Legal 500
Country Comparative Guides 2024

India
TMT

Contributor

G&W Legal

Sherry Shukla

Associate | sherry.shukla@gnwlegal.com

Hardik Choudhary

Associate | hardik.choudhary@gnwlegal.com

Dhruv Singh

Counsel | dhruv@gnwlegal.com

Arjun Khurana

Partner | arjun@gnwlegal.com

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

For a full list of jurisdictional Q&As visit **legal500.com/guides**

India: TMT

1. Is there a single regulatory regime that governs software?

No, there is no single regulatory regime that governs software in India. Instead, there are various laws and regulations that apply to and protect different aspects of software development, distribution, and usage. These include criminal laws, intellectual property laws, information technology and data protection laws, as well as consumer protection laws. Additionally, there are also government policies which apply to the domain.

2. How are proprietary rights in software and associated materials protected?

Proprietary rights in software and associated materials are primarily protected through copyright. The definition of 'literary work' under the Copyright Act, 1957 includes '*computer programmes and compilation, including computer databases.*' Copyright protection is granted to the expression of an idea and in respect of software, it extends to protecting original works such as software code (including source code & object code), and related materials like user manuals, documentation, etc. Copyright protection is a result of the creation of the work itself and while a formal registration is advisable, it is not strictly necessary.

Another possibility of protection is under patent law. Software *per se* is not patentable in India, but if there are other things ancillary to the software, then it may become patentable. In other words, software-related inventions may be patentable. To demonstrate patentability, there would be a need to demonstrate either a 'combination with hardware' or a 'technical effect'. There have been instances of patents being granted to software where a technical effect was shown.

Trade Secrets can be another avenue of protection. In cases of proprietary software, source code, algorithms, etc., may be unavailable to the public / not published and therefore not protected under copyright. In such cases, these are protected as trade secrets. India does not have a specific law on trade secrets, and these are generally protected through private agreements between parties.

Lastly, there is also an argument in support of extending design protection to the 'Graphical User Interface ('GUI') aspect of software. The Controller of Designs in the past has denied design protection for GUI on the grounds that they do not meet the requirements under the law, namely qualifying as an 'article' and application to the article by an 'industrial process'. However, in 2023, the Calcutta High Court disagreed with the Controller of Designs in case where a design application was filed for a "Touch Screen" for a novel surface ornamentation which is a GUI. The Court held that GUIs can fall under Locarno Class 14 and that a source code can be embedded in controllers / processors and displayed in a screen by illuminating pixels by electronic means, which satisfies the industrial process requirement.

3. In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

Ownership of software is generally governed by the Copyright Act, 1957. In the absence of a contract to the contrary, the software developer / consultant / other party who creates a software for a customer will own the copyright therein.

If an agreement is signed between the parties, the ownership of proprietary rights in newly created software will generally be determined by the principle of "work for hire". This means that the customer who commissioned the development of the software will own all rights to it, unless otherwise specified in a contract.

4. Are there any specific laws that govern the harm / liability caused by Software / computer systems?

Different aspects of the harm / liability caused by software / computer systems are governed by different laws. Primarily, such harm / liability is dealt with under the contract between the parties. Additionally, the Information Technology Act, 2000 (IT Act) covers the framework to address issues of cybersecurity, data protection and cybercrime. Remedies to final consumers may also be available under the Consumer Protection Act, 2019.

The new Indian criminal law, called the Bharatiya Nyaya Sanhita (which replaced the erstwhile Indian Penal Code) has also expanded the scope of certain crimes (such as hate speech and spreading misinformation to disrupt public order) to include activities conducted over electronic communications.

Monetary penalties have also been prescribed under the Digital Personal Data Protection Act, 2023 ('DPDPA') in respect of breach / violation of personal data but the jurisprudence is yet to develop on this front.

Since the Indian Supreme Court's recognition of the right to privacy as a fundamental right granted under the Indian Constitution, writ petitions may also be filed for the violation of this right to privacy by the State.

