The Legal 500 & The In-House Lawyer
Comparative Legal Guide
India: Technology

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

It will cover communications networks and their operators, databases and software, data protection, AI, cybersecurity as well as the author's view on planned future reforms of the merger control regime.

This Q&A is part of the global guide to Technology. For a full list of jurisdictional Q&As visit http://www.inhouselawyer.co.uk/index.php/practice-areas/technology

Country Author: Dhir & Dhir Associates

The Legal 500

Mr. KPS Kohli, Associate Partner

kps.kohli@dhirassociates.com

Mr. Vishy Vincent, Associate

vishy.vincent@dhirassociates.com

1. **Are communications networks or services regulated? If so what activities are covered and what licences or authorisations are required?**

   The communication networks and services are highly regulated in India. The (i) Indian Telegraph Act, 1885; (ii) Indian Wireless Telegraph Act, 1933; (iii) Cable Television Networks (Regulations) Act, 1995; (iii) Telecom Regulatory Authority of India Act, 1997; and (iv) Information Technology Act, 2000, provide the statutory framework for all permissible activities in the domain. The requirement of licenses and authorisations for communication networks, services and devices is the norm and the following three

Central Government Ministries oversee, regulate and grant the requisite licenses and authorisations: (i) the Ministry of Communications (MoC); (ii) the Ministry of Electronics and Information Technology (MeitY); and (iii) the Ministry of Information and Broadcasting (MIB).

The licensing framework can be broadly categorised into three sub-groups:

(i) Telecom and Spectrum: The MoC identifies the benefits of convergence and strives towards the idea of One Nation – One License and has introduced the Unified Licensing Regime for basic telephony, cellular mobile services and internet services among others. Spectrum, on the other hand was delinked from telecom licenses (in 2012) and is only allocated via an auction process.

(ii) Other Service Providers: Activities that have the potential to bypass the existing license conditions of authorised voice and data service providers are also regulated under a special category, called the Other Service Providers (OSP) category. For instance, call-centres are regulated under the OSP category, and these cannot commence or continue operations unless their network operations are cleared and authorised by the Department of Telecommunications (DoT) under the aegis of the MoC.

(iii) Broadcasting: Broadcasting services in India can be further bifurcated into two categories: (a) content services; and (b) carriage services. The MIB grants licenses and regulates both categories. License is required for operating (i) Community Radio Stations (content); (ii) private FM channels (content); (iii) Teleports and satellite TV Channels (content); (iv) Headend-In-The-Sky (HITS) broadcasting services (carriage); (v) Direct-To-Home (DTH) broadcasting services (carriage); (vi) cable company (Multi System Operator) services (carriage).

2. **Is there any specific regulator for the provisions of communications-related services? Are they independent of the**

government control?

Communications-related services in India can be broadly categorised into (i) telecommunication services; (ii) electronics and information technology services; and (iii) broadcasting services.

For telecommunications services (i) the Department of Telecommunications (DoT); and (ii) the Telecom Regulatory Authority of India (TRAI), are the two key regulatory bodies. The DoT is a government department and is part of the MoC. It is the rule making and licensing arm of the MoC. The TRAI is an independent statutory body and is established under the Telecom Regulatory Authority of India Act, 1997, after the entry of private players in the telecom sector in India was permitted. The TRAI regulates tariffs and interconnections, lays down quality of service parameters, ensures compliance of the terms and conditions of licenses among others. The TRAI in addition, also recommends either suo moto or at the request of the Central Government on the need and timing for introduction of new service provider, terms and conditions of licenses to service providers, revocation of license for non-compliance, promotion of competition, technology improvements amongst other such matters.

For electronics, information technology services and broadcasting services the MeitY and the MIB have multiple subordinate departments/ organisations. In certain matters, the broadcasting sector is also regulated by the TRAI.

In addition, the broadcasting industry has several self-regulating bodies such as the Indian Broadcasting Foundation (IBF), Broadcasting Content Complaints Council (BCCC), Advertising Standards Council of India (ASCI), News Broadcasters Association (NBA) that are free of government control.

3. **Does an operator need to be domiciled in the country? Are there any restrictions on foreign ownership of telecoms operators?**

Yes, any license required in the telecommunication sector will only be granted to an entity incorporated in India. However, 100% foreign ownership is allowed in the sector and investments of up to 49% are under the automatic route (which do not require

approvals). 100% foreign direct investments (FDI) under the automatic route is allowed in respect of the OSP category.

Also, foreign nationals are restricted from participation in the management of telecom companies.

4. **Are there any regulations covering interconnection between operators? If so are these different for operators with market power?**

Yes, interconnection between operators is regulated under the Telecommunication Interconnection Regulations, 2018 (Regulations) issued by the Telecom Regulatory Authority of India (TRAI). The Regulations require operators to enter into an Interconnection Agreement with the interconnection seeker on a non-discriminatory basis within a period of thirty (30) days. Prior to February, 2018, the concept of a Significant Market Player (SMP) was recognised wherein an operator holding 30% or more share of the total activity in a licensed telecommunication service area was required to get an approval from TRAI for its base contractual agreement containing the technical and commercial specifications (called Reference Interconnect Offers). However, this requirement has now been done away with.

