The Legal 500
Country Comparative Guides

India
TECHNOLOGY

Contributing firm
Trilegal

Nikhil Narendran
Partner | nikhil.narendran@trilegal.com

Jishnu Sanyal
Senior Associate | jishnu.sanyal@trilegal.com

Cheta Sheth
Associate | cheta.sheth@trilegal.com

Samvit Ganesh
Associate | samvit.ganesh@trilegal.com

This country-specific Q&A provides an overview of technology laws and regulations applicable in India.

For a full list of jurisdictional Q&As visit legal500.com/guides
1. What is the regulatory regime for technology?

The regime for technology regulation in India involves multiple legislations and regulatory bodies spread across the domains of data privacy and protection, media and content regulations, payment systems, telecommunications and broadcasting.

Information technology regulations in India

The Information Technology Act, 2000 (IT Act) is the primary legislation dealing with the protection of personal data and regulation of electronic transactions/communications in India. The IT Act provides a regulatory regime for internet intermediaries and framework for electronic transactions. The IT Act empowers the government to frame regulations for digital and electronic signatures, intermediary liabilities, interception and monitoring of electronic communications, website blocking, information requests, cyber security, etc.

Although, India does not have a specific data privacy law at present, the processing of personal information (PI) and sensitive personal information (SPI) is governed by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Data Privacy Rules) issued under the IT Act. The Data Privacy Rules impose restrictions on the collection of SPI without consent, information security standards and mandates publishing of a privacy policy.

The government has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules) in suppression of the Information Technology (Intermediary Guidelines), Rules, 2011 which mandate due diligence requirements to be followed by online intermediaries for availing the safe harbour exemption. The IT Rules regulate, inter alia: (a) intermediaries and social media intermediaries (including significant social media intermediaries); and (b) publishers of news and current affairs (NCA) and online curated content (OCC). The IT Rules introduce a new concept of social media intermediaries (SMI) as entities which primarily or solely enable online interaction between two or more users, and allows users to create, upload, share, disseminate, modify or access information using its services. Significant social media intermediaries (SSMI) have been defined as SMI’s with more than 5 million registered users and are required to comply with additional obligations such as appointment of key officers including a Grievance Officer, Chief Compliance Officer and nodal point of contact resident in India, publishing periodic reports containing details of the complaints received and addressed and enabling identification of the first originator of information as may be required by a judicial order. Publishers of NCA and OCC are required to comply with the Code of Ethics, adopt a self-regulating mechanism with three levels for redressal of grievances and making regular disclosures of the same. Several petitions have been filed before various High Courts challenging the constitutional validity of the IT Rules. The scope and ambit of the IT Rules will be clear once such litigations have been heard and resolved by the Courts.

The government has also framed the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009. These rules allow interception, monitoring and decryption of any information generated, transmitted, received or stored in any computer resource only when specifically mandated by the Government.

The Government has appointed the Indian Computer Emergency Response Team (CERT-In) for handling cyber security incidents and has notified the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (CERT-In Rules). The CERT-In serves as a national agency to perform the following functions in the area of cyber security:

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

The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (Blocking Rules) read along with the IT Act, empowers the Government to block public access to content that is deemed to be threatening the security of the State; the sovereignty, integrity or defence of India; friendly relations with foreign States; public order.

Personal Data Protection Bill

In the year 2017, India’s apex court recognised the privacy of individuals as a fundamental right under the Indian Constitution and highlighted the need for a privacy legislation. In response to this, the Government set up a committee of experts to look into the contours of a privacy legislation. The committee came up with a draft Personal Data Protection Bill (2018 Bill) after country-wide consultations, which was released in the year 2018. After the 2018 Bill, the Government conducted a series of consultations and a revised Bill (PDP Bill) was released in December 2019. The PDP Bill has undergone further stakeholder consultations and is currently placed before a joint parliamentary committee (JPC) for examination. The JPC had been granted an extension till the monsoon session of the Parliament to submit its report. In a press conference on the preparation for the monsoon session of the Parliament, it was agreed not to grant further extensions to the JPC to submit its report on the PDP Bill. Therefore, we expect the report to be presented before the Parliament in the monsoon session commencing from 19 July 2021.

Regulation of Non-personal data (NPD)

The Ministry of Electronics and Information Technology (MEITY) constituted a committee of experts (NPD Committee) in September 2019, to devise a framework to regulate non-personal data (NPD). The Committee released its report (NPD Report) on 12 July 2020 for public consultation / feedback. The NPD Report proposes the introduction of a legislation governing NPD (NPD Legislation) and lays down key principles to be incorporated in the NPD Legislation such as localization of certain categories of NPD, mechanisms for data sharing, purposes for data sharing and regulation of data of certain key businesses classified as ‘Data Businesses’.

The NPD Report also proposes the establishment of an NPD Authority (NPDA) to enforce the NPD Legislation.

The primary objectives of regulating NPD are to incentivise innovation and encourage start-ups, make community and public data available for social/public/economic value creation, and address privacy concerns from processing NPD. This is a distinctive move given that most other nations, including the European Union (EU), primarily regulate the flow of NPD between countries. The NPD Legislation would be one of the first to govern the collection and processing of NPD within a jurisdiction.

Pursuant to the public feedback and suggestions received on the NPD Report, the NPD Committee released a revised version of the report in December 2020 (Revised Report), for another round of public consultation. The Revised Report has inter alia clarified the definition of NPD, application of the PDP Bill vis a vis the NPD Legislation in relation to the overlapping provisions and proposes a data sharing mechanism for NPD. The Revised Report also contains suggestions for introducing a technology architecture for sharing of NPD.

Telecom regulatory regime in India

The telecommunications services sector in India is regulated by the Department of Telecommunication (DoT) and the Telecom Regulatory Authority of India (TRAI) set up under the Telecom Regulatory Authority of India Act, 1997 (TRAI Act). The DoT is the government agency that issues telecom licenses, makes communications policy and manages spectrum allocations. The TRAI is an independent regulatory body tasked with making recommendations on key policy issues in telecom. They have the additional mandate to make regulations regarding quality of service, consumer protection, interconnection and tariff. TRAI also issues orders and directions to ensure compliance with license conditions.

The primary legislation for this sector is the Indian Telegraph Act, 1885 (the Telegraph Act) which governs the establishment, maintenance and working of telecom equipment and networks in India. In addition, the Wireless Telegraph Act, 1933 (WTA) regulates wireless equipment and wireless networks.

The Telecom Disputes Settlement Authority of India (TDSAT) has the powers to adjudicate disputes between licensors, licensees, service providers and consumers.

Spectrum Management

Spectrum management is the domain of the Wireless Planning and Coordination wing (WPC) of the DoT, along
with the Standing Advisory Committee on Frequency Allocation (SACFA). SACFA is an inter-ministerial body that is tasked with taking policy decisions about spectrum allocation and management. SACFA comprises representatives from the Defence Ministry, Airport Authority, Home Ministry, Wireless Department and DoT. The WPC also handles the certification of all wireless products and their imports. The DoT also introduced a Simplified Application for Registration and Licenses ‘Saral Sanchar’ Portal for facilitating a paperless mechanism for grant of Unified License (UL), Unified License (Virtual Network Operator) (UL(VNO)), registrations for PM – Wi-Fi Access Network (PM-WANI) and WPC clearances.

Broadcasting

The Ministry of Information and Broadcasting (MIB) oversees and regulates broadcasting services in India. Broadcasting services include content services and carriage services. The MIB grants licenses and regulates both categories. License is required for operating (i) Community Radio Stations; (ii) private FM channels; (iii) Teleports and satellite TV Channels; (iv) Headend-in-The-Sky broadcasting services; (v) Direct-To-Home broadcasting services; (vi) cable company services.

Other Service Providers

Entities providing voice based Business Process Outsourcing (BPO) services are known as Other Service Providers (OSP) and are governed under the OSP guidelines. Earlier, the Terms and Conditions for OSPs issued by the DoT imposed stringent conditions such as registration and furnishing bank guarantees. This was replaced with the Guidelines for OSP dated 5 November 2020 in a progressive overhaul to the Business Process Outsourcing (BPO) sector. The OSP Guidelines have been further revised on 23 June 2021 (OSP Guidelines) to provide additional relaxations and clarity with respect to some definitions. The OSP Guidelines remove onerous registration requirements, audit and penalty provisions, restrictions on infrastructure sharing and content monitoring. Broadly, the OSP Guidelines are applicable to entities providing voice-based services such as call support services, help desks or support centres and exclude non-voice or data-based BPOs. The OSP Guidelines now prescribe various networking related conditions with respect to interconnection, carriage of traffic, use and sharing of Electronic Private Automatic Branch Exchange (EPABX), etc.

Equipment standards and regulation

The DoT is also assisted by the Telecommunication Engineering Centre (TEC) in approving hardware and infrastructure equipment used in telecom operations. Consumer electronic products are also subject to the Compulsory Registration Scheme of the Bureau of Indian Standards (BIS), and there must be a mandatory registration and acceptance of these products by the BIS. All telecommunications equipment has also now been notified under a Mandatory Testing and Certification of Telecommunication Equipment (MTCTE) order under the DoT. The government empowered through National Cyber Security Coordinator has also amended the security conditions in the UL, UL(VNO) and standalone licenses. pertaining to procurement of telecom equipment ‘Trusted Products’ from ‘Trusted Sources’ as may be identified. For details on telecom licenses please refer to Question 1.2.

The DoT has also released a Production Linked Incentive Scheme (PLI Scheme) for promoting telecom and networking products manufacturing in India. The PLI Scheme covers equipment such as core transmission equipment, 4G/5G next generation radio access network and wireless equipment, access and customer premises equipment, internet of things, etc. Additionally, the Ministry of Electronics and Information Technology (MEITY) has also implemented PLI Schemes for IT hardware and large-scale electronics manufacturing to boost manufacturing in India and reduce dependence on imports.

Fintech regulations in India

The Reserve Bank of India (RBI) regulates the operations of payment systems in India under the Payment and Settlement Systems Act, 2007 (PSSA). Payment systems are defined as systems that enable payments to be effected between payers and beneficiaries, that involve clearing, payment and/or settlement service. Only payment systems authorised by the RBI can be operated in India.

The RBI has issued the Master Direction on Issuance and Operation of Prepaid Payment Instruments dated 11 October 2017 (PPI Master Direction) under the PSSA to regulate prepaid payment instruments (PPI). The PPI Master Direction defines a PPI as a payment instrument that facilitates the purchase of goods and services against the value stored on such instruments. There are three kinds of PPIs that can be issued in India – Open PPIs, Semi-closed PPIs and Closed PPIs.

Apart from this RBI also regulates payment gateways and payment aggregators, account aggregators, P2P lending platforms, digital payments etc. Further, sectoral regulators like the Insurance Regulatory and Development Authority of India (IRDAI), specifically regulate insurance related services. The Securities and Exchange Board of India (SEBI) also regulates security market related technology services. The SEBI, RBI and
the IRDAI also offer a Regulatory Sandbox for the testing of relevant fintech services. The RBI also has issued a Cyber Security Framework for Banks, IT Framework for NBFCs and guidelines and a code of conduct for the outsourcing by Banks and NBFCs.

The RBI has issued the finalised the Framework for authorisation of a pan-India New Umbrella Entity (NUE) for Retail Payment Systems (Framework) on 18 August 2020. The Framework aims to incentivise participation in the payments sector, which is currently dominated by the National Payments Corporation of India (NPCI). The NUE will be a non-profit entity authorised under the PSSA to manage and operate new payments systems in India. The Framework envisages several functions of a NUE including operating payment systems, clearing and settlement systems, ensuring fairness, equity and competitive neutrality, fostering the retail payments ecosystem in India and interoperability.

The RBI in 2019 had also announced the opening of the first cohort of its Regulatory Sandbox (Sandbox) with retail payments as its theme, with an expectation to spur innovation in the digital payments space. In November 2020 the first cohort of entities began testing their products on the Sandbox. A fresh call for applicants was also released for the theme ‘Cross border payments’ in December 2020, and concluded in February 2021, however as of date, these entities have not yet begun testing.

Content regulations

The Cinematograph Act, 1952 and the Cable Television (Networks) Regulation Act, 1995 regulates film and television content in India. These do not apply to online content and internet content is regulated under the IT Act. The IT Act prohibits publishing or transmitting of obscene material and child pornography. Further, the IT Rules implement a Code of Ethics for digital media including online curated content and news and current affairs content. The Code of Ethics provides the general principles, for self-classification by publishers of content based on age and taking into account of various factors such as the theme and message, context, tone and impact, target audience. Content shall also be classified on the basis of violence, nudity, sex, language, drugs or substance abuse, horror etc. and publishers are to ensure to prominently display such classification for viewers. The IT Act also has extraterritorial jurisdiction in certain circumstances. Apart from this, the Indian Penal Code, 1860, Criminal Law (Amendment) Act, 1961, the Drugs and Magic Remedies (Objectionable Advertisements) Act, 1954 and the Indecent Representation of Women (Prohibition) Act, 1986 also impose restrictions relating to certain forms of content.

2. Are communications networks or services regulated?

Yes, telecommunication networks and services are regulated in India under the Telegraph Act and the TRAI Act. Commercial telecom services in India are regulated under the UL framework formulated by the DoT.

The TRAI has also issued specific regulations including ones for number portability, tariff for specific services, broadcasting and cable services, unsolicited commercial communications and interconnectivity.

3. If so, what activities are covered and what licences or authorisations are required?

Unified License

Commercial telecommunication services in India are regulated under the UL issued by the DoT. The UL combines multiple telecom services, including Access Service, Internet Services, National Long Distance (NLD), International Long Distance (ILD), Global Mobile Personal Communication by Satellite (GMPCS), Public Mobile Radio Trunking Service (PMRTS), Very Small Aperture Terminal (VSAT) Closed User Group (CUG), INSAT MSS-Reporting (MSS-R) Service and Resale of International Private Leased Circuit (IPLC) Services.

The UL lays down general conditions applicable to all services and service specific conditions for each service. However, each service must separately be authorised by the DoT against the payment of entry fee and license fee for each service. Services are broadly divided into license for Access Services and other services. While the Access Service authorisation combines licenses for provision of voice, text and data, other authorisations like internet service, NLD service, ILD service etc. entities are required to apply for the provision of those services specifically.

The license for the services is separate from spectrum allocation. Spectrum is auctioned through a Notice Inviting Application (NIA) which is the governing document of the auction and the spectrum. An NIA imposes conditions on the use of spectrum and prescribes the procedure for auctions. It details eligibility conditions, roll out obligations, payment terms and bidding procedures.

Licenses for both – provision of services and use of spectrum are granted for different regions – referred as circles. These circles are divided into Categories A, B and C based on the size of the market of the respective
Apart from this, the UL (VNO) licence was introduced by the DoT to de-link networks owned by Network Service Operators (NSO) (TSPs who own the core telecom network) from the delivery of services. A VNO licensee with access service authorisation can undertake collection, carriage, transmission and delivery of voice and/or non-voice messages over the NSO’s network in a designated area. The VNO licensee may also provide internet telephony, internet services including IPTV, broadband services, and triple play, i.e., voice, video and data. It can also provide IVR, video/audio conferencing, voice mail and unified messaging services. The services can be provided on a national level or in a specific telecom circle/metro area for which the authorization is procured.

The government of India’s Digital Communications Policy, 2018[1] is the master policy document which governs the telecom sector. This policy was issued with the goal to unlock the transformative power of digital communications networks – to achieve the objective of digital empowerment. The government has outlined its objective to provide broadband to all citizens, create jobs in the digital communication sector and ensure digital sovereignty.

Reference

4. Is there any specific regulator for the provisions of communications-related services?

As mentioned above, the DoT and the TRAI are the two main regulators that handle telecommunication networks and services. Electronic communications are regulated under the IT Act and the MEITY is the main regulator. Additionally, the MIB has been entrusted with the power to regulate publishers of NCA and OCC through digital media vide the IT Rules.

5. Are they independent of the government control?

No, these regulators are government bodies. The TRAI is however an independent regulator.

6. Are platform providers (social media, content sharing, information search engines) regulated?

Yes, platform providers including social media, content sharing, information search engines are regulated under the IT Rules. As mentioned above in Question 1, the IT Rules also provide a new class of intermediaries termed as SMIs and SSMIs which govern social media and content sharing.

7. If so, does the reach of the regulator extend outside your jurisdiction?

No, the jurisdiction of DoT and TRAI are restricted to India. Having said that the jurisdiction of the IT Act extends outside India in certain cases. The IT Act applies to offences and contravention committed outside India by any person if the offence or contravention involves a computer or a computer system or a computer network located in India.

8. Does a telecoms operator need to be domiciled in the country?

Yes, a telecom operator must be registered as a company under the Companies Act, 2013.

9. Are there any restrictions on foreign ownership of telecoms operators?

Foreign investment (FDI) is governed by the Foreign Exchange Management Act, 1999 (FEMA) read with Foreign Exchange Management (Non-debt. Instruments) Rules, 2019 (NDI Rules).

There are two entry routes for FDI:

the ‘government/approval route’: FDI in certain identified sectors/activities requires the prior permission of the concerned ministry/department together with post investment filings; and

the ‘automatic route’: FDI in other sectors/activities does not require the prior permission of the concerned ministry/department or the RBI with only post investment filings required to be made.

The NDI Rules allow for 100% investment in the telecom sector, of which up to 49% is allowed through the automatic route. FDI beyond 49% requires Government approval. The competent authority which grants approval for the foreign investment in the telecom sector is the DoT.
10. Are there any regulations covering interconnection between operators?

The TRAI has formulated a framework for the efficient interconnection between a variety of access networks (such as fixed, mobile, national long distance and international long distance) to interconnect to make national and international connectivity possible. The TRAI has created regulations that set pricing for interconnection usage charges.

The Telecommunications Interconnection Regulations, 2018 governs interconnection agreement between telecom service providers and mandates that telecommunications operators must enter into interconnection agreements with the requesting service provider within 30 days from their request on a non-discriminatory basis. The regulation also states that the interconnection charges such as set-up charges and infrastructure charges may be mutually negotiated between service providers subject to the regulations or directions issued by TRAI from time to time. The regulations have been amended in 2020, to provide for the location of Point of Interconnection (POI) for calls between two fixed line networks or between a fixed line network and NLD network, as may be mutually decided between the parties. In a situation where the parties fail to agree on a POI, the POI shall be at the Long Distance Charging Centre.

The Telecommunication Interconnection Usage Charges Regulation, 2003 also sets out the interconnection usage charges (including domestic and international termination charges) applicable for interconnection arrangements between telecommunications operators. The regulations have undergone an amendment in 2020 to provide for a non-discriminatory rate of termination charges for all international calls and provides the range within such charges may be levied. In furtherance of an earlier amendment to the regulations in 2019, interconnection usage charges have been brought down to zero for domestic calls with effect from January 2021.

11. If so are these different for operators with market power?

The regulations apply to all telecom service providers irrespective of market power. The regulation however states that any interconnection charges agreed pursuant to the interconnection agreement, must be reasonable, transparent and non-discriminatory.

12. What are the principal consumer protection regulations that apply specifically to telecoms services?

The Telecom Consumer Protection Regulation, 2012 was issued by TRAI to address the concerns of the consumer in relation to transparency in tariff orders, transparency provision of information relating to activation of vouchers, usage, tariff plan subscribed etc.

In order to ensure efficiency in the grievance redressal mechanism provided by telecom service providers, TRAI has issued the Telecom Complaint Redressal Regulations, 2012.

Apart from this, to regulate commercial calls and protect consumer from unsolicited commercial calls and messages, TRAI has notified the Telecom Commercial Communication Customer Preference Regulations, 2018.

The Consumer Protection Act, 2019 (CPA 2019) which repealed the Consumer Protection Act, 1986 is the main legislation for consumer protection in India. The CPA creates a Central Consumer Protection authority that would promote, protect and enforce the rights of consumers. There is also a provision for the bringing of class action suits against manufacturers under the CPA. It also provides for a simplified dispute resolution process, including mediation and e-filing of cases. The CPA 2019 contains product liability provisions to address defective or deficient products/services delivery.

13. What legal protections are offered in relation to the creators of computer software?

Computer software and programmes are protected as literary work in which copyright subsists, under the Indian Copyright Act, 1957 (Copyright Act). A computer program is defined to mean a set of instructions expressed in words, codes, schemes or in any other form, including a machine readable medium, capable of causing a computer to perform a particular task or achieve a particular result. Authors / owners of computer programs are granted the exclusive right to reproduce, offer for sale, sell, rent the computer program, among others. The term of protection is the lifetime of the author plus sixty years. Software per se, on a standalone basis, is not eligible for patent protection in India. However, software that can be shown to be an integral part of a novel hardware invention could be is eligible for patent protection. This is a difficult test to satisfy in India.
14. Do you recognise specific intellectual property rights in respect of data/databases?

Copyright subsists in any tables and compilation including a computer database, as this is protected under the Copyright Act as a literary work. Such database is protected to the limited extent of its selection, arrangement and presentation and the underlying data itself may not be offered any protection.

15. What key protections exist for personal data?

The IT Act and the Data Privacy Rules lay down requirements as to how personal data is to be stored, processed, transferred and secured. Under the Data Privacy Rules, data is classified into PI and SPI.

PI is defined as any information that relates to a natural person and must, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, be capable of identifying such person.

The Data Privacy Rules define SPI to mean PI that contains information relating to: (a) passwords; (b) financial information; (c) physical, physiological and mental health condition; (d) sexual orientation; (e) medical records and history; and (f) biometric information.

Under the Data Privacy Rules, any body corporate collecting, handling or storing SPI is required to comply with the following obligations:

a. Maintaining a privacy policy on its website providing for privacy practices and policies, the PI or SPI being collected, the purpose, usage and the manner of disclosure of such information, the security measures implemented in this process etc.;
b. Ensuring that the information is used for the purpose for which it has been collected;
c. Ensuring that the data is retained only for the period required to fulfill the purposes for which it may lawfully be used unless required to be maintained under any other law;
d. Obtaining consent prior to the collection of information and ensuring that the data subject is made aware of the collection of information, the purpose of collection, the intended recipients of the information and the name and address of agencies collecting and retaining the information;
e. Providing an option to the data subject, prior to collection, to not provide the information sought to be collected and allow the data subject to withdraw the consent at any time;
f. Permitting the data subjects, as and when requested by them, to review such information and to correct or amend any information found to be inaccurate or deficient;
g. Obtaining prior permission from the data subject for transfer or disclosure of its information with a third party (including cross-border transfer) and ensuring that such third party maintains similar data protection standards as prescribed in the Data Privacy Rules;
h. Appointing a grievance officer and publishing such officer’s name and contact details on its website; and
i. Adhering to reasonable security standards and having a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected and with the nature of business, such as international standard IS/ISO/IEC 27001 on “Information Technology – Security Techniques – Information Security Management System – Requirements”.

16. Are there restrictions on the transfer of personal data overseas?

Currently, the Data Privacy Rules permit the transfer of PI (including SPI, provided consent for such transfer is procured) outside India subject to the condition that the same level of data protection is adhered to in the other country, which is applicable to the body corporate under the Data Privacy Rules in India.

There are different sectoral rules that may apply to the transfer of data. For instance, the RBI has mandated that all data of payment system operators in respect of transactions in the payments eco-system should be stored within India. The SEBI Advisory for Financial Sector Organisations regarding SaaS based solutions also mandates maintaining critical data within India. Under the UL, telecommunications data relating to subscriber accounting information (not including international roaming/billing) and subscriber information (except pertaining to foreign subscribers using Indian Operator’s network while roaming and IPLC subscribers) are to be localised and are non-transferable outside
Further, the PDP Bill proposes localisation of all sensitive personal and critical personal data. Sensitive personal data under the PDP Bill includes financial data, health data, official identifiers, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliations. Critical personal data is such data as may be notified by the Indian Government.

17. What is the maximum fine that can be applied for breach of data protection laws?

The Data Privacy Rules are issued under Section 43A of the IT Act. Section 43A penalizes bodies corporate for negligence in implementing and maintaining reasonable security practices and procedures specified under the Data Privacy Rules while dealing with SPI.

Failure to comply with the Data Privacy Rules will amount to negligence on part of the body corporate and if such negligence causes wrongful loss or wrongful gain to any person, then body corporate could be required to pay damages by way of compensation to the affected person/ employee. Further, non-compliance with the Data Privacy Rules may attract a penalty of up to INR 25,000.

Disclosure of personal information obtained under a contract with knowledge or intent to cause wrongful loss or wrongful gain is punishable under Section 72A of the IT Act with imprisonment of a term which may extend to three years or fine which may extend to INR 5,00,000.

18. What additional protections have been implemented, over and above the GDPR requirements?

The GDPR applies only in a limited to context in India to entities that process personal data of residents or citizens of the EU. No additional requirements are in force other than what is mentioned above.

19. Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?

There is no single legislation governing cloud services. Currently, cloud services are mainly regulated under the IT Act, the Data Privacy Rules and the IT Rules. The Data Privacy Rules apply to cloud service providers in relation to collection, storage, transfer of PI and SPI. Further, cloud service providers may also be subject to interception and monitoring orders from the Government under the IT Act.

Sectoral regulators such as RBI, IRDAI and SEBI provide guidelines for entities regulated by these regulators – on service level agreements, access control mechanisms and data security measures to be used while engaging cloud-based service providers. The government of India, through MEITY has initiated “MeghRaj” cloud initiative for setting up State and National Clouds, empanelment of Cloud Service Providers (CSPs) and setting up of a Cloud Management Office, which may be relevant for government procurement of cloud services.

TRAI had issued recommendations on regulation of cloud services and has proposed a light touch regulatory regime on the basis that they are a service provider under the TRAI Act. The recommendations call for the creation of a registered not for profit industry body working in conjunction with the DoT/TRAI to which CSPs are required to be members. The scope of the CSPs contemplated under the recommendations is limited to providers offering Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) in India or to customers in India.

20. Are there specific requirements for the validity of an electronic signature?

Only certain types of electronic signatures are recognised under the IT Act, i.e. (a) digital signatures using asymmetric crypto system and hash function, and (b) eSign using various authentication techniques such as Aadhaar e-KYC, One Time Passwords or trusted third parties. There is a legal presumption in favour of the validity of any electronic documents signed using digital signature or electronic signature, provided that:

- the electronic signatures must be unique to the signatory (i.e. it must be uniquely linked to the person signing the document, and no other person);
- at the time of signing, the signatory must have control over the data used to generate the electronic signature (for example, by directly affixing the electronic signature to the document);
- any alteration to the affixed electronic signature, or the document to which the signature is affixed, must be detectable (for example, by encrypting the document with a tamper-evident seal);
- there should be audit trail of steps taken during the signing process; and
- signer certificates must be issued by a
The exclusions or type of documents which cannot be electronically signed are as follows:

- A negotiable instrument (other than a cheque) as defined in Section 13 of the Negotiable Instruments Act, 1881.
- A power-of-attorney as defined in Section 1-A of the Power of Attorney Act, 1882.
- A trust as defined in Section 3 of the Indian Trusts Act, 1882.
- A will as defined in clause (h) of Section 2 of the Indian Successions Act, 1925, including any other testamentary disposition.
- Any contract for sale or conveyance of immovable property or any interest in such property.

Validity of electronic signatures not specifically recognized under the IT Act

Electronic signatures apart from the ones mentioned above are not specifically recognized under the IT Act. This does not mean that any contract signed using such signature is invalid, but that there is no accompanying presumption of validity. This would make it possible for a party to dispute the validity of the e-contract. In such a case, the party will be required to prove its validity specifically under the IT Act.

21. In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?

No, Indian law does not mandate automatic transfers. Such transfers will be guided by the terms of the outsourcing agreement entered into by the parties. The Contract Labour (Regulation and Abolition) Act, 1970 (CLRA) would apply in such instances and the outsourcing agreements will need to be structured as per the CLRA.

22. If a software program which purports to be a form of A.I. malfunctions, who is liable?

Currently, A.I. is not specifically regulated in India. Case laws and jurisprudence on matters involving loss / injury caused due to A.I is lacking. Having said that, if the A.I. forms part of a product, then product liability claim can be made against the service provider under the Consumer Protection Act, 2019 in case the service is offered to end consumer.

23. What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?

(a) Maintenance of cyber security

The IT Act prescribed penalties for activities such as hacking, identity-theft, cyber-terrorism, privacy breaches and publication of obscene content. Such activities impede cybersecurity which is defined as protection given to information, equipment, devices, computers, computer resources, communication device and information stored therein from authorised access, use, disclosure, disruption, modification or destruction. In order to further cybersecurity, the IT Act also mandates body corporates to implement the ISO/IEC 270001 information security standards or other similar standards.

Further, the CERT-In handles and responds to cyber security incidents in the country. The CERT-In has listed different types of cybersecurity threats and incidents that all individuals and body corporates are expected to notify to the CERT-In upon occurrence.

(b) Criminality of hacking / DDOS attacks

The IT Act contain provisions to criminalise both hacking and DDOS attacks. Any person who, without the permission of the owner or any other person who is in charge of the computer resource or network (a) accesses or secures access to a computer resource; or (b) downloads, copies or extracts any data; (c) introduces a computer contaminant or a virus; (d) damages or disrupts computer network or data stored; (e) denies or causes denial or access or; (f) tampers or manipulates the computer system/ network is liable to compensate the person affected. Further, if such acts are performed dishonestly or fraudulently, such person will be punishable with imprisonment for a term of up to 3 years or with fine which may extend up to INR 5,00,000 or with both. If the offence is committed by a company, in addition to the company, every person who, at the time
the offence was committed, was responsible for the conduct of business, may face penalty for such contravention. If it is proved that the contravention has taken place with the consent of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, then such officer may also be held liable. Please note that the IT Act applies to an offence committed outside India if the act or conduct constituting the offence involved a computer system or computer network located in India.

24. What technology development will create the most legal change in your jurisdiction?

The year 2020 built on the year 2019 saw many changes in terms of regulatory and legislative measures by the Government. One of the major changes expected includes the PDP Bill which was introduced in the Lok Sabha in 2019 and is currently before the JPC. The JPC has reportedly made several amendments to the PDP Bill and has been granted an extension up to the first week of the monsoon session of the Parliament to submit its report, which is scheduled to commence on 19 July 2021. The enactment of the PDP Bill is likely to bring significant change in the India’s data protection space with the manner in which entities obtain consent for collection of data, conduct of data intensive businesses, ensuring compliance with stringent localisation requirements, enhancement of data subject rights along with heavy fines and penalties in cases of violations. It is expected that the PDP Bill will be implemented through a phased manner over a period of two years till 2023.

The notification of the Consumer Protection (E-Commerce) Rules, 2020 (E-Commerce Rules) also brought focus to consumer protection in the age of e-commerce and online retail and regulate marketing, sale and purchase of goods and services online. The E-Commerce Rules apply to all goods and services sold over a digital or electronic network and includes inventory and marketplace models within its ambit. It primarily governs B2C e-commerce. It imposes specific duties on all e-commerce entities along with additional obligations and liabilities specific to marketplace sellers and marketplace and inventory entities. The Department of Consumer Affairs has also released a draft amendment to the E-Commerce Rules for consultation recently.

Another significant change came by way of the IT Rules, which imposes onerous obligations on intermediaries, SSMIs and publishers of NCA and OCC. In addition to the earlier compliance requirements under the Information Technology (Intermediary Guidelines) Rules, 2011, the IT Rules introduce new categories of prohibited information to combat fake news, increase in record retention time periods, and require speedy resolution of customer complaints within 15 days. The IT Rules also regulate publishers of NCA and OCC on digital media, which were unregulated earlier. Several petitions have been filed challenging the constitutionality of the IT Rules before High Courts in India, and the MEITY has applied before the Supreme Court for a transfer petition for clubbing of the pending petitions in High Courts. The scope of the IT Rules is likely to become clearer on the basis of a decision given by a High Court or the Supreme Court.

The Revised Report on the NPD framework released in December 2020 provide more clarity and address issues raised in the consultation. While the Revised Report clarifies several aspects raised in the initial round of consultation, it fails to provide clarity in respect of certain issues such as localisation requirements which may be imposed on NPD which is sensitive or critical, similar to the PDP Bill and the treatment of Private NPD (which includes global datasets collected from foreign jurisdictions) and whether it would be subject to mandatory sharing as well.

The government is also likely to introduce the Cryptocurrency and Regulation of Official Digital Currency Bill, 2021 to create a framework for an official digital currency as issued by the RBI and regulate private cryptocurrencies in India. The proposed law also encourages the use and application of the underlying blockchain technology. In line with this bill, the MEITY has released a draft National Strategy on Blockchain which proposes a national level blockchain framework and integration of services such as digital signatures, DigiLocker and authentication to the blockchain for promotion of the technology.

It must be noted that localisation continues to be the common theme among all the recent policy development. The Indian government has also been pushing an overall policy doctrine of digital sovereignty and promotion of national manufacturers, service providers and entities in the digital space. This can be inferred from the PDP Bill, NPD Report, E-Commerce Rules and other policy documents. Further, the amendments to the telecom licenses for procurement of equipment from ‘Trusted Sources’, adoption of stringent controls over intermediaries and mandatory sharing of NPD indicate an increasing push towards promoting ‘Make in India’ and digital sovereignty. This is bound to change the ways in which digital business is carried out in the country.
25. Which current legal provision/regime creates the greatest impediment to economic development/commerce?

The requirements on data localisation under the PDP Bill and various sectoral regulations will create a significant impediment to digital commerce. The RBI has mandated that all data of payment system operators in respect of transactions in the payments eco-system should be stored within India. Further, the PDP Bill proposes localisation requirements for sensitive and critical personal data. Implementation of localisation requirements will increase compliance costs for companies operating in India.

The government has also proposed amendments to the E-Commerce Rules which inter alia includes requirements such compulsory listing of origin of all products, and providing Indian alternatives, registration of all e-commerce entities with the Department of Promotion for Industry and Internal Trade. The draft E-Commerce Rules also suggest changes to the operation of ‘related parties’ to cover entities in common or direct control as the e-commerce entity. The draft E-Commerce Rules bars the listing of related parties as sellers on the marketplace operated by an e-commerce entity. These changes if enacted could cause significant impediment for foreign e-commerce entities operating in India and their business models.

The IT Rules have also proven to be an extremely significant piece of legislation negatively affecting business operating in India. SSMIs are required to comply with additional obligations such as resident chief compliance officer, nodal and grievance officers, publish period compliance reports and endeavour deploy technology-based tools for removal of unlawful content. Additionally, intermediaries are required to address any complaints within a time period of 15 days as opposed to the earlier requirement of 1 month. Publishers of NCA and OCC also have to comply with the digital media ethics code and adopt of the self-regulating mechanism for grievance redressal. In furtherance of this, the MEITY and MIB also set strict timelines of 3 months for intimating of the compliance with the additional requirements under the IT Rules.

26. Do you believe your legal system specifically encourages or hinders digital services?

The legal, business and regulatory environment is conducive for the growth and development of digital services in India. Over the past few years, the Government has taken significant steps to promote the growth of digital services such as the Digital India initiative through implementation of infrastructure and services. Additionally, the DoT and WPC have allotted 5G technology spectrum to telecom operators in India for conducting trials for a period of 6 months.

27. To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?

As stated before, AI is not specifically regulated in India. However, policy framers are recognising the requirement to development systems to encourage the use of AI as well as regulate its development. The National Institution for Transforming India (NITI) Aayog, the policy think tank of the Government, has released an approach document for India on Responsible AI for All in February 2021. The paper provides guidelines and suggested future policy in relation to the use, governance and legal restrictions on artificial intelligence. The paper also sets out a recommended framework for the use and deployment of AI in India, as well as an analysis of use cases, challenges, and advantages of its use. The MEITY had also launched the National AI Portal in May 2020, a joint initiative of MEITY, the National e-Governance Division and the National Association of Software and Service Companies (NASSCOM). The National AI Portal acts as a centralized hub for AI related news, activities, events, articles in India and abroad and can be accessed at – https://indiaai.gov.in/.

Additionally, the MEITY is also implementing ‘Mission AI’ and setting up of an AI specific cloud computing infrastructure platform ‘AIRAWAT’ based on the recommendations of the National Strategy for AI. The Ministry of Corporate Affairs (MCA) is also in the process of launching a new portal drive on data analytics with options for e-Adjudication, e-Consultation and compliance management. The new portal will also facilitate compliance management and ease filing of forms.

As discussed, PDP Bill and the NPD Report have been drafted with a view to encourage the development of local AI. Once the PDP Bill is enacted and implemented, the Indian legal system will be equipped to handle the challenges posed by AI.
Contributors

Nikhil Narendran
Partner
nikhil.narendran@trilegal.com

Jishnu Sanyal
Senior Associate
jishnu.sanyal@trilegal.com

Cheta Sheth
Associate
cheta.sheth@trilegal.com

Samvit Ganesh
Associate
samvit.ganesh@trilegal.com