5. To the extent not covered by (4) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021) have been issued under the IT Act. The IT Rules 2021 regulate content / media / games offered over the internet and have potential implications for software / computer systems. Additionally, there are Directions by the Indian Computer Emergency Response Team (CERT-In) which regulate cyber incidents and cyber security incidents.

India's primary antitrust regulation, the Competition Act, 2002, may also serve to regulate software companies relating to noncompetitive practices. The Competition Commission of India ("CCI"), India's antitrust regulator, has passed orders against major players such as Google and MakeMyTrip (an Indian travel aggregator) for violations of the Competition Act.

6. Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

There are no other laws that specifically govern the provision of software by a software vendor to a customer, or cloud technology. The IT Act and its rules such as the SPDI Rule 2011 and IT Rules 2021, Cert-In Guidelines as well as the soon to be implemented DPDPA would broadly cover the space. Cloud service providers are expressly named under the Cert-In Guidelines. Sector specific regulations by the Reserve Bank of India ('RBI') and Insurance Regulatory and Development Authority of India ('IRDAI') can also come into the picture. For example, very recently, the RBI issued its Cyber Resilience and Digital Payment Security Controls for Non-Bank Payment System Operators Master Directions, 2024 (PSO Master Directions 2024). These Directions mandate that each PSO shall obtain the source code of all critical applications procured from third-party vendors. The Directions are already in effect but will be implemented and enforced in a phased manner from April 2025 – April 2028.

7. Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

It is quite typical for a software vendor to try and cap its maximum financial lability to a customer in a software transaction. There is no standard market level cap, and this value would largely depend on factors such as transaction size, potential fallouts, risk appetite of the vendor, customer's negotiations, etc. That said, in cases of pre-packaged software licenses, software vendors tend to limit their maximum liability up to the cost of the software to the end-customer. While such caps may be prescribed by the vendors through the terms of use of the software license, the same will not preclude the end-user from seeking compensation of a greater amount as per the Consumer Protection Act, 2019.

8. Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

a. Confidentiality breaches – Would largely depend on the negotiations between the parties. A customer would push for exclusion considering, *inter alia,* the fallout in case of breach of any sensitive information. On the other hand, software vendors prefer to have confidentiality breaches subject to the general cap on liability.
b. Data protection breaches – Again, this would largely

depend on the negotiations between the parties. However, this would cover at least the maximum statutory liability under the IT Act currently and the DPDPA once it is implemented.

c. Data security breaches (including loss of data) – same as b).
d. IPR infringement claims – Unless provided to the contrary, these are generally excluded. The IPR infringement claims can result in third-party indemnification and hence, the values involved cannot generally be pre-determined.
e. Breaches of applicable law – This is typically included in the transaction and limited to the maximum applicable liability under the law.
f. Regulatory fines – same as e).
g. Wilful or deliberate breaches – These are generally excluded from the standard cap as the vendors may be held responsible for deliberate misconduct, giving rise to unlimited liabilities being imposed.

9. Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

In India, placing software source codes in escrow is not as common as it is in some Western countries, but is becoming more accepted, especially in larger and more complex software transactions. This is even more so in cases involving multi-nationals and cross-border transactions. In its recent PSO Master Directions 2024, the RBI has mandated that in cases where obtaining source code from a third-party vendor is not possible for a PSO, then there shall be an escrow arrangement for the source code to ensure continuity of services.

10. Are there any export controls that apply to software transactions?

Dual-use items such as software, technology, etc., which can be used for both civil and military applications require an authorization for exporting out of the country by the Directorate General of Foreign Trade. India maintains a list of items which need an export license called the Special Chemicals, Organisms, Materials, Equipment and Technologies (SCOMET) list. Different types of software are included in the list. Privacy laws discussed in this questionnaire can also kick in where transfer of personal data is involved. Specifically, the DPDPA allows the government to blacklist certain countries to which transfers of personal data shall be restricted.

11. Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

There are no specific technology laws that govern IT outsourcing transactions in India. The IT Act, its rules and the soon to be implemented DPDPA would form the main technology regulatory framework. As stated above, the DPDPA allows for cross border transfer of digital personal data, except to countries / territories that may be notified by the government.

