Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering comparative analysis from top-ranked lawyers

Data Protection & Privacy

India: Law & Practice

Anoop Narayanan and Priyanka Gupta
ANA Law Group

practiceguides.chambers.com

2021

INDIA

Law and Practice

Contributed by:
Anoop Narayanan and Priyanka Gupta
ANA Law Group see p.18

Contents

1. Basic National 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 right 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).

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 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 and passwords.

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. Consequently, the draft Personal Data Protection Bill 2019 (PDP Bill) was introduced. The PDP Bill intends to be applicable to any processing of personal data by the government, any Indian company, any citizen of India or any person or body of persons incorporated or created under Indian law. It also extends to foreign data fiduciaries and data processors processing personal data involving any business carried on in India, offering goods or services to data principals in India or profiling 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 protection authority as yet. The ITA mandates the central government to appoint an adjudicating officer to conduct an inquiry for injury or damages for claims valued up to INR5 crore (approximately USD700,000). 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).

Some of the sector-specific regulators are set out below.

Banking Sector

The Reserve Bank of India (RBI) governs both public and private sector banks. The RBI's guidelines allow it to request an inspection, at any time, of any of the banks' cyber-resilience capabilities. The RBI has set up a Cyber Security and Information Technology Examination (CSITE) Cell of the Department of Banking Supervision, to periodically assess the progress made by banks in the implementation of the Cyber Security Framework in Banks (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 setting up an online portal to investigate and address cybersecurity concerns and complaints.

In March 2020, the RBI also issued Guidelines on Regulation of Payment Aggregators and Payment Gateways, directing payment aggregators to put in place adequate information and data security infrastructure as well as systems for the prevention and detection of fraud, and has specifically recommended the implementation of data security standards and best practices such as PCI-DSS, PA-DSS, latest encryption standards, transport channel security, etc. Payment aggregators must establish a mechanism for the monitoring, handling and following-up of cybersecurity incidents and breaches, and are obliged to report incidents to RBI and the Indian Computer Emergency Response Team (Cert-In), an office within MeitY.

The RBI regularly conducts audits and enquiries into banks' security frameworks, and has imposed penalties on banks for non-compliance with the RBI's cybersecurity framework for banks. For instance, in the past couple of years, the RBI has imposed monetary penalties on several banks including INR3 crore (approximately USD421,000) on SBM Bank (India) Ltd., INR1 crore (approximately USD140,000) on the Corporation Bank and INR1 crore (approximately USD140,000) on the Union Bank of India, for non-compliance with certain RBI directions including non-compliance with the CSF.

Insurance Sector

The Insurance Regulatory and Development Authority of India (IRDAI) conducts regular onsite and offsite inspections of insurers to ensure compliance with the legal and regulatory framework. In addition, the IRDAI's guidelines on Information and Cyber Security for Insurers (IRDAI Cyber Security Policy) was updated in December 2020, requiring vulnerability assess-

ments and penetration testing annually and closing any identified gaps within a month. Some other relevant guidelines issued by the IRDAI include the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations 2017, the 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.

Telecoms Sector

Telecoms operators are governed by regulations laid down by regulatory bodies including:

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

Furthermore, the Unified Access Service Licence (UASL) extends information security to the telecoms 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.

In September 2020, the TRAI 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).

Securities

The Securities Exchange Board of India (SEBI) has issued detailed guidelines to market infrastructure institutions to set up their respective cybersecurity operation centres and to have their operations overseen by dedicated security analysts. The cyber-resilience framework has also been extended to stock-brokers and depository participants.

Recently, in July 2020, SEBI signed a formal Memorandum of Understanding with the Central Board of Direct Taxes (CBDT) for data exchange between the two organisations, on an automatic and regular basis. SEBI and the CBDT will also exchange any information available in their respective databases, for the purpose of carrying out their functions under various laws.

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 with the data protection laws;
- register data fiduciaries;
- conduct inquiries into, and adjudicate on, 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 the PDP Bill propose the appointment of a data protection officer (DPO) to address data principals' grievances. In December 2020, the Ministry of Health and Family Welfare approved a health data management policy (HDM policy) largely based on the PDP Bill to govern data in the national digital health ecosystem. The HDM policy, similarly to the PDP Bill, recognises entities such as data fiduciaries and data processors and establishes a consent-based data sharing framework.

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 USD700,000). 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 offence rather than mere contravention, and entails punishment greater than a financial penalty, the officer will transfer the case to the Magistrate having jurisdiction.

The first appeal from an adjudicating officer's decision can be filed before the Telecoms Disputes Settlement and Appellate Tribunal (TDSAT), and the subsequent appeal before the High Court.

The PDP Bill prescribes filing the complaint before a 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 PDP Bill also prescribes imprisonment of up to three years and/or a penalty of up to INR200,000 (approximately USD2,800) against any persons who knowingly or intentionally, and without the consent of the data fiduciary, re-identify personal data which has been de-identified by a data fiduciary/data processor, or re-identify and process such personal data. The aforesaid offences under the PDP Bill are cognisable (ie, the police have the power to arrest the offender without a court warrant) and non-bailable.

The PDP Bill proposes that the central government 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 EU data protection law. However, the expert committee has adopted a nuanced approach in drafting the PDP Bill. In several respects, the PDP Bill is aligned with the General Data Protection Regulation (GDPR). For instance, "personal data" is as broadly defined under the PDP Bill and includes any data relating to a natural person, directly or indirectly identifiable. The PDP Bill also introduces the concepts of "data fiduciary" and "data principal", similar to "data controller" and "data subject" under the EU's GDPR. The PDP Bill includes similar principles relating to the processing of personal data such as lawfulness, fairness, and transparency, purpose limitation, data minimisation, accuracy or quality of data, storage limitation, integrity and confidentiality, and accountability. Additionally, it includes the concepts of right to confirmation and access to data, the right to be forgotten, the right to correction or erasure of data, right to data portability, right to withdraw consent and so on, similar to the GDPR.

However, unlike the GPDR, the PDP Bill mandates data localisation. Furthermore, the PDP Bill does not grant individual rights in respect of automated decision-making or profiling (except for minors), as prescribed under the GDPR. The PDP Bill does not recognise joint controllers' agreements or obligations. However, the concept is to some extent recognised in the PDP Bill, such as in liability provisions and definition of data fiduciary.

The PDP Bill does not contain concepts comparable to the GDPR's "performance of a contract" or "legitimate interests" as the basis for personal data processing, and mandatorily requires consent for processing the personal data, except for grounds such as performance of government-authorised functions, for purposes relating to employment/recruitment, and for other government-defined purposes.

1.5 Major NGOs and Self-Regulatory Organisations

The major data privacy non-governmental organisations (NGOs) and industry self-regulatory organisations (SROs) 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);
- the National Cyber Safety and Security Standards (NCSSS), a self-governing body to protect critical information infrastructure (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 producers, and internet service providers (ISPs) in India, which interacts directly with ministries, policymakers, 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 the internet and digital technologies from policy and academic perspectives.

1.6 System Characteristics

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

1.7 Key Developments

Leading Cases

In April 2020, the Kerala High Court restricted the government from sharing citizens' sensitive personal data with a US-based data analysis company, unless the data was anonymised. The court also recognised the importance of data subjects' informed consent prior to collecting their personal data and the safeguards to ensure confidentiality of the data collected.

In November 2020, Odisha High Court observed the importance of the right to be forgotten of an individual and how it remains unaddressed in legislation. The case involved objectionable content posted online regarding a woman, and the court encouraged the victim to seek an order for the protection of her fundamental right to privacy even in the absence of an explicit right to be forgotten.

General Data Developments

During 2020, the government banned more than 200 mobile applications within the country based on the comprehensive reports received from the Indian Cyber Crime Coordination Centre citing unauthorised exports and the threat to the country's sovereignty, integrity, and national security.

India witnessed a tremendous increase in cybercrime and data breach incidents in 2020. One of the world's largest IT services providers, Cognizant, also became a victim of Maze ransomware that caused disruption to its clients.

MEITY constituted the Non-Personal Data Committee, which released its report on the non-personal data governance framework for public comment. The report specifies that only anonymous data will fall under the non-personal data framework.

Transport and Drones

The Ministry of Road Transport and Highways published the Motor Vehicle Aggregator Guidelines 2020 (MV Guidelines) in November 2020 to regulate transport aggregators, regulation of fares, compliances by vehicles, apps and websites, ride-sharing, safety measures and ride cancellations.

In November 2020, the Ministry of Civil Aviation released a draft National Unmanned Aircraft System Traffic Management Policy recommending robust data privacy and data security mechanisms relating to data collected by unmanned drones for both commercial and non-commercial purposes.

Finance

In August 2020, NITI Aayog (the central government's policy think tank) released a draft framework on Data Empowerment and Protection Architecture (DEPA) to set up a mechanism for secure consent-based data sharing in the fintech sector.

The government has been working on draft e-commerce policy and proposes to set up an e-commerce regulator with broad powers over e-commerce entities and platforms.

In December 2020, the RBI released a statement proposing to issue the Digital Payment Security Controls Directions 2020, which will require regulated entities to set up a robust governance structure for digital payment systems as well as implement minimum security controls for internet, mobile banking, and card payments.

In September 2020, the RBI released cybersecurity plan for urban co-operative banks for 2020-2023, aiming at enhancing cybersecurity of urban co-operative banking sector against evolving IT and cyberthreats.

In June 2020, the RBI published its Oversight Framework for Financial Market Infrastructures and Retail Payment Systems to enable better regulatory compliance by payment system operators.

In February 2021, the RBI issued a statement proposing guidelines to regulate outsourcing in payment systems, primarily to optimise efficiency, lower costs, and eliminate vulnerabilities and cybersecurity risks.

The Minister of Finance has recently clarified that all entities regulated by the RBI are advised not to deal in virtual currencies or provide services to facilitate the same.

TRAI Recommendations

In September 2020, the TRAI 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 (CSPs).

The TRAI released its recommendations on a Regulatory Framework for Over-The-Top (OTT) Communication Services, stating that, currently, there is no need for regulatory intervention in relation to the privacy and security of OTT services, and the framework may be considered after receiving clarity from other jurisdictions.

1.8 Significant Pending Changes, Hot Topics and Issues

The PDP Bill

The PDP Bill was introduced in the lower house of the Indian Parliament (*Lok Sabha*) on 11 December 2019, and was immediately referred to a Joint Parliamentary Committee for further debate and examination on 12 December 2019. The government had directed the Parliamentary Committee to provide its report to the *Lok Sabha* by February 2020.

However, reportedly, the Joint Parliamentary Committee is proposing to expand the scope of the PDP Bill to "encompass overall data protection" and non-personal data. Furthermore, the deliberations over the key issues of data localisation and government access to data shared on social media platforms, are ongoing, and the possibility of further amendments to the PDP Bill cannot be eliminated.

This may lead to some delays in finalising the new comprehensive law.

After the PDP Bill is notified as law, the RBI may strengthen the enforcement of its data localisation mandate for payment-related data to be stored within India only.

Data Security and Tech Giants

The SCI has issued notices to the RBI, Google LLC, Amazon.com, Inc., WhatsApp Inc., and Facebook, Inc. in a petition requiring the tech companies ensure data security and implement data localisation measures before using the Unified Payments Interface (UPI) over data security concerns. It will be interesting to note the apex court's view on the applicability of the RBI's data localisation requirements on these tech companies and the data security mandates imposed on them.

Spam, Malware, Etc

Reportedly, there were more than 900,000 spam messages, 700 malware attacks, and 48,000 malicious domains within the first four months of 2020, mostly related to COVID-19. The surge in e-commerce and digital payments in 2021 will be consistent across the country. This exponential rise may deepen concerns about potential data breach risks for consumers and businesses, as well as new kinds of data security breaches. Additionally, with remote working becoming a norm, such risks may continue until combined efforts are taken by the stakeholders, users, and the government.

Government Policy

The government's e-commerce policy that proposes the setting up of an e-commerce regulator with broad powers over e-commerce entities and platforms.

The government is working towards updating its national cybersecurity strategy to improve its position in cyberspace. The updated policy may be issued in 2021.

The government's health data management (HDM) policy will have a significant impact on the medical and pharmaceutical industry once implemented, as healthcare institutions will have increased compliance obligations. However, as the HDM policy has significant overlaps with the PDP Bill, it may cause a conflict and it remains to be seen which will prevail.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

DP Rules

General requirements under the DP Rules include the following.

- A company handling personal data or sensitive personal data (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 their 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 purposes for which information is collected, the intended recipients of that information, the agency collecting and retaining the information, etc (furthermore, the data provider must be given the option to not provide the information, or revise or withdraw the information).
- Entities holding SPD should not retain the information for longer than is required for the purpose for which it was collected or lawfully used.
- The transfer of SPD within or outside India is only permitted with restrictions, such as that:
  - (a) the recipient entity ensures adherence to the same level of data protection and that the transfer is necessary to comply with a lawful contract; or
  - (b) the data provider has given prior consent.
- Companies must have "reasonable security practices and procedures".
- Companies must appoint a grievance officer and address complaints in a timely manner.

PDP Bill

The PDP Bill is not applicable to the processing of anonymised data (personal or non-personal). The principles relating to the processing of personal data include:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy or quality of data;
- storage limitation;
- integrity and confidentiality;
- accountability;
- notice; and
- consent.

The legal bases for processing personal data include the following.

- Consent (Sections 5(b) and 11).
- Performance of any state-authorised function.
- Compliance with any law currently in force.
- Compliance with any order or judgment of any court or tribunal in India.

- Purposes related to employment (excluding the matter related to sensitive personal data).
- The reasonable purposes as notified by the government or the DPA, including:
  (a) prevention and detection of any unlawful activity including fraud;
  (b) whistle-blowing;
  (c) mergers and acquisitions;
  (d) network and information security;
  (e) credit scoring;
  (f) recovery of debt;
  (g) processing of publicly available personal data; or
  (h) the operation of search engines.
- Notice must be provided to the data principal at the time of collection of the personal data containing the prescribed information.

The data principals' rights include:

- the right to confirmation and access;
- the right to correction;
- the right to erasure;
- the right to data portability;
- the right to be forgotten; and
- the right to withdrawal of consent – the data principal may give or withdraw his or her consent to the data fiduciary through a consent manager (appointed by the data fiduciary and registered with the DPA).

A significant data fiduciary (those notified by the DPA) must carry out a data protection impact assessment when it intends to undertake any processing of personal data, which involves:

- new technologies;
- large scale profiling;
- use of sensitive personal data, such as genetic data or biometric data; or
- any other processing which carries a risk of significant harm to data principals.

DPOs

The DP Rules do not provide for the appointment of data protection officers (DPOs). However, the PDP Bill provide for the appointment of DPOs by data fiduciaries possessing the qualifications prescribed under the regulations for carrying out the functions prescribed in the PDP Bill. The DPO must be based in India and must represent the data fiduciary under the PDP Bill. The data fiduciary may assign any other function to the DPO that it may consider necessary.

Authorised Data Collection and Processing

Under the DP Rules, bodies corporate must seek the data provider's consent before the collection, transfer or 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, this requirement is exempted in cases where government agencies require the individual's SPD for identity verification or for the prevention, detection, investigation, prosecution and punishment of offences.

The legal bases for processing personal data under the PDP Bill include the following.

Consent – it must be free, informed and specific to the purpose of processing as well as clear and capable of being withdrawn.

Performance of any state-authorised function.

Compliance with any law currently in force.

Compliance with any order or judgment of any court or tribunal in India.

Purposes related to employment (excluding the matter related to sensitive personal data).

Reasonable purposes as notified by the government or DPA, such as the following:

- prevention and detection of any unlawful activity including fraud;
- whistle-blowing;
- mergers and acquisitions;
- network and information security;
- credit scoring;
- recovery of debt;
- processing of publicly available personal data; and
- the operation of search engines.

Privacy by Design and Default

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

- provision of 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 only so long as that purpose gets fulfilled.

The PDP Bill specifically provides that data fiduciaries must prepare a privacy design policy, containing the following.

- The managerial, organisational and technical systems (as well as business practices) designed to anticipate, identity and avoid harm to the data principal.
- The obligations of data fiduciaries.
- The technology used in the processing of personal data in accordance with commercially accepted or certified standards.
- Provisions and procedures ensuring:
  (a) that the legitimate interests of businesses, including any innovation, are achieved without compromising privacy interests;
  (b) the protection of privacy throughout the processing, from the point of collection to deletion, of personal data;
  (c) the processing of personal data in a transparent manner; and
  (d) that the interest of the data principal is accounted for at every stage of processing.
- Subject to the PDP regulations, the privacy by design policy may require certification from the DPA.

The certified privacy by design policy must be published on the data fiduciary's and the DPA's websites.

Privacy Impact Analysis

The current 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 SPD that has a risk of causing significant harm to data principals.

Upon completion of the DPIA, the DPO must review the assessment and submit the assessment report to the DPA.

On receipt of the assessment and its review, if the DPA has reason to believe that the processing is likely to cause harm to the data principals, it may direct the data fiduciary to cease such processing or impose conditions, as it may deem fit.

Privacy Policies

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

Data Provider Rights

The DP Rules grant the right to the data providers to review, edit and update their personal data, and to withdraw their consent to personal data provision.

The PDP Bills grants additional rights to data principals including:

- the right to confirmation and access;
- the right to correction;
- the right to erasure;
- the right to data portability;
- the right to be forgotten; and
- the right to withdrawal of consent – the data principal may give or withdraw his or her consent to the data fiduciary through a consent manager (appointed by the data fiduciary and registered with DPA).

Anonymisation, De-identification and Pseudonymisation

The current 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 the processing of both anonymised and pseudonymised data.

The PDP is not applicable to the processing of anonymised data (personal or non-personal). However, the PDP will be applicable to anonymised data (personal or non-personal) collected by the central government from a data fiduciary to enable better targeting of services or formulation of evidence-based policies.

The PDP Bill also requires the data fiduciary and data processor to implement appropriate security safeguards for data pseudonymisation (de-identification) and encryption. It proposes that re-identification of de-identified data without the data fiduciary's consent shall be a punishable offence.

Emerging Technologies

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 in **2.2 Sectoral and Special Issues**, the PDP Bill addresses some of these issues.

Harm

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 and privacy policy 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 and Special 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 identifiers, 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 SPD can be processed based on explicit consent; for the function of the government; if mandated by law; or if certain SPD is strictly necessary to respond to any medical emergency, disaster or outbreak of disease that may threaten public health.

Financial Data

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

The CIC Act and CIC Regulations primarily apply to credit information companies; recognise them as data collectors; require that they ensure data security and secrecy; and require that they adhere to privacy principles in respect of data collection, use, disclosure, 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 – provide privacy and customer confidentiality obligations that must 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.

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

Health Data

Data protection laws in respect to health data are inadequate in India. The PDP Bill categorises "health data" as sensitive personal data, and defines it as the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of that data principal; data collected in the course of registration for, or provision of, health services; and data associating the data principal to the provision of specific health services. Health data cannot be processed or transferred without obtaining the data principals' consent, unless for the exceptional grounds specified under the PDP Bill.

Additionally, 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 government 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. Further, the DP Rules recognise health information as SPD, and thus, regulate its collection, use and disclosure. However, as the DP Rules apply only to bodies corporate, 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 man-

dated under a law or where 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.

The HDM policy discussed in **1.2 Regulators (Health Sector)** will have a significant impact on the medical and pharmaceutical industry once implemented, as healthcare institutions will have increased compliance obligations. However, as the HDM policy has significant overlaps with the PDP Bill, it may cause a conflict and it remains to be seen which will prevail.

Communications Data

Although there are multiple telecoms laws, data protection norms in the telecoms sector are primarily governed by the UASL issued to telecoms 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 if the disclosure is in accordance with the terms of such consent.

Some of the key TRAI recommendations concerning TSPs include:

- the user being the owner of his or her data, and data processors being mere custodians;
- entities in the digital ecosystem refraining from using metadata 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;
- telecoms 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 and the TRAI recommendations propose to regulate data privacy issues relating to the internet in India.

Voice Telephony

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.

Children's Data

Current Indian data privacy law does not address privacy issues specifically 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 the processing of children's personal data and to protect and advance the child's rights and best interests. The data fiduciary is barred from profiling, tracking or behaviourally monitoring, or targeting advertising directly at, children and undertaking any other processing of personal data that could cause significant harm to the child.

Employment Data

Currently, India does not have any specific law to deal with workplace privacy or, protection of employee data, etc. Please refer to **2.4 Workplace Privacy** for further discussion.

Internet, Streaming and Video Issues

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

There are no specific provisions under the current law regarding browsing data, viewing data, cookies and beacons, or location data. The current Indian data protection framework does not provide for any "do not track" mechanisms nor does it regulate behavioural advertising; however, the proposed PDP Bill prohibits tracking of personal data of minors by data fiduciaries and categorises behavioural characteristics as SPD, and also prohibits behavioural monitoring and/or advertising in respect of minors.

Social media, search engines and large online platforms

Critical data privacy issues relating to social media, search engines, online platforms and the like are not adequately governed under the current Indian law.

The PDP Bill has incorporated provisions regulating social media intermediaries. The PDP Bill provides that the government can notify a social media intermediary as a "significant data fiduciary" and subject it to additional obligations under the PDP Bill. A social media intermediary with users above such threshold as may be notified by the central government – and whose actions have, or are likely to have, a significant impact on electoral democracy, the security of the state, public order or the sovereignty and integrity of India – can be notified as a significant data fiduciary.

Telecoms and network service providers, such as web-hosting service providers, search engines and online platforms are defined as "intermediaries" under the ITA. Furthermore, the MeitY proposes to include social media companies as intermediaries. The ITA and intermediaries' guidelines prescribe certain obligations on intermediaries, including:

- compliance with all the data privacy principles prescribed by the DP Rules;
- compliance with government directions relating to blocking data access to the public;
- monitoring and collecting data through any computer resource;
- publishing the rules and regulations, privacy policy and user agreement for access or usage of the computer resource by any person;
- not hosting or publishing any information or initiating the transmission of restricted content;
- informing its users of non-compliance consequences; and
- promptly reporting cybersecurity incidents to the CERT-In.

Addressing hate speech

The publication of hate speech, abusive material and political manipulation is regarded as an offence under the ITA, and punishable with imprisonment extending up to three years, and/or a fine.

Other Issues

Data subject rights

The DP Rules provide that the data subject must be given the option to not provide their information, or revise or update that information, or withdraw his or her consent at any time.

The PDP Bill Grants the following rights to the data subjects:

- the right to confirmation and access;
- the right to correction;
- the right to erasure;
- the right to data portability;
- the right to be forgotten; and
- the right to withdrawal of consent.

Right to be forgotten

The DP Rules do not provide 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 the 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.

Data portability

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

Right of rectification or correction

The DP Rules grant the right to the data providers to review, edit and update their personal data. The PDP Bill also provides the data subject with the right to request correction or erasure of their personal data which is no longer necessary for the purpose for which it was initially processed. The data fiduciary must take necessary steps to notify all third parties to whom such personal data is disclosed.

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 SMSs, based on a customers' preferences where they can register themselves under the fully blocked category or the partially blocked category. The TRAI has formed a Do-Not-Call Registry where customers can register to prevent any unsolicited calls or SMSs. The Regulations impose penalties of up to INR250,000 (approximately USD3,563) for any non-compliance.

Please refer to **2.2 Sectoral and Special Issues** (Internet, Streaming and Video Issues) for information on constraints on behavioural advertising.

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 recruitment or termination;
- to provide any service or benefit;
- to verify employee attendance; or
- to accurately assess an employee's performance.

The need for employee consent can be dispensed with if it involves a disproportionate effort by the employer considering the nature of the processing activities. Nevertheless, consent is required to process employees' sensitive personal data.

The current Indian law does not prohibit or restrict the camera surveillance, or the monitoring, of employees' office e-mails, telephone calls and data on office devices provided, such activities are reasonable and do not violate the 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 the employment laws.

Whistle-Blowing

The PDP Bill permits the processing of personal data without consent if such processing is necessary for the purposes of whistle-blowing.

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 whistle-blowers. However, a major shortfall is that a whistle-blower must disclose his or her identity in the complaint.

Furthermore, the Companies Act, 2013, mandates that certain publicly listed companies 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.

There is no specific legal provision with regard to e-discovery issues and no prohibition against deploying digital loss prevention tools or 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, having 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 that causes wrongful loss or wrongful gain to any person, is liable to pay damages, not exceeding INR5 crores (approximately USD700,000) to the person so affected. Cases involving damages of more than INR5 crores are brought before the competent civil court.

The adjudicating officer can either grant either 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 USD360).

PDP Bill Enforcement Penalties

A data fiduciary's non-compliance with a data principal's request can attract a penalty of INR5,000 (approximately USD60) for each day, subject to a maximum of INR1 million (approximately USD14,100) in the case of "significant" data fiduciaries and INR500,000 (approximately USD70,000) in other cases.

A data fiduciary's failure to take prompt and appropriate action against breaches is punishable with a penalty of INR50 million (approximately USD704,000) or 2% of its total worldwide turnover in the preceding financial year, whichever is higher.

The penalty for wrongful data processing or for breach of security safeguards, and unauthorised transfer will be INR150 million (approximately USD2.1 million) or 4% of its total worldwide turnover in the preceding financial year, whichever is higher.

Failure to report a data breach to the DPA will attract penalty of INR10,000 (USD140) for each day, subject to a maximum of INR2 million (approximately USD28,000) in the case of a significant data fiduciary and INR500,000 (approximately USD70,000) in other cases.

Non-compliance with the DPA's directions will trigger a penalty of up to INR20,000 (USD281) for each day, subject to a maximum of INR20 million (approximately USD280,000).

Certain additional offences under the PDP Bill are cognisable and non-bailable.

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.

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 its law enforcement agencies) has wide powers under various laws 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 governs interception of telephone 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;
- 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 the law;
- the mass surveillance programme, Centralized 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, integrity and state security; and
- the PDP Bill.

Government agencies can unilaterally authorise, 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, the UASL, etc, as well as the CMS (not yet fully operational).

3.3 Invoking Foreign Government Obligations

A foreign government's access request is not a legitimate basis to collect and transfer SPD. Providing SPD to a foreign government only becomes mandatory through an Indian court's 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 the 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.

India has not signed a Cloud Act agreement with the USA and also will not qualify for its criteria until it notifies its PDP Bill and enacts a stronger data privacy regime.

3.4 Key Privacy Issues, Conflicts and Public Debates

The RBI's mandatory payment data localisation requirement is the subject of much debate. Similarly, the data localisation provisions under the PDP Bill, which are not present in the GDPR, and their effective enforcement against and impact on multinational companies operating in India, are highly controversial.

Indian laws give expansive powers to the government to access data for reasons including intelligence gathering, anti-terrorism and national security. The SCI has directed the government to make laws to curb fake news and rumours 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.

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 to disable access within 24 hours to content deemed defamatory or a danger to national security. Intermediaries with above 50 lac (5 million) users must be incorporated in India and have a permanent, registered, physical address in India. These provisions have also resulted in public debate on the monitoring of 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

There are no statutory provisions under the current law prohibiting the overseas transfer of personal information. The DP Rules permit overseas data transfer subject to certain restrictions for SPD, such as:

- the recipient entity ensuring adherence to the same level of data protection (reasonable security practices are prescribed under the Rules) and only if the transfer of information is necessary to comply with a lawful contract; or
- with the prior consent of the data provider.

As regards the PDP Bill, there are restrictions on transfer of personal data outside India (Sections 33 and 34).

The sensitive personal data may be transferred outside India subject to certain conditions, however, the data should continue to be stored in India.

In addition, critical personal data must only be processed in India, subject to certain conditions, and any transfer must be reported to the DPA. The "critical personal data" is the personal data as may be notified by the central government.

4.2 Mechanisms That Apply to International Data Transfers

Besides the restrictions prescribed under the DP Rules, Indian law does not currently have any mechanism to apply to international data transfers.

4.3 Government Notifications and Approvals

Under the DP Rules, there are no government notifications or approvals required under Indian law to transfer data internationally.

However, under the PDP Bill, prior government approval will be required to transfer sensitive personal data and critical personal data, in addition to other conditions.

4.4 Data Localisation Requirements

The current Indian law on data privacy does not require data localisation. However, the RBI has mandated that payment system operators store the payment-related information of Indian citizens within India only. The RBI has further clarified that although the processing of payment transactions can take place outside India, the data must be deleted from the systems abroad and brought back to India within one business day or 24 hours from the payment processing, whichever is earlier, so that the data is stored only in India.

As regards data localisation under the PDP Bill, a copy of all SPD must be stored in India, although it may be transferred outside India, subject to conditions. Critical personal data (which will be defined by the central government) must be processed only in India, with certain exceptions.

4.5 Sharing Technical Details

There is no mandatory requirement under the current Indian law for the sharing of software code or algorithms or similar technical details with the government.

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.

In this regard, in April 2020, the Kerala High Court restricted the government from sharing citizens' sensitive personal data with a foreign aggregator, unless the data was anonymised. The court had also recognised the importance of the data subjects' informed consent prior to collecting their personal data and the safeguards to ensure confidentiality of the data collected.

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

There is a lot of debate on the ethical limits of the use of big data, and big data processing poses serious risks to privacy. In the absence of specific regulatory guidance, 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.

India's proposed law intends to address the accountability and obligations of data fiduciaries for processing personal data, which may also extend to big data.

Automated Decision-Making

The current Indian data privacy law does not deal with automated decision-making. The PDP Bill, however, recognises automated processing and decision-making, and defines "data" to include a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means.

The PDP Bill further provides that where the processing is carried out by automated means, the data principal shall have the right to receive the personal data in a structured, commonly used and machine-readable format, and the right of data portability of his or her personal data to any other data fiduciary.

Profiling

The DP Rules do not recognise profiling. The PDP Bill defines profiling as any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a data principal. The PDP Bill prohibits the profiling of minors' personal data and SPD. Further, the PDP Bill mandates data fiduciaries to carry out a DPIA before undertaking large-scale profiling of SPD that may pose significant harm to data principals.

Artificial Intelligence

Artificial intelligence (AI) is not dealt with under the current data privacy regime. However, reliance on AI is increasing significantly among organisations wishing to secure their networks and their data.

MEITY has constituted four committees for promoting AI initiatives and developing a policy framework. 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.

Internet of Things (IOT)

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.

Autonomous Decision-Making

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

Facial Recognition and Biometrics

There are no specific provisions under Indian data privacy or sectoral laws to address the privacy concerns arising from facial recognition technology. Some of 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, and thus, including it in the category of SPD.

Biometric data is categorised as SPD under the DP Rules as well as the PDP Bill, and its collection, processing and transfer is subject to the prescribed statutory restrictions. The PDP Bill defines "biometric data" as facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person. The PDP Bill prohibits processing of such biometric data as notified by the central government, unless such processing is permitted by law.

Furthermore, the PDP Bill requires data fiduciaries to carry out a DPIA prior to the processing of any SPD including biometric data, which may carry a risk of significant harm to data principals.

India's central government enacted the Aadhaar Act for the targeted delivery of financial benefits and subsidies to the underprivileged. The Aadhaar Act establishes an authority, the UIDAI, responsible for the administration of the Aadhaar Act. It also establishes a Central Identities Data Repository (CIDR), which is a database holding Aadhaar numbers and corresponding demographic and biometric information. Aadhaar is currently the largest database of biometrics globally.

Geolocation Data and Drones

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

The use of drones other than by government organisations was prohibited under Indian law prior to December 2018. However, the civil aviation regulator issued the Civil Aviation Requirements (Drone Regulations 1.0) in August 2018 with effect from December 2018 permitting the civil use of drones by non-government agencies, subject to the prescribed restrictions.

The Ministry of Civil Aviation has taken several initiatives in the past year to regulate and experiment with drones and their potential commercial uses.

The National Unmanned Aircraft System Traffic Management Policy recommending robust data privacy and data security mechanisms is expected to be released within the year.

5.2 "Digital Governance" or Fair Data Practice Review Boards

There is no statutory requirement to establish protocols for digital governance, or fair data practice review boards, in addition to those measures already required under the DP Rules or sector-specific laws.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

Sectoral audits, investigations and penalties are discussed in **1.2 Regulators**.

There has been no significant private litigation involving privacy or data protection in the past year although class actions, forms of collective redress and representative actions are permitted in India.

5.4 Due Diligence

There is no prescribed due diligence procedure with regard to data protection and privacy. The acquiring companies normally demand a target company's data privacy policies and framework, the annual audit reports on data security compliance, details of any breaches and reporting in that regard.

5.5 Public Disclosure

There is no specific legal provision requiring an organisation's mandatory disclosure of its cybersecurity risk profile or experience.

5.6 Other Significant Issues

There are no other major data privacy and protection issues not already addressed in this chapter.

ANA Law Group is a full-service law firm based in Mumbai, with a team of experienced professionals who have broad industry knowledge and who specialise in a wide spectrum of business areas. 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, consumer goods, healthcare, payroll-processing, pharmaceuticals, telecommunications, 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; regulatory requirement compliance; transfers of sensitive personal data within and outside India; security breaches and drafting security breach policies; international compliance projects; and prosecutions and offences.

Authors

Anoop Narayanan is the founder of ANA Law Group and has been in practice for more than 27 years. He has vast advisory and transactional experience in all areas of Indian law as well as being a distinguished employment, technology and intellectual property law expert. His clients include multinational corporations, law firms from around the world and Indian companies and individuals. Mr Narayanan is a member of the International Bar Association (IBA) and the American Bar Association (ABA) and is a regular speaker at both Indian and international conferences on his areas of practice; he has also published many articles in leading national dailies touching upon several areas of Indian law.

Priyanka Gupta is a senior attorney at ANA Law Group who has been in practice for more than 13 years. She qualified from a premier law school and has strong domain knowledge. Ms Gupta regularly advises on international TMT transactions and regulatory aspects of the Indian telecoms sector. She 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.

ANA Law Group

303 Madhava Premises
Bandra Kurla Complex
Bandra East
Mumbai - 400 051

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

ANA LAW GROUP
ANOOP NARAYANAN & ASSOCIATES