutions and offences.

## Authors

**Anoop Narayanan** is founder of the firm and has more than 25 years' experience as an attorney, focusing on a broad range of IP, IT, outsourcing, employment, technology, data protection, telecommunications and entertainment law matters. He has worked with some of the nation's highest-profile companies, including global corporates in the manufacturing industry, and banking and finance sectors, in addition to TMT companies. Anoop's expertise in the TMT and data privacy sector developed during liberalisation in India in the mid to late-1990s, when he, as an external counsel in the country, advised on the India entry-related legal aspects, assisted in setting up the Indian operations of large global technology companies, and handled several India-bound outsourcing transactions with major Indian IT companies. His team regularly advises on all technology advancements and the related legal developments, including cloud computing, internet-enabled mobile devices, VOIP, online gaming, cookie technology and the widespread social networking, that carry significant legal challenges.

**Priyanka Gupta** is a senior attorney at ANA Law Group who has been in practice for more than twelve years. She is qualified from a premier national law university and regularly advises on international TMT transactions and regulatory aspects of the Indian telecoms sector. Ms Gupta also advises multinational banks, financial institutions, technology businesses and other companies on data protection and privacy law issues. She has extensive experience in handling advisory, transactional and litigation projects in all areas of TMT and IP practice.

## 1. Basic National Legal Regime

### 1.1 Laws

The Constitution of India guarantees the right to privacy 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 ('privacy judgment').

India does not currently have a comprehensive data privacy law. Personal and confidential information is protected under the Information Technology Act 2000 (ITA) and the IT Rules. India's Central (Federal) Government has ratified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (DP Rules) under the ITA, to govern entities that collect and process sensitive personal information in India.

The DP Rules:

- mandate consent for the collection of information;
- insist that it be done only for a lawful purpose;
- require organisations to have a privacy policy;
- set out instructions for data retention;
- give individuals the right to correct their information, and impose restrictions on disclosure, data transfer, security measures, etc.

The DP Rules apply only to corporate entities, and are restricted to sensitive personal data (SPD), which includes

attributes such as sexual orientation, medical records and history, biometric information, passwords, and so on.

In addition, specific sectors such as banking, insurance, telecom, health, etc, have data privacy provisions under their respective statutes.

Under the ITA, the Indian government has constituted the Indian Computer Emergency Response Team ('the CERT-In') as the national nodal agency for cybersecurity. The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 ('CERT-In Rules') prescribe the functions and responsibilities of CERT-In, the procedure for cyber-breach incident reporting, response and information dissemination, and so on. The CERT-In Rules mandate that service-providers, intermediaries, data centres and body corporates (handling SPD) report all cybersecurity incidents to CERT-In "as early as possible." CERT-In has also set up sectoral CERTs to implement cybersecurity measures at a sectoral level.

For critical sectors, the government has set up the National Critical Information Infrastructure Protection Centre (NCIIPC) under the ITA, as a nodal agency, and 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.

India's unique identification project ('Aadhaar Project') is the world's largest biometrics-based identity project, and is governed by the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 ('Aadhaar Act'). The data protection norms for personal information collected under the project are regulated by the Aadhaar (Data Security) Regulations 2016 ('Aadhaar Security Regulations'), which prescribe technical and organisational measures to be adopted to secure information.

Pursuant to the privacy judgment, the Indian Ministry of Electronics and Information Technology ('MeitY') formed the Justice B N Srikrishna Committee ('expert committee'), to frame an all-encompassing data protection law in India. The expert committee has submitted a draft Personal Data Protection Bill 2018 ('PDP Bill') along with an expert committee report. The PDP Bill intends to be applicable to any personal data collected, disclosed, shared or processed by any Indian entity in India. It also extends to foreign 'data fiduciary' and 'data processor' processing personal data involving any business carried on in India, offering goods or services to data principals in India or profiling of data principals in India.

India now awaits a robust data protection regime with the approval of the PDP Bill based on the expert committee report.

### 1.2 Regulators

India does not have a data privacy authority as yet. The ITA mandates the central government to appoint an adjudicating officer to conduct an inquiry for injury or damages of claims valued up to INR5 crore (approximately USD703,981). Claims exceeding this amount must be filed before the competent civil court. 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. Appeals from the adjudicating officer can be filed before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

Regulators are consistently engaged in supervising their relevant intermediaries on the progress of implementation and robustness of cybersecurity frameworks. They regularly conduct cybersecurity/system audits of the intermediaries, which are reported to the relevant regulators.

Sector-specific regulators include the following.

***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 recently set up Cyber Security and Information Technology Examination (CSITE) Cell of Department of Banking Supervision, periodically to assess the progress made by banks in the implementation of the CSF and other regulatory instructions/advisories through on-site examinations and off-site submissions. The RBI has also introduced an internal ombudsman scheme for commercial banks with more than ten branches as a redressal forum, and has also proposed to set up an online portal to investigate and address cybersecurity concerns and complaints.

***Insurance sector***

The Insurance Regulatory and Development Authority (IRDA) conducts regular on-site and off-site inspections of insurers to ensure compliance with the legal and regulatory framework. In addition, the IRDA's guidelines on Information and Cyber Security for Insurers (IRDA Cyber Security Policy) mandates a separate information security audit plan for insurers covering IT/technology infrastructure and applications.

***Telecom sector***

Telecom operators are governed by regulations laid down by regulatory bodies, including:

- the Telecom Regulatory Authority of India (TRAI) (to be renamed the Digital Communications Regulatory Authority of India);
- the Department of Telecom (DoT);
- the TDSAT;
- the Group on Telecom and IT (GOTIT);
- the Wireless Planning Commission (WPC); and
- the Telecom Commission (to be renamed the Digital Communications Commission) (DCC), which also includes information security requirements.

Furthermore, the Unified Access Service Licence (UASL) extends information security to the telecom networks as well as to third parties of operators. The regulator requires telecom operators to audit their network (internal/external) at least once a year. The regulator, in its National Digital Communications Policy of 2018, seeks to establish a comprehensive data protection regime and assure security for digital communication.

***Securities***

The Securities Exchange Board of India (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 has also been extended to stockbrokers and depository participants.

***Health sector***

The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (IMCR) impose patient confidentiality obligations on medical practitioners. In addition, data privacy in the healthcare industry is currently governed under the DP Rules. The Ministry of Health and Family Welfare ('Health Ministry') has issued draft legislation known as the Digital Information Security in Healthcare Act ('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 a 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 PDP Bill prescribe central government to appoint a Data Protection Authority (DPA) to ensure compliance of 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. In the case of significant data fiduciaries, the expert committee report and PDP Bill proposes appointment of a data protection officer (DPO) to address data principals' grievances.

### 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 INR5 crore (approximately USD703,981). MeitY has appointed the Secretary of the Department of Information Technology of each Indian State or Union Territories 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 Telecom Disputes Settlement and Appellate Tribunal (TDSAT), and the subsequent appeal before the High Court.

The PDP Bill prescribes filing the complaint before the data protection officer, which can be appealed before the adjudicating officer of the DPA, who will have the authority to impose penalties on the data fiduciary. The maximum penalty for violation of the PDP Bill's provisions is INR15 crores (approximately USD2 million) or 4% of the data fiduciary's total global turnover in the preceding financial year, whichever is higher.

The expert committee report and PDP Bill propose the central government to establish an appellate tribunal to adjudicate on appeals from the orders of the DPA, and the SCI as the final appellate authority for all purposes under the PDP Bill.

### 1.4 Multilateral and Subnational Issues

The current data privacy principles under the DP Rules are similar in many respects to the EU data protection law. However, considering the digital economy, technological advancements in India, and the need to protect innovation while protecting the right to privacy, the expert committee has adopted a nuanced approach to drafting the PDP Bill. In several respects, the PDP Bill is aligned with the GDPR. For instance, 'personal data' under the PDP Bill is as broadly defined as under the GDPR and includes any data relating to a natural person, who is directly or indirectly identifiable. The PDP Bill also introduces the concepts of 'data fiduciary' and 'data principal', similar to that of 'data controller' and 'data subject' under the EU's General Data Protection Regulation (GDPR). The PDP Bill includes the concepts of right to confirmation and access to data, the right to be for-

gotten, the right to correction of data, and so on, similar to the GDPR.

Furthermore, unlike the GPDR, the PDP Bill prescribes for data localisation, ie, every data fiduciary is required to ensure storage on a server or data centre located in India of at least one serving copy of personal data. In addition, the PDP Bill does not grant individual rights in respect of automated decision-making, profiling (except for minors), as prescribed under the GDPR.

The SCI has acknowledged the US understanding of the right to be left alone in the privacy judgment, and the PDP Bill, which proposes to implement an individual's right to be forgotten.

In view of the foregoing, and to encourage innovation, the expert committee has adopted a nuanced approach towards data privacy with reasonable restrictions. Furthermore, the expert committee has encouraged the co-regulation enforcement model in India, which involves both government and industry participation in drafting and enforcing regulatory standards, and combines the flexibility of self-regulation with the rigour of government rule-making.

### 1.5 Major NGOs and Self-Regulatory Organisations

The major data privacy non-governmental organisations and industry self-regulatory organisations in India include:

- the Data Security Council of India (DSCI), a not-for-profit industry body, set up by the National Association of Software and Services Companies (NASSCOM), which engages with governments and their agencies, regulators, industry sectors, industry associations and think-tanks for policy advocacy, thought leadership, capacity-building and outreach activities;
- the 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 Centre for Internet and Society (CIS), a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives.

### 1.6 System Characteristics

Please refer to section **1.4 Multilateral and Subnational Issues** above.

### 1.7 Key Developments

Key developments in the industry in the past 12 months have included:

- pursuant to the privacy judgement, the expert committee submitted its report and the PDP Bill, which is the first comprehensive and all-encompassing data protection framework in India, is soon expected to be finalised and enacted;
- the MeitY ratified the Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018 (the 'Protected System Rules'), which provide a detailed infrastructure to secure the CII and the protected system (computer resource);
- the TRAI released Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector ('TRAI Recommendations');
- the RBI proposed to set up an integrated compliance and tracking system portal to supervise cybersecurity measures of payment system-providers;
- the RBI notified the CSF for Urban Co-operative Banks;
- the MeitY proposed the Information Technology Intermediaries Guidelines (Amendment) Rules 2018, to strengthen the legal framework and enhance intermediary liability concerning security and cybersecurity;
- the SCI upheld the validity of the Aadhaar Act and allowed for number-based authentication to establish an individual's identity for receipt of a subsidy, benefit or service given by the Central or State Government. However, SCI disallowed the mandatory demand for individual Aadhaar numbers by private entities including banks, telecom companies, etc, to provide the services, on the basis that it was contrary to the fundamental right to privacy;
- the SCI issued a notice to WhatsApp to respond to a petition that states that WhatsApp must follow all conditions mandated for telecom operators, including having a grievance redressal system and data localisation. The petition also challenges WhatsApp's proposed launch of a payment platform while the company does not have a physical presence in India;
- the guidelines of the Directorate General of Civil Aviation (DGCA) for the operation and import of remotely piloted aircraft systems (RPAS) were made effective from 1 December 2018;
- the RBI mandated data localisation for storage of payment system data;
- India's Ministry of Home Affairs (Cyber and Information Security Division) passed an order in December 2018

authorising ten central agencies to intercept, monitor and decrypt "any information generated, transmitted, received or stored in any computer" in an attempt to curb fake news and rumours through social media;
- the DSCI, in association with Microsoft and ISEA of MeitY, launched 'Project Cyber Shikshaa' to train women engineering graduates in the niche field of cybersecurity; and
- the MeitY issued Top Best Practices for a Safe and Secure Cyber Environment for chief information security officers (CISOs) appointed under the Protected System Rules.

### 1.8 Significant Pending Changes, Hot Topics and Issues

The government may soon enact the PDP Bill, and India may finally have comprehensive data privacy legislation.

Cert-Fin may be established as an exclusive cyber-response team for the financial sector, along with a functioning National Cyber Co-ordination Centre, and robust cybersecurity measures for 'protected systems.'

Amendments to the intermediary guidelines with the primary aim of avoiding misuse of social media platforms and the spreading of fake news may also be ratified.

## 2. Fundamental Laws

### 2.1 Omnibus Laws and General Requirements

General requirements under the DP Rules include:

- a company handling personal data or SPD must provide a privacy policy on its website, accessible to data-providers;
- companies must obtain express prior consent from data-providers regarding the purpose and use of information;
- a company can only collect SPD for a lawful purpose connected with a company's business;
- data-providers must be made aware of the purpose for which information is collected, the intended recipients of the information, the agency collecting and retaining the information, etc. Furthermore, the data-provider must be given the option not to provide the information, or to revise or withdraw the information;
- entities holding SPD should not retain the information longer than the required purpose for which it was collected or lawfully used;
- transfer of SPD within or outside India is permitted with restrictions, such as:
  (a) the recipient entity ensures adherence to the same level of data protection; and
  (b) the transfer is necessary to comply with a lawful contract; or
  (c) the data-provider has given prior consent.
- companies must have "reasonable security practices and procedures;" and
- companies must appoint a grievance officer and address complaints in a timely manner.

The DP Rules do not provide for the appointment of DPOs. However, the expert committee report and the PDP Bill provide for appointment of DPOs by data fiduciaries as the point of contact for data principals' grievances. DPOs shall monitor personal data processing and guide the data fiduciaries towards compliance with the PDP Bill.

Under the DP Rules, body corporates must seek the data-provider's consent before the collection, transfer, disclosure to third parties of his or her SPD, and take reasonable steps to ensure that the individual has knowledge about the personal data or SPD being collected, the purpose of its collection, its intended recipients and the collecting agency's name and address. However, the data-provider's consent is excepted in cases where government agencies require the individual's SPD for identity verification, or for prevention, detection, investigation, prosecution and punishment of offences.

The concepts of 'privacy by design' and 'privacy by default' are not defined in the current Indian data protection law, but are provided under the PDP Bill. However, these concepts are reflected in the ITA and the DP Rules, as they incorporate provisions such as:

- providing a privacy policy and disclosure of information;
- collection of information for lawful purposes with a data-provider's consent;
- use of information for the purpose for which it was collected; and
- retention of information for only as long as the purpose is being fulfilled, etc.

The current Indian data protection law does not prescribe the need to conduct privacy impact analyses. However, the PDP Bill mandates data protection impact assessment (DPIA) for data fiduciaries prior to undertaking any processing involving new technologies or large-scale profiling or use of sensitive personal data that has a risk of causing significant harm to data principals.

The DP Rules mandate data controllers to publish a privacy policy on their website, accessible to data-providers, based on the prescribed privacy principles.

The DP Rules grant the right to data providers to review, edit and update their personal data, and to withdraw their consent to provide personal data. Additionally, the PDP Bill provides data portability rights to the data principal.

The current Indian data protection law does not contain any provisions relating to anonymisation or pseudonymisation. In the absence of a specific provision, technically, the DP Rules will apply to processing of both anonymised and pseu-

donymised data. However, the PDP Bill proposes that the provisions relating to processing of personal data will apply to anonymised data, and requires the data fiduciary and data processor to implement appropriate security safeguards for data pseudonymisation (de-identification) and encryption. It also proposes that re-identification of de-identified data without the data fiduciary's consent shall be a punishable offence. The technical standards and safekeeping measures related to anonymisation and de-identification will be prescribed by the DPA.

The current Indian law does not address the emerging issues of profiling, automated decision-making, online monitoring or tracking, Big Data analysis and artificial intelligence. As discussed below, the PDP Bill addresses some of these issues.

The current Indian data protection law does not define the concepts of 'injury' or 'harm.' However, the PDP Bill defines 'harm' as well as 'significant harm,' and imposes obligations on data fiduciaries to design technical systems to avoid any harm to the data principal, to conduct a DPIA to minimise or mitigate any potential harm to the data principal, and provide remedies for unauthorised and harmful processing, etc.

### 2.2 Sectoral Issues

Under the DP Rules, SDP consists of personal information relating to:

- passwords;
- financial information such as bank accounts, credit cards, debit cards or other payment instrument details;
- physical, physiological and mental health conditions;
- sexual orientation;
- medical records and history;
- biometric information;
- any details relating to the above, as provided to a body corporate for providing a service; and
- any of the information received under the above by a body corporate for processing, stored or processed under lawful contract or otherwise.

The PDP Bill expands the scope of SPD to include official identifier, sex life, genetic data, transgender and intersex status, religious/political beliefs and affiliations, caste or tribe and any other category that the DPA may specify. The PDP Bill clarifies that the SPD can be processed based on explicit consent, or for the function of the government, if mandated under law, or if certain SPD is strictly necessary to respond to any medical emergency, disaster or outbreak of disease that may threaten public health.

The DP Rules recognise financial information such as credit cards, debit cards and other payment instrument details as SPD; thus, to an extent regulate their use, collection and disclosure. Furthermore, the key legislation that address data protection in the finance sector include the Credit Information Companies (Regulation) Act 2005 ('CIC Act'), the Credit Information Companies Regulation 2006 ('CIC Regulations') and circulars issued by the RBI.

The CIC Act and CIC Regulations primarily apply to CICs, recognise them as data collectors, require the CICs to ensure data security and secrecy, adhere to privacy principles in respect of data collection, use, disclosure, data accuracy and protection against loss or unauthorised use, access and disclosure.

The Know Your Customer (KYC) norm categorises the information that banks and financial institutions can seek from their customers. Once such information is collected, banks have an obligation to keep it confidential. Furthermore, multiple RBI circulars, such as the Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks and Credit Card issuing NBFCs, the Master Circular on Customer Services, and the Code of Banks Commitment to Customers, etc, provide for privacy and customer confidentiality obligations to be complied with by various financial institutions.

The RBI's recent guidelines on data localisation of payment system data in India will also to an extent help protect financial data.

The Public Financial Institutions (Obligations as to Fidelity and Secrecy) Act 1983 prohibits public financial institutions from disclosing a client's information to third parties, except in accordance with the laws of practice and usage.

The RBI Guidelines on Managing Risks and Code of Conduct in the Outsourcing of Financial Services by Banks prescribe measures maintaining the confidentiality and security of customer data while transferring data to third-party service-providers.

The Banking Codes and Standards Board of India prescribes a code of conduct on banking operations, including privacy and confidentiality of customer information.

The SEBI requires securities market intermediaries to maintain client data confidentiality, including personal data.

Data protection laws in respect to health data are inadequate in India. The Health Ministry has proposed the DISH Act to ensure electronic health data privacy, security and standardisation in the healthcare sector. The DISH Act is pending the government's approval and is expected to be notified soon. Currently, the Clinical Establishments (Central Government) Rules 2012 mandate that clinical establishments must store, maintain and provide health information in an electronic format. Furthermore, the DP Rules recognise health information as SPD, and thus, regulate its collection, use and disclosure. However, as the DP Rules apply only to body

corporates, the public health sector is still unregulated. The PDP Bill proposes applicability of data privacy obligations to both state and non-state entities.

Furthermore, the IMCR prescribes that a patient's health data must not be disclosed without his or her consent, unless mandated under a law or there is a risk to an individual or community, or the disease is notifiable. In addition, physicians are encouraged to computerise medical records, maintain them for a period of three years, and provide access to a patient upon request. The limited privacy safeguards and absence of an enforcement mechanism renders the MCI Code of Medical Ethics largely inadequate to address health information concerns.

Although there are multiple telecom laws, such as the Indian Telegraph Act 1885 ('Telegraph Act'), the Indian Wireless Telegraphy Act 1933, the Telecom Regulatory Authority of India Act 1997 ('TRAI Act') and various regulations issued thereunder, data protection norms in the telecom sector are primarily governed by the UASL issued to telecom service providers (TSPs) by the DoT. A TSP has an obligation to take necessary steps to safeguard the privacy and confidentiality of users' information. Furthermore, customer information can be disclosed only after obtaining the individual's consent and the disclosure is in accordance with the terms of that consent.

Some of the key TRAI recommendations concerning TSPs include:

- the user is the owner of his or her data, and data processors are only custodians;
- entities in the digital ecosystem should refrain from using meta data to identify users;
- until the PDP Bill is enforced, all entities in the digital ecosystem must be governed under the licence conditions of TSPs;
- privacy by design, along with data minimisation, should apply to all entities in the digital ecosystem;
- telecom users must have rights to notice, consent, data portability, and the right to be forgotten;
- data controllers should be prohibited from using 'pre-ticked boxes' to gain users' consent;
- data should be encrypted during processing and storage; and
- privacy breach information should be shared for greater transparency.

The TRAI's UASL regime for internet service-providers governs data privacy issues relating to the internet, to some extent. The current DP Rules require data controllers to provide a privacy policy on their website that is accessible to data-providers.

The PDP Bill, expert committee report and the TRAI recommendations propose to regulate data privacy issues relating to the internet in India.

Sexual orientation information is considered as SPD, and thus protected under the DP Rules. The PDP Bill proposes to expand the definition of SPD to include religious or political beliefs and affiliations, official identifiers, transgender/intersex status and caste or tribe information. Indian law does not recognise union membership as SPD.

The DP Rules do not regard voice telephony as SPD. However, in October 2017, the TRAI released recommendations on a regulatory framework for internet telephony, recognising internet telephony as an aspect of Voice over Internet Protocol (VoIP), governed by the UASL. The agreement requires service-providers to safeguard communication information privacy and confidentiality and prevent unauthorised interception.

The DP Rules mandate body corporates to provide a privacy policy on their website accessible to data-providers, containing the body corporate's practices and policies, type, purpose and usage of the personal data or SPD collected, disclosure of personal data or SPD, and the company's security practices.

India does not have specific regulations on the use of cookies, beacons or tracking technologies. However, the PDP Bill prohibits data fiduciaries from tracking minors.

The current Indian data protection framework does not provide for any 'Do not track' mechanism. However, the proposed PDP Bill prohibits tracking of personal data of minors by data fiduciaries.

Behavioural advertising is not regulated under current Indian data protection laws. The PDP Bill prohibits behavioural monitoring and advertising in respect of minors. Furthermore, the expert committee report contemplates that behavioural monitoring must require mandatory user consent prior to accessing online content.

Television is regulated under various broadcasting laws, specifically the Cable Television Networks (Regulation) Act 1995. However, India does not currently have specific laws to govern privacy issues relating to smart TVs and videos.

Critical data privacy issues relating to social media, search engines, online platforms and so on are not adequately governed under the current Indian law. Telecom and network service-providers, web-hosting service-providers, search engines and online platforms, etc are defined as 'intermediaries' under the ITA. Furthermore, the MeitY proposes to include social media companies under 'intermediaries.' The ITA and intermediaries guidelines prescribe certain obligations on intermediaries, including:

- compliance with all the data privacy principles prescribed by the DP Rules;
- government directions relating to block data access to public;
- to monitor and collect data through any computer resource;
- to publish the rules and regulations, privacy policy and user agreement for access or usage of the computer resource by any person;
- not to host or publish any information or initiate the transmission of restricted content;
- to inform its users of non-compliance consequences; and
- to promptly report cybersecurity incidents to the CERT-In.

The DP Rules do not provide for the right to be forgotten to data-providers. However, the PDP Bill proposes that a data principal has the right to restrict or prevent continuing disclosure of personal data by a data fiduciary, subject to the adjudicating officer determining that the right to be forgotten does not override the right to freedom of speech and expression and the right to information of any citizen.

Furthermore, the TRAI recommendations specify regarding the right to be forgotten to all users of digital services, subject to restrictions under other applicable laws.

The Indian courts have also observed that the right to be forgotten should be safeguarded in sensitive cases involving women in general, and highly sensitive cases affecting the modesty and reputation of the person concerned.

The right is also emphasised in the privacy judgment in which the SCI observed that:

"In the digital world, preservation is the norm and forgetting a struggle. People are not static; they are entitled to re-invent themselves and correct their past actions. It is privacy which nurtures this ability and removes the shackles of unadvisable things which may have been done in the past."

The publication of hate-speech, abusive material and political manipulation are regarded as offences under the ITA. The ITA prescribes that if a person sends any information, using the internet or a computer, that is offensive, or any information for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, they must be punished with imprisonment for a term that may extend up to three years, and a fine.

The current law does not provide for data portability. The PDP Bill prescribes the right to data portability in the case of automated data processing only, and the data principal can demand data transfer to any other data fiduciary in a structured, commonly used and machine-readable format. Additionally, the TRAI's recommendations prescribe that users have primary control over personal data and must have data portability rights.

The current Indian data privacy law does not address privacy issues relating to children. Under India's contract law, a contract executed by a minor (below 18 years) is invalid, and parental or legal guardian consent must be obtained for all online contracts. The PDP Bill recognises a data principal below the age of 18 years as a child and mandates data fiduciaries to incorporate an appropriate mechanism for the verification of a child's age and parental consent to process children's personal data to protect and advance the child's rights and best interests.

The PDP Bill proposes that the DPA will notify guardian data fiduciaries (operators of commercial websites or online services that process personal data related to children) who will be barred from profiling, tracking, monitoring behaviour, targeting advertisements or processing data that may cause harm to children, and will offer child-counselling and protection services.

### 2.3 Online Marketing

The TRAI has ratified the Telecom Commercial Communication Customer Preference Regulations, restricting unsolicited commercial or marketing communications such as telephone calls and SMS based on a customer's preference where they can register themselves under the fully blocked category or partially blocked category. The TRAI has formed a 'Do-Not-Call Registry' where customers can register to restrain any unsolicited calls or SMS. The Regulations impose penalties of up to INR250,000 (approximately USD3,563) for non-compliance.

Please see **2.1 Omnibus Laws and General Requirements**.

The current law does not have any specific provision to deal with privacy issues arising from location-based advertising or other communications.

### 2.4 Workplace Privacy

Currently, India does not have any specific law to deal with workplace privacy or protection of employee data. However, the PDP Bill proposes that employees' personal data can be processed if it is necessary for an employee's recruitment or termination, providing any service or benefit sought by an employee, attendance verification of the employee or any activity relating to employee's performance assessment. The employer need not obtain the employee's consent where the consent is not appropriate, having regard to the employment relationship between them, or would involve a disproportionate effort by the employer due to the nature of the processing activities.

The current law does not prohibit or restrict camera surveillance, or the monitoring of employees' office emails, telephone calls and data on office devices, provided such activities are reasonable and do not violate employees' privacy. To avoid any risks, many employers obtain employees' consent, either as part of the employment agreement, company policies, or through separate letters.

The role of labour organisations or works councils with respect to workplace privacy is not covered under the ITA, DP Rules, or employment laws.

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 his or her identity in the complaint.

Furthermore, 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, misconduct, actual or suspended fraud, and violation of code conduct.

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

Employers are subject to the DP Rules for data collection and data transfer in deploying digital loss prevention technologies.

### 2.5 Enforcement and Litigation

As India currently does not have a specific DPA, data protection issues are adjudicated by an adjudicating officer appointed under the ITA, who has the powers of a civil court.

The penalties for data breaches are prescribed under the ITA.

A body corporate (which owns, controls or deals, or handles any SPD in a computer resource) that is negligent in implementing and maintaining reasonable security practices and procedures, and causes wrongful loss or wrongful gain to any person, is liable to pay damages, not exceeding INR5 crore (approximately USD703,981) to the person so affected. Cases involving damages of more than INR5 crore (approximately USD703,981) are brought before the competent civil court.

The adjudicating officer can either grant a penalty or any amount of compensation. For offences for which no separate penalty is prescribed, the amount of compensation is limited to INR25,000 (approximately USD358).

ITA provisions do not factor the wide range of data breach instances due to technology advancements. Moreover, the quantum of penalty under the ITA can be inadequate to act as a deterrent for emerging e-commerce and other technology-based players in India.

However, offences under the proposed PDP Bill are cognisable and non-bailable, and entail much stricter penalties including imprisonment and fines.

In a landmark litigation relating to the Aadhaar Project, several writ petitions, including the privacy judgment, were consolidated, as the SCI upheld the validity of the Aadhaar Act, but disallowed the mandatory linking of Aadhaar numbers with bank accounts, mobile numbers, insurance policies, passports, etc, except for tax filings, which entails the sharing of SPD, including biometrics, with third parties, as it violated the DP Rules and the right to privacy.

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 redressing situations such as when a company's affairs are not managed in its best interests, etc.

Data-breach complaints before an adjudicating officer are not reported systematically in any public database. Some states' departments of information technology provide a few orders on their website, mostly relating to bank fraud. For instance, in a private litigation filed by Anant Ganesh Jog against the State Bank of India, unauthorised online transactions were made from his account by an unknown individual who had exchanged the complainant's SIM card from Vodafone (the telecom operator). The adjudicating officer ruled in the complainant's favour, and directed the bank to credit a certain amount into the complainant's account. The officer also imposed a penalty of INR15,000 (approximately USD200) on the bank for non-compliance with the KYC requirements. The officer further observed that there appeared to be a lack of awareness of the civil remedies available to citizens in terms of penalties as well as compensation under the ITA. To ensure that citizens become more aware of the legal provisions and be more vigilant, there is a general need to increase awareness of the legal framework. Accordingly, the officer ordered that the decision in this case be put into the public domain and widely publicised.

## 3. Law Enforcement and National Security Access and Surveillance

### 3.1 Laws and Standards for Access to Data for Serious Crimes

The Indian government (including law enforcement agencies) has wide powers under various legislations for surveillance, monitoring and access to data for investigations of serious crimes, national security and anti-terrorism.

Key legislation includes:

- the Indian Telegraph Act 1885, which allows the interception of telephonic conversations in the case of a public emergency or in the public interest, and requires the disclosure of call data records to law enforcement agencies;
- the ITA and IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, which allow for the interception, monitoring and decryption of digital information in any computer resource in the interest of the sovereignty, integrity and defence of India, security of the state, friendly relations with foreign nations, public order, preventing incitement to the commission of any cognisable offence relating to the above, and for the investigation of an offence;
- the IT (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules 2009, which permit any government agency to monitor and collect traffic in any computer resource for the purposes stated under the ITA;
- the DP Rules, which permit the disclosure of personal data to government agencies without obtaining the data provider's consent;
- the IT (Intermediaries Guidelines) Rules 2011 and IT (Guidelines for Cyber Cafe) Rules 2011, which require intermediaries to provide any information to government agencies under lawful order within 72 hours;
- the TRAI's various licence agreements for ISPs, TSPs and UASL, which provide for surveillance of communications, monitoring telecommunications traffic in every node or in any other technically feasible point in the network, and prohibits bulk encryption and encryption that exceeds 40 key bits;
- the Income Tax Act 1961, which allows state tax authorities to process personal data in respect of an assessee's financial information for enquiry and investigation purposes made in compliance with law;
- the mass surveillance programme, Centralised Monitoring System (CMS), operated by the government's telecommunications technology development centre's Telecom Enforcement Resource and Monitoring (TERM) cells, which empowers the government to intercept any and all communications deemed 'necessary or expedient' for purposes such as national sovereignty and integrity, state security, friendly relations with foreign states, public order, for preventing incitement to the commission of an offence, etc; and
- the PDP Bill, which proposes non-consensual collection, storage and processing of personal data and SPD for securing state security and for the prevention, detection, investigation and prosecution of any offence.

Government agencies can authorise unilaterally under a lawful order, without judicial approval.

### 3.2 Laws and Standards for Access to Data for National Security Purposes

The laws and standards applicable to government access to data are the same as those for law enforcement agencies, such as the Indian Telegraph Act (ITA) and various rules thereunder including the DP Rules, TRAI's licence agreements for ISPs, TSPs, UASL, etc, and the CMS (not yet fully operational).

Government agencies can authorise unilaterally under a lawful order, without judicial approval.

### 3.3 Invoking a Foreign Government

A foreign government's access request is not a legitimate basis to collect and transfer SPD. Providing SPD to a foreign government becomes mandatory only by an Indian court order or a mutual national reciprocity arrangement with that country.

The current law does not mandate or prohibit a private organisation from providing SPD to a foreign government, and the transfer is subject to DP Rules.

The PDP Bill mandates data localisation for SPD, and allows for the transfer of personal data outside India, subject to the prescribed conditions.

### 3.4 Key Privacy Issues, Conflicts and Public Debates

Indian laws give expansive powers to government to access data for reasons including intelligence, anti-terrorism or national security. The SCI has recently directed the government to make laws to curb fake news and rumours spread on social media that may lead to mob violence and lynching. The SCI and the government have made social media companies liable for incriminating and false content circulated on their platforms. Reportedly, the government has asked WhatsApp to set up a local entity and find a solution to trace the origin of fake messages on its platform and to deal with 'sinister developments' such as mob lynching and revenge porn.

In addition, the government's authorisation to ten central agencies to intercept, monitor and decrypt "any information generated, transmitted, received or stored in any computer" has attracted criticism.

The proposed amendments to the intermediary guidelines mandate companies to trace and report the origin of messages within 72 hours of receiving a complaint from law enforcement agencies, as well as 'disable access' within 24 hours to content deemed defamatory or against national security. These provisions have also resulted in public debate on monitoring users' social media accounts.

Implementation of the PDP Bill, which will entail stringent compliance with the privacy regulations by data fiduciaries and data controllers, is much awaited.

## 4. International Considerations

### 4.1 Restrictions on International Data Issues

The DP Rules permit overseas data transfer, subject to certain restrictions such as the recipient entity ensuring the same level of data protection, and if the transfer is necessary to comply with a lawful contract, or with the data-provider's prior consent.

The PDP Bill proposes to permit cross-border transfer of personal data and SPD subject to certain conditions, including data localisation and the transfer being subject to the DPA's approval.

The MeitY guidelines for government use of cloud services prescribe that the service provider must store the data within the country. If the data is located in one or more discreet sites in foreign countries, the conditions for data location have to be mentioned in an agreement with the service-provider.

The telecom regulations prohibit telecom companies from transferring customer account information outside India.

### 4.2 Mechanisms That Apply to International Data Transfers

Besides the restrictions prescribed under the DP Rules, Indian law currently does not have any mechanism to apply to international data transfers. The PDP Bill prescribes that the international transfer of personal data, excluding government-notified SPD, would be subject to DPA-approved standard contractual clauses or intra-group schemes. In such transfers, the transferor would have to periodically notify the DPA of its compliance with the contract/scheme. The PDP Bill extends the transferor's liability to non-compliance by the transferee entity. Furthermore, the transferor entity must store at least one serving copy of the personal data on a local server or data centre in India.

### 4.3 Government Notifications and Approvals

Currently, there are no government notifications or approvals required to transfer data internationally. The PDP Bill mandates government approval while transferring data to a particular country, a particular sector within a country or a particular organisation.

### 4.4 Data Localisation Requirements

The current data privacy law does not require data localisation. The RBI has recently mandated all payment-system operators to store their payment information within India. Furthermore, the PDP Bill recommends the localisation of at least one serving copy of personal data in India and that SPD will be stored only in servers located in India.

Furthermore, the government may approve a cross-border data transfer in an emergency situation where the government is convinced that transfer is necessary.

### 4.5 Sharing Technical Details

There is no mandatory requirement to share software code or algorithms with the government. The ISP licence agreement requires submission of the decryption key, split in two parts, with the DoT if the service-provider employs the encryption technologies of more than the permitted standard of up to 40 key bits.

### 4.6 Limitations and Considerations

An organisation can collect and transfer personal data to a foreign government if it complies with the overseas data transfer restrictions under the DP Rules.

### 4.7 "Blocking" Statutes

India does not have a blocking statute, related to data privacy or otherwise.

## 5. Emerging Digital and Technology Issues

### 5.1 Addressing Current Issues in Law

Big Data analytics is not dealt with under current Indian law. In the absence of a specific regulatory environment, the legal aspects applicable to Big Data in India are similar to those in other countries, such as copyright law issues, database breaches, data protection and privacy issues.

Privacy concerns from automated decision-making are not addressed under the current law. The PDP Bill, however, addresses adversities that may arise out of automated decision-making.

The current law does not recognise profiling. The PDP Bill prohibits profiling of minors' personal data and SPD, and mandates data fiduciaries to carry out a DPIA if the profiling could cause significant harm to individuals.

Artificial intelligence is not dealt with under the current data privacy regime. However, reliance on AI is significantly

increasing among organisations to secure their networks and data.

The IoT and related privacy issues are not addressed under the current data protection framework. The data privacy principles under the DP Rules are applicable. MeitY's draft IoT policy of 2015 (yet to be approved) proposes to appoint a nodal organisation for formalising privacy and security standards, and to create a national expert committee for developing and adopting IoT standards in the country.

Indian law does not address data privacy concerns relating to autonomous decision-making including autonomous vehicles.

There are no specific provisions to address privacy concerns arising from facial recognition technology. The large amount of emotional and factual data collected from facial recognition technology can be regarded as SPD. The PDP Bill proposes including facial images under the definition of biometric data.

Biometrics are specifically categorised as SPD under the DP Rules, and its collection, processing and transfer is subject to the prescribed statutory restrictions.

The PDP Bill also prescribes strict conditions for processing biometric data. Please also refer to the discussions on the Aadhar Project.

Sharing geolocation and the data collected through this technology is not regulated under India's current data privacy laws.

The Civil Aviation Requirements (Drone Regulations 1.0) August 2018 permit the civil use of drones by non-government agencies, subject to prescribed restrictions.

As the Drone Regulations 1.0 do not address the issue of data privacy, these concerns are governed under the DP Rules.

## 6. Cybersecurity and Data Breaches

### 6.1 Key Laws and Regulators

The CERT-In is the national nodal agency for cybersecurity. The CERT-In Rules prescribe the functions and responsibilities of CERT-In, as well as procedures for incident reporting, response and information dissemination, etc. The MeitY has authorised the CERT-In to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

The CERT-In Rules mandate service-providers, intermediaries, data centres and body corporates to report prescribed cybersecurity incidents to CERT-In at the earliest.

Furthermore, the government has set up the NCIIPC to facilitate a safe, secure and resilient CII for certain sectors, such as transport, telecoms, power and energy, banking and financial institutions, e-governance and strategic public enterprises.

The MeitY's recently ratified protected system rules also provide a detailed infrastructure to secure the CII and the protected systems.

At present, there is no over-arching cybersecurity agency for India similar to ENISA.

The role of data protection authorities or privacy regulators is discussed in **1.2 Regulators**.

The RBI is the financial sector regulator. 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. Furthermore, the IDRBT owns the Indian Financial Network (INFINET), the communication backbone for the Indian banking and finance sector.

The RBI's Regulations, the Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds ('RBI Cyber Security Guidelines'), provide comprehensive guidance on information technology governance for banks in India.

The RBI has also issued Guidelines on CSF in Banks, advising banking companies to have an adaptive incident response, management and recovery framework to deal with adverse incidents and disruptions. Recently, the RBI has issued separate cybersecurity guidelines for urban co-operative banks.

The Finance Minister has proposed to establish a CERT-FIN, which will act as an umbrella CERT for the finance sector. Until such time, the RBI is the lead regulator.

Additionally, the SEBI has issued guidelines on Cyber Security and Cyber Resilience for Stock Exchanges, Clearing Corporation and Depositories, and the IRDA has issued guidelines on Information and Cyber Security for Insurers, for cybersecurity protection of policyholders' information.

The Ministry of Power has created a CERT to mitigate cybersecurity threats in power systems, and four sub-CERTs for Transmission, Thermal, Hydro and Distribution to co-ordinate with power utilities.

The Intermediary Guidelines also impose an obligation on any intermediary to report cyber-incidents to the CERT-In.

### 6.2 Key Frameworks

The DP 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 – Information Security Management System – Requirements, such as ISO 27001 and the use of codes of best practices created by self-regulatory bodies.

Furthermore, the RBI has announced a project to implement the RBI's guidelines for information security using COBIT 5 standards.

### 6.3 Legal Requirements

The DP Rules require body corporates to have a comprehensive documented information security programme and security policies containing managerial, technical, operational and physical security measures.

There is no statutory requirement under Indian data protection law to maintain an incident response plan.

The RBI requires banks to have a written incident response programme and cybersecurity policy to handle cyber threats, 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 also requires insurers to have an incident response plan.

The DP Rules provide for the appointment of a grievance officer to redress the information-provider's grievances expeditiously.

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 shall report any incident directly to the bank's head of risk management.

The IRDA also requires the appointment of a CISO for implementing a cybersecurity framework.

NCIIPC guidelines recommend that all CIIs have an information security department headed by a CISO.

The RBI and IRDA guidelines provide for involvement of the board of directors to approve the cybersecurity policy and cyber-crisis management plan and to take overall responsibility for the information security governance framework.

The DP 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.

Similarly, the IRDA cybersecurity policy recognises the need for testing programmes, vulnerability assessments and penetration tests.

India does not have an insider threat programme or standards under its current data protection framework.

The DP Rules do not have any provisions for vendor/service-provider due diligence or monitoring. However, sectoral guidelines on outsourcing and cloud services by the IRDA, TRAI and RBI incorporate guidance for companies and banks to carry out due diligence, audits and regular monitoring on vendors and service-providers.

The DP Rules do not prescribe any training requirements. The CERT-In provides for training of technical know-how to stakeholders and other entities. Furthermore, the RBI and IRDA prescribe appropriate training and security awareness to human resources on cybersecurity policies and programmes.

### 6.4 Key Multinational Relationships

***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.

Similarly, India has signed MoUs with Australia, Bangladesh, Indonesia, Kenya, Portugal, Serbia, the UAE, Vietnam, France, Malaysia, Mauritius, Qatar and Singapore, inter alia, on cybersecurity co-operation.

Furthermore, India has signed mutual legal assistance treaties (MLAT) with approximately 35 countries to establish cross-border co-operation for access to data in different jurisdictions.

### 6.5 Key Affirmative Security Requirements

The DP Rules require all body corporates to implement reasonable security practices and standards, and to document their security programmes and policies.

The RBI requires banks to classify data based on business complexity and risk levels, and the sensitivity criteria of a bank. Similarly, the IRDA cybersecurity policy provides that systems should be classified under categories based on criticality and severity.

The NCIIPC guidelines recommend that all CIIs have an information security department headed by a CISO, and all cybersecurity breach incidents must be reported to the NCIIPC.

There are no specific provisions relating to denial of service (DoS) attacks under the ITA or the DP Rules. The NCIIPC guidelines and the sectoral cybersecurity guidelines prescribe preventive and corrective measures when addressing DoS attacks and similar attacks on systems. The implementation of such security measures is debatable, considering the numerous ransomware attacks on Indian systems in the past couple of years.

The CERT-In Rules and sectoral guidelines prescribe physical as well as network security measures for corporate data and systems.

### 6.6 Data Breach Reporting and Notification

The DP Rules define cyber-incidents 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."

The terms 'cyber-incident' and 'cybersecurity breaches' are also defined under the CERT-In Rules.

Cybersecurity incidents prescribed under the CERT-In Rules must be mandatorily 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/spyware;
- attacks on servers such as databases, mail 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 application such as e-governance, e-commerce, etc.

The PDP Bill also defines personal data breaches and mandates data fiduciaries to report any personal data breach that may cause harm to the data principal to the DPA.

The CERT-In incident reporting process requires providing information such as time of incident, sector, information on the affected system, type of incident, symptoms observed, and the relevant technical information including security systems deployed, mitigation measures taken, etc.

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

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

There is no specific statutory provision that applies to the IoT. Please refer to section 35(v).

Incidents specified under the CERT-In Rules must be mandatorily reported to CERT-In. 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.

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

### 6.7 Ability to Monitor Networks for Cybersecurity

The relevant laws in India that regulate the monitoring and interception of data are:

- the ITA;
- the Interception Rules;
- the DP Rules;
- the CERT-In Rules;
- 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 DP 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 addition, India does not have any specific laws relating to employee monitoring and thus companies can monitor their networks and servers.

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 the to the DoT.

**ANA Law Group**

Indiabulls Finance Centre
Tower-2, 11th Floor, 1103
Elphinstone Road
Mumbai – 400 013

Tel: +91 22 6112 8484
Fax: +91 22 6112 8485
Email: mailbox@anaassociates.com
Web: www.anaassociates.com

ANA LAW GROUP
ANOOP NARAYANAN & ASSOCIATES

### 6.8 Cyberthreat Information Sharing Arrangements

There is no statutory provision mandating the sharing of cybersecurity information with the government.

Indian laws do not restrict or mandate any individual/body corporate to share voluntarily any information regarding cyber-threats with government agencies.

### 6.9 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation

India has reportedly seen a 10% rise in cyber-attacks in 2018, as compared to approximately 53,000 cases reported the year before. Cyber-attacks have caused significant financial loss of around USD500,000 to Indian companies in the last 12 to 18 months. Only 5% of cyber-attacks are estimated to be reported to the authorities.

A major cyber-attack in India was that on Cosmos Bank, where the hackers launched a malware attack and siphoned off almost USD13,151,300, transferring the money to a bank account in Hong Kong. In another instance, the offenders used SIM cards to siphon off approximately USD550,000 from the bank accounts of almost 30 individuals as well as some companies. In July 2018, hackers hacked into Canara Bank ATM servers and stole almost USD30,000 from 50 different bank accounts.

Additionally, more than 20,000 websites have been hacked, including many government websites.

### 6.10 Other Significant Issues

India is set to enforce the PDP Bill. The government and organisations will rely on trends such as machine learning and artificial intelligence for cybersecurity solutions, anomaly detection and response, and on IoT infrastructure for automation and efficiency, specifically for the CII. Concepts such as blockchain to prevent data theft may also be in demand.

However, the skills needed to deal with continually changing cyber-threats are evolving and India is facing a shortage of cybersecurity skills in the workplace. There are 2.9 million vacant cybersecurity positions, a significant increase from the previous year. In this scenario, government initiatives such as Project Cyber Shikshaa for training women engineering graduates in the niche field of cybersecurity seem optimistic.