Additionally, in April 2023, the RBI issued 'Master Direction on Outsourcing of Information Technology Service' for the financial sector. These directions have been effective since October 1, 2023.

12. Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

Labour / employment is a subject regulated by both the central and state governments in India. Therefore, different laws can apply in such a condition. These include the Industrial Disputes Act, 1947, which is one of the primary labour laws in the country. State-specific labour laws for termination/other accrued benefit entitlements, i.e., industrial disputes state rules, shops and establishments acts, employees' provident fund, gratuity, and insurance laws, can also apply. Other than these, the employment contracts of the individual staff and company policies would also be relevant in this context.

13. Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

The principal legislation governing the telecommunications space is the Telecommunications Act, 2023. This law deals with development, expansion and operation of telecommunication services and telecommunication networks, assignment of spectrums, and matters connected therewith or incidental thereto. It also regulates extra-territorial applicability, biometric verification for using telecommunication services, right of

way, critical telecommunication infrastructure, powers of interception by the Government, reduced penalties, etc. This Act replaces the Indian Telegraph Act, 1885 and the Indian Wireless Telegraphy Act, 1933. Not all provisions of the Act are currently in force. In late June and early July 2024, various provisions of the Act were brought into force – these include the right of way framework, common ducts and cable corridors, protection of users against unsolicited commercial communications, the establishment of a grievance redressal mechanism and an online dispute resolution framework, prohibition of use of equipment which block telecommunications, criteria for appointment as chairperson and members of Telecom Regulatory Authority of India ('TRAI'), etc.

Another relevant law is the Telecom Regulatory Authority of India Act, 1997, which deals with the establishment, appointment, and powers of the TRAI, which is the regulatory body governing the telecommunications space.

14. What are the principal standard development organisations governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

There are several governmental / quasi-governmental / private SSOs that play a crucial role in governing the development of technical standards related to mobile communications and emerging technologies such as digital health and connected and autonomous vehicles. Some of the principal SSO are:

i. **Bureau of Indian Standards (BIS)** – Established under the Ministry of Consumer Affairs, BIS is the national standard body / primary SSO of India for the harmonious development of the activities of standardization, marking and quality certification of goods, and for matters connected therewith or incidental thereto. BIS sets standards for a wide range of products and services, including those related to digital health and connected technologies, etc.
ii. **Telecommunication Engineering Centre (TEC)** – TEC is a technical arm of the Department of Telecommunications (DoT), under the Ministry of Communications. It is the **primary agency** responsible for the preparation of standards and specifications in the information and telecommunications sector and covers telecom network equipment, services, and interoperability.
iii. **Telecom Regulatory Authority of India (TRAI)** – In addition to its regulatory role, TRAI also helps in the development of standards and guidelines for telecommunications services and infrastructure. Among other things, it lays down standards of quality for services to be provided by the telecom service providers.
iv. **Automotive Research Association of India (ARAI) –** It is an autonomous body affiliated to the Ministry of Heavy Industries, Government of India and is the **prime testing and certification agency** notified by Government of India for motor vehicles. ARAI also has an autonomous vehicle development platform for development of ADAS / Autonomous vehicle functionality.
v. **National Health Authority (NHA) –** It is the apex body responsible for implementing India's flagship public health insurance/assurance scheme called "Ayushman Bharat Pradhan Mantri Jan Arogya Yojana" and has been entrusted with the role of designing strategy, building technological infrastructure and implementation of the National Digital Health Mission to create a National Digital Health Eco-system. Its roles include development and enforcement of compliance with standards for treatment protocols, quality protocols, minimum documentation protocols, data sharing protocols, data privacy and security protocols, fraud prevention and control including penal provisions, etc.

Additionally, there are private organization which also operate in this space. Some of these are:

i. **Telecommunications Standards Development Society of India (TSDSI) –** TSDSI is an autonomous, membership based, standards development organization for Telecom/ICT products and services in India and supported by the DoT. It works closely with global standards bodies to reflect Indian requirements into international telecom/ICT standards.
ii. **Global ICT Standardization Forum for India (GISFI) –** This is a standardization body active in the area of Information and Communication Technologies (ICT) and related applications.

15. How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Technical standards facilitating interoperability help in improving compatibility of technologies, reducing costs, increasing efficiency, fostering innovation, enhancing the safety and security of systems, etc. For instance, mobile communications standards like 5G ensure that devices

can operate across different networks globally, boosting the adoption of connected technologies and services. An Indian example is use of Unified Payments Interface (UPI) for mobile banking. UPI is a system that allows users to transact directly from multiple bank accounts in a single mobile application (of any participating bank), as well as merging several banking features, seamless fund routing and merchant payments under one hood. It is in use across India as well as in countries such as France, Singapore, United Arab Emirates, Bhutan, Nepal, etc. Technical standards also help in developing Industry 'best practices' and facilitates organizations to stay competitive.

16. When negotiating agreements which involve mobile communications or other connected technologies, are there any different considerations in respect of liabilities/warranties relating to standard essential patents (SEPs)?

SEPs are patents that protect technology essential to a standard. They are crucial in ensuring that devices and systems from different manufacturers are compatible and can work together seamlessly. In terms of liabilities, important considerations would include clear identification of its scope, identification of licensee for patent infringement, financial caps in the liability claim, etc. In terms of warranties, important considerations for mobile communication and connected technologies would include compliance of the SEP with applicable standards, warranty of performance as prescribed, duration of the warranty, etc.

17. Which body(ies), if any, is/are responsible for data protection regulation?

The data protection regime in India falls under the Ministry of Electronics and Information Technology (MeitY), Government of India. There is no standalone data regulator just yet, but one is likely to come up soon– see details below. Currently, actions relating to breach of personal data regulation are adjudicated upon by adjudicating officers appointed by the government. **Cert-In** has also been identified as the national agency for performing various functions in the area of cybersecurity. Cert-In draws its powers from IT Act.

There are also sector specific bodies, which issue additional regulations for their sectors. These include:

- **Reserve Bank of India** – For the financial sector, the RBI issues guidelines and regulations concerning data protection and cybersecurity.
- **Insurance Regulatory and Development Authority of India** – For the insurance sector, IRDAI issues data protection guidelines.
- **Telecom Regulatory Authority of India** – For the telecom sector, TRAI also engages in developing data protection regulation.

Further, under the soon to be implemented DPDPA, a **Data Protection Board of India ('DP Board')** will be set up and would shape up to be the principal data regulator in India. Its functions would include inquiring into personal data breaches, direct remedial and mitigation measures, adjudicating complaints by data principals / data subjects, and imposing penalties.

18. Please summarise the principal laws (present or impending), if any, that that govern data protection, including a brief explanation of the general purpose of those laws.

As provided in the preceding questions, India has enacted a bespoke data protection law for digital personal data, known as the Digital Personal Data Protection Act, 2023. Although it is notified in the Official Gazette as 'law', the DPDPA has not been officially implemented. Rules to implement the act are currently being framed by the Government and some progress is likely in the coming months. Once implemented, the DPDPA will regulate the processing of 'digital' personal data in India. The term 'processing,' defined similarly to the European Union's General Data Protection Regulation (GDPR), includes the collection of personal data. The DPDPA identifies data fiduciaries (entities that determine the purpose and means of processing personal data, akin to 'data controllers' under the GDPR), data processors (entities that process personal data, including on behalf of data fiduciaries), and data principals (individuals to whom the personal data relates). It outlines their obligations, rights, and duties. Furthermore, the DPDPA grants the Indian government the authority to regulate the transfer of personal data outside India, which is crucial for cross-border investigations.

The DPDPA upon its implementation will replace the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules 2011), which were established under the Information Technology Act 2000 (IT Act), and currently serve as the primary data privacy law in India. The SPDI Rules 2011 set out guidelines for the collection, processing, storage, and transfer of sensitive personal data or information in India. These

Rules define sensitive personal data to include information such as passwords, financial information, medical information, sexual orientation, and biometric data.

In addition to the above, there also exist certain sector-specific laws in fields such as banking, insurance, medicine or healthcare, and telecoms, which also regulate processing of certain types of personal data. There are also subordinate rules and regulations framed under the IT Act (other than SPDI Rules 2011) relating to data protection or privacy in specific scenarios. These will continue to apply, provided they do not conflict with the provision(s) of the DPDPA or are expressly repealed. If a sectoral law provides for higher obligation(s) than the DPDPA, then the obligations under the specific sectoral law may have to be met. These sectoral laws would similarly be relevant depending on the nature and/or scope of a given cross-border investigation. Some of these are:

- **RBI's direction on 'Storage of Payment System Data' dated April 6, 2018** – the RBI has issued a direction to all banks and Payment System Operators to store all payment data in systems located in India only, except in the case of cross-border transactions where a copy of the payment data, including the domestic component, may also be stored abroad.
- **Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015** – This requires that all insurers are to maintain records of their issued policies and claims, and these records, whether maintained electronically or otherwise, are to be maintained in India only.
- **RBI's PSO Master Directions 2024** – These mandate that PSOs shall prepare a Cyber Crisis Management Plan to detect, contain, respond and recover from cyber threats and cyber-attacks and follow guidelines of agencies such as Cert-In.

Other than these, the IT Rules 2021 & CERT-In Directions, discussed in the software section, also apply. For instance, the Cert-In Directions mandate that cybersecurity incidents (including data breaches) are to be reported to CERT-In within six hours of becoming aware of the incident, and a contravention of this directive carries with it penal provisions. Taking its cue from Cert-In, the RBI in its PSO Master Directions 2024 has mandated that in addition to reporting to Cert-In, incidents like cyber-attacks, outage of critical system / infrastructure, internal fraud, settlement delay, etc., shall also be reported to the RBI within 6 hours of detection.

19. What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

Previously, the IT Act governed sanctions and penalties related to personal data, imposing a fine of up to 2,500,000 rupees for non-compliance. The Digital Personal Data Protection Act (DPDPA) significantly enhances these penalties, with fines now reaching up to 2.5 billion rupees for failing to implement reasonable security safeguards. The Data Protection Board of India will determine penalties based on factors such as the nature, gravity, and duration of the contravention, as well as its repetitive nature. Decisions made by the DP Board can be challenged.

20. Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

In India, technology contracts generally focus on compliance with domestic data protection laws, such as the IT Act and its associated rules, including the SPDI Rules 2011. This is likely to continue and only increase once DPDPA is implemented since it provides a more comprehensive compliance framework and places the entire compliance burden solely on the data fiduciary.

That said, in some cases, especially when dealing with multinational companies who might have incidental obligations, these contracts may reference external data protection regimes like the EU GDPR or CCPA. With this, companies or individuals indulging in technology transfers can meet global standards and help protect data, meet demands, ensure consistent regulatory compliance and ultimately maintain data privacy and security.

21. Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

Currently, there is no dedicated body that is responsible for regulating artificial intelligence ('AI') in the country. While the MeitY is largely responsible for coming up with policies / laws that would govern AI, different sectoral regulators and government think-tanks also contribute to the space.

In 2018, MeitY instituted four Committees for promoting Artificial Intelligence (AI) initiatives and developing a policy framework – Committee on Platforms and Data for

AI; Committee on Leveraging AI for identifying National Missions in Key Sectors; Committee on Mapping Technological capabilities, Key Policy enablers required across sectors, Skilling and Re-skilling, R & D; and Committee on Cyber Security, Safety, Legal and Ethical Issues. All four committees have since tendered their reports, which are publicly available.

The Ministry of Commerce and Industry has also set up an 'Artificial Intelligence Task Force', which claims its aim is the integration of AI for India's economic transformation.

22. Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

Currently, there is no *sui generis* law governing AI in the country. Different existing laws / guidelines / policies regulate the deployment and use of AI in the interim. These include:

- **IT Act** – As has been established in this questionnaire, the IT Act is the primary legislation for regulating all things online / digital in India. The IT Act along with its rules such as the SPDI Rules 2011 and IT Rules 2021 come into the picture in regulating AI to some extent.
- **MeitY's Advisory on deepfakes** – In November & December 2023, MeitY issued advisories to social media intermediaries under the IT Act and IT Rules 2021 to regulate misinformation on their platforms by AI generated deepfakes.
- **Meity's Advisory on Large Language Models and/or generative AI –** This was released on March 15, 2024. Please see details in the next question.
- **DPDPA** – The soon to be implemented law will have implications for deployment and use of AI where they would concern digital personal data. This is likely to have implications for Generative AI. However, it is relevant to note that the DPDPA is not applicable to personal data available in the public domain.
- **The Consumer Protection Act, 2019** – The Consumer Protection Act can come into play and govern AI, if we consider AI systems as a product or a service from the point of view of a customer.
- **Guidelines for Prevention and Regulation of Dark Patterns, 2023** – The Central Consumer Protection Authority issued these guidelines which prohibit entities (including AI service providers) from engaging in dark patterns such as false urgency, basket sneaking, subscription trap, bait and switch, drip pricing, etc.
- **National Data Governance Framework Policy 2022 –** This was a draft policy released by MeitY to transform and modernize government data collection and management processes and systems. One of its core objectives is to enable and catalyse vibrant AI and data led research and start-up ecosystem, by creating a large repository of India datasets.
- **National Strategy for Artificial Intelligence (NSAI) & its subsequent papers –** This was policy document released by the NITI Aayog (Government of India's primary think-tank) in 2018 to guide the development and deployment of AI in India. In continuation of the NSAI, NITI Aayog also released policy documents on Principles for Responsible AI in 2021 and on AI for Facial Recognition Technology in 2022. These documents are important because they give a sneak peek into the government's view on AI and also help in shaping relevant policies.
- **TRAI's recommendations on 'Leveraging Artificial Intelligence and Big Data in Telecommunication Sector' –** On July 20, 2023, TRAI issued its recommendations for regulation and use of AI in the telecom sector. These include an independent statutory authority for AI, categorizations of AI use cases based on their risk, and regulating them according to broad principles of Responsible AI.
- **BIS' draft Indian standard on AI –** In January 2024, the BIS released the draft Indian equivalent of IS/ISO/IEC 42001:2023 which provides guidance for establishing, implementing, maintaining, and continually improving an AI management system within the context of an organization.
- **IPR Laws** – Deployment and use of AI is also regulated by the Copyright Act, 1957 and the Patents Act, 1970 so far as they concern content / inventions generated by and/or using AI.
- **Economic Advisory Council (EAC) to the PM's Complex Adaptive System Framework to Regulate Artificial Intelligence** – Recently in January 2024, EAC to the PM published guidelines in the form of 5 key principles for regulating AI in India.
- **Nasscom's Responsible AI** – Guidelines for Generative AI – The National Association of Software and Service Companies (Nasscom) in June 2023 published these guidelines for researchers, developers and users of generative AI for responsible use of AI.
- **Telecommunication Engineering Centre's Fairness Assessment and Rating of Artificial Intelligence Systems** – The Telecommunication Engineering Centre under the Department of Telecommunications, in July 2023 published a framework for monitoring the fairness in AI systems.
- **Indian Council of Medical Research (ICMR)** – Ethical

Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare – ICMR published voluntary guidelines with 10 principles of ethical AI to deal with AI-related issues in the healthcare industry.

23. Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI?

MeitY released an advisory on March 15, 2024, for intermediaries and platforms under the IT Rules 2021 in relation to use of AI model(s) / LLM / Generative AI. Under the advisory, intermediaries and platforms have been instructed to insure, *inter alia,* that:

- Use of AI model(s) / LLM / Generative AI, software(s) or algorithm(s) on or through its computer resource does not permit its users to host, display, upload, modify, publish, transmit, store, update or share any unlawful content under law.
- Use of AI model(s) / LLM / Generative AI, software(s) or algorithm(s) does not permit any bias or discrimination or threaten the integrity of the electoral process.
- Under-tested/unreliable AI foundational model(s) / LLM / Generative AI, software(s) or algorithm(s) or further development on such models should be made available to users in India only after appropriately labeling the possible inherent fallibility or unreliability of the output generated. Further, "consent popup" or equivalent mechanisms may be used to explicitly inform the users about the possible inherent fallibility or unreliability of the output generated.

This advisory was issued in subversion of an earlier advisory, which had a provision requiring seeking permission from MeitY before deployment of AI model(s) /LLM/Generative AI but faced resistance from the industry.

24. Do technology contracts in your jurisdiction typically contain either mandatory (e.g mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

Currently, there is no explicit mandate under law to incorporate provisions dealing with AI risk in technology contracts in India. However, it would be advisable to take into account the laws and regulations discussed in the previous questions while negotiating such contracts. Their incorporation would have to be determined on a case to case basis.

25. Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

Depending on the facts and circumstances of such contracts, it may be advisable to include provisions relating to intellectual property rights. This would especially be the case where issues such as ownership of data / outputs and inventions generated by and / or using AI are concerned.

26. What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

There is no *sui generis* law covering either blockchain technology or digital assets. In 2018, the RBI had imposed a virtual ban on cryptocurrencies in the country. This ban was set aside by India's Supreme Court in 2020. This was followed by an attempt to legislate the domain, and the government indicated an intention to introduce the 'Cryptocurrency and Regulation of Official Digital Currency Bill' in 2021. It was reported that the purpose of the bill was to create a facilitative framework for creation of the official digital currency to be issued by the RBI and also to prohibit all private cryptocurrencies in India with certain exceptions. However, this bill never saw the light of day.

With that context, there are other laws / regulations / guidelines, which operate in relation to blockchain and digital assets. With regards to blockchain, MeitY released the '**National Strategy on Blockchain**' in 2021. This strategy aims to establish a comprehensive framework for the adoption and implementation of blockchain technology across various sectors in India. While not legally binding, it focuses on creating a national Blockchain infrastructure to enhance transparency, security, and efficiency in digital transactions and services. In February 2024, the RBI issued its latest version of '**Enabling Framework for Regulatory Sandbox'**,

which allows a safe and protected environment for innovators, Fintechs, etc., to test their product before taking it to the market. The products allowed include *applications under blockchain technologies* but expressly exclude crypto currency / crypto assets services.

Digital assets, particularly virtual currencies like cryptocurrency, have been more in focus, and legislative efforts to regulate them have gone beyond the 2021 bill discussed above. The Income Tax Act, 1961 has been amended, *inter alia,* to define the term 'Virtual Digital Asset'. It broadly means any information or code or number or token (not being Indian currency or foreign currency), generated through cryptographic means, and also includes NFTs and any other digital assets as the government may notify. This definition is the primary source of reference for other applicable laws, which are listed below.

- **Companies Act, 2013 –** This is primary company law in India. In 2021, the government had amended this act to make reporting of crypto / virtual currency mandatory for companies.
- **Prevention of Money-laundering Act, 2002 ('PMLA') –** This is the primary law to combat money laundering and has stringent penal provisions. Vide a notification dated March 7, 2023, all entities dealing with virtual digital assets and fiat currencies were brought under the ambit of this law. Under the PMLA, the Financial Intelligence Unit – India ('FIU-IND') has mandated that all Virtual Digital Asset Service Providers have to register themselves with FIU-IND. Further, they have also issued 'Anti Money Laundering & Countering the Financing of Terrorism Guidelines For Reporting Entities Providing Services Related To Virtual Digital Assets', which have to complied by such entities.
- **Cert-In Guidelines –** These also cover block chain, virtual assets, virtual asset exchanges and are mandatorily applicable on the industry.
- **Foreign Exchange Management Act, 1999 and its rules** are also applicable where cross-border transfer of digital assets is involved.

Lastly, as part of its digital push, the RBI also launched the first pilot for digital Rupee (eINR / e -R). The e -R is in the form of a digital token that represents legal tender.

27. Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

There is no sui generis law covering search engines and marketplaces. Different laws across taxation, privacy, competition, consumer protections, etc., govern different aspects, with the primary purpose of promoting fair competition, protecting consumer rights, and ensuring secure online transactions. Some of the primary laws include:

- **IT Act and its rules**– The IT Act covers online transactions, cybersecurity, etc., and has contains safe harbour provisions for entities