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

The TRAI in exercise of its powers has framed various regulations to protect the consumer interests, which include:

1. Mobile Number Portability (MNP) across telecom circles in India;
2. Curbing of Unsolicited Commercial Communication (UCC);
3. Seamless migration across post-paid and pre-paid platforms;
4. Billing accuracy;

5. Safeguards against hike in tariff;
6. Ease of activation and deactivation of Value Added Services (VAS);
7. Strict adherence to Quality of Service (QoS) standards by operators.

The Telecom Consumers Complaint Redressal Regulations, 2012 notified by the TRAI goes on to create an institutional mechanism to handle consumer complaints in the sector.

Further, India also has an umbrella legislation for ensuring consumer protection, the Consumer Protection Act, 1986, the benefits of which also extend to telecom consumers.

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

Computer software can be described as a computer programme or a set of computer programmes, and the Copyright Act, 1957 in India recognises computer programmes as “literary work” in line with the Berne Convention for the Protection of Literary and Artistic Works, 1886. The creator is granted exclusive rights including inter alia the right to reproduce, sell or rent the software to the public, for a period of sixty (60) years, under the Copyright Act, 1957.

Further, though a computer software is not patentable on a stand-alone basis, protection under the Patents Act, 1970 may be granted in case the software can be shown to be an integral part of a novel hardware invention. The term of a patent is for a period of twenty (20) years in India.

Also, if the source code of a software is maintained as a trade secret under contractual arrangements, the courts in India recognise such agreements and enforce the same.

The on-screen look and feel of a software can be protected under the Trademarks Act, 1999. The protection is for an initial period of ten (10) years and may be extended by

an additional ten (10) years.

7. Do you recognise specific intellectual property rights in respect of data/databases?

Intellectual property rights associated with the compilation, verification, presentation and a format based usage of data that creates value in such data, are granted and protected under the Copyright Act, 1957. The Act recognises databases as “literary works” and provides both civil and criminal remedies against infringement.

The underlying data does not automatically draw protection under the Copyright Act, 1957 or other similar intellectual property statues. Factors relating to creation, use and application of the data determines the scope and extent of protection that may be availed under the intellectual property laws in India.

8. What key protections exist for personal data?

The Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011 (RSPP-SPD Rules or Rules) notified under the Information Technology Act, 2000 (IT Act) presently governs the handling of personal data by body corporates. The RSPP-SPD Rules defines ‘personal data’ and ‘sensitive personal data’, and puts forth the conditions for obtaining consent, processing, usage and transfer of both personal and sensitive personal data. The Rules also mandate the implementation of an organisational policy for dealing with personal data.

The year 2017-2018 has been a watershed year for data privacy laws in India. The Supreme Court of India recognised ‘the right to privacy’ as a fundamental right enshrined in the Constitution and outlined the principles on which the State must enact laws for data privacy. Many sectoral regulators also proposed draft legislations protecting the rights of data subjects within their respective domains. The Reserve Bank of India (RBI) which is the central bank of India issued a data localisation order in April, 2018, requiring all payment system operators in India to store all transactional

data with respect of payments ‘eco-system’ within the Country. Later, the Ministry of Electronics and Information Technology (MeitY) published the draft Personal Data Protection Bill (on July 27, 2018) which is an all-encompassing legal framework for data privacy in India. This Bill once enacted will supersede existing legislations.

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

The Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011 (RSPP-SPD Rules) permit the transfer of personal data 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 RSPP-SPD Rules in India.

However, the Reserve Bank of India (RBI) has mandated that all data of payment system operators in respect of transactions in the payments eco-system should be stored within the Country.

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

A body-corporate shall be liable to pay monetary value to the extent of the wrongful loss or wrongful gain caused due to a failure to comply with the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011 (RSPP-SPD Rules). There is no upper limit.

Further, any person who secures access to personal data, whether through a lawful contract or otherwise, and discloses/ transfers the data to a third party without the consent of concerned party, or damages the data, or denies lawful access to the owner of the data, may be imprisoned for a period of three (3) years and a fine of INR 5,00,000/- (Indian Rupees Five Lakhs; USD 7,200/- approximately) may also be imposed.

11. Are there any restrictions applicable to cloud-based services?

There are no laws exclusively regulating cloud-based services in India.

That said, sectoral regulators have from time to time indicated cyber-security measures which touch upon the dos and dont's while utilising cloud based services. For instance, the Insurance Regulatory and Development Authority of India (IRDAI) provides guidelines on service level agreements, access control mechanisms and data security measures to be used while engaging cloud-based service providers.

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

The Evidence Act, 1872 recognises both: (i) 'electronic signatures' that have their own security protocols; and (ii) electronic signatures based on an authentication method prescribed by the law (asymmetric crypto system and hash function as required under the Information Technology Act, 2000 (IT Act)) issued by authorities appointed under the IT Act, legally termed as 'digital signatures'.

Validity of an electronic signature (that follows its own security protocols) is presently subject to the below conditions:

- The data created with respect to signature creation and authentication is linked between the signatory and the authenticator only;
- The signatory of the electronic document has the intent to sign the document and he alone has the control of the electronic signature;
- Any change made to the signature, information, data, etc. is evident and detectable.

Digital Signatures are considered more authentic and are not subjected to tests, given that the entire authentication process is prescribed and regulated under the IT Act.

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

The law does not provide for an automatic transfer of employees, assets or third-party contracts in case of an outsourcing arrangement. The transfers, if any, will only be guided by the contractual terms agreed to between the parties.

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

A.I. is not regulated per se and courts in India are yet to adjudicate on a matter involving loss/ harm caused due to an A.I. based system. At present a machine based on A.I. will be treated like a regular machine and liability arising due to the use of such a machine will be settled through the strict product liability principle whereby the creator/ manufacturer shall be held liable. Product liability in India is based on the Consumer Protection Act, 1986, The Sales of Goods Act, 1930 and the law of torts.

15. What key laws exist in terms of obligations as to the maintenance of cyber security?

The Information Technology Act, 2000 (IT Act) defines cybersecurity as the protection given to information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction and then prescribes penalties for a wide array of activities all of which obstruct cybersecurity, including, hacking, identity-theft, cyber-terrorism, privacy breaches and publication of obscene content.

The IT Act also recommends, without mandating, the ISO/IEC 270001 information security standard for all body corporates.

Further, sectoral regulators, such as the Reserve Bank of India (RBI) and the Insurance Regulatory and Development Authority of India (IRDAI) prescribe cybersecurity measures to be adhered to by the players within their respective domains. For instance, the RBI prescribes use of the encryption technology of at least 128 bit secure socket locker for all critical web applications of banking institutions.

Also, the Ministry of Electronics and Information Technology (MeitY) has set up a nodal organisation called the Indian Computer Emergency Response Team (CERT) which handles and responds to cyber security incidents in the country. The CERT has listed different types of cybersecurity threats and incidents that all individuals and body corporates are expected to notify to the CERT upon occurrence.

16. What key laws exist in terms of the criminality of hacking/DDOS attacks?

The Information Technology Act, 2000 (IT Act) contains sufficient provisions to criminalise both hacking and DDOS attacks. Though these terms are not defined under the Act, activities such as accessing or securing access, downloading data, introducing viruses, causing damage, disrupting operations and denying access, to computers, computer systems and computer networks, are prohibited, when committed in the absence of a consent from the owner or person in charge of such computer, computer system or computer network. Providing assistance to any person involved in any of the above listed activities is also treated at par with the actual act committed.

The nature and intent of hacking/ conduct of DDOS attacks may also trigger provisions under the Indian Penal Code, 1860.

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

While A.I. and Robotic Process Automation continued to dominate debates in the legal circles for the last few years, the disruptive appearance and spread of Blockchain

technology has completely changed things in India. While A.I. continues to be a critical area of study, it is Blockchain that has been identified to have the potential to affect the legal system in India to a larger extent.

In its Budget for 2018-19, the Government of India has committed to explore the usage of Blockchain technology and usher in a digital economy. The Reserve Bank of India (RBI) has prohibited banks and financial institutions regulated by it, from dealing with cryptocurrencies. However, the potential of the underlying Blockchain technology is acknowledged and both the Government and the RBI permit its usage in other avenues.

Some of the foreseeable changes that Blockchain technology could cause include:

a. Redundancy of various central agencies and/ or financial intermediaries;

b. Complete overhaul in the mode and manner of property registrations, making title verifications redundant;

c. Complete overhaul in intellectual property registration and enforcement, making the process fully effective.

18. Which current legal provision/regime creates the greatest impediment to economic development/commerce?

The data localisation order of the Reserve Bank of India (RBI) in 2018 requires all payment system operators to store their transactional data within the country. It has been criticised immensely for being anti-commerce. While the RBI states that its intention is to have unfettered supervisory access to all transactional data in the payments eco-system to protect users in the said eco-system, industry experts estimate that such a mandate has the potential to slow economic growth.

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

The Indian legal system creates a conducive environment for the growth of digital services in India.

Currently, the communication/ network infrastructure that facilitates digital services is more tightly regulated than digital services itself. A large majority of digital services continue to be provided without many conditions or restrictions.

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

India does not regulate Artificial Intelligence (A.I.) yet. As stated in response to Question 13, a hardware based on A.I. is presently treated at par with any other machine, and liabilities are assigned on the basis of the strict product liability principle, wherein the creator/ manufacturer is held liable. The product liability principle is based on the provisions of the Consumer Protection Act, 1986, the Sales of Goods Act, 1930 and the law of torts.

However, the policy framers in India do recognise A.I. as the likely cause for the next stage of technological evolution of the digital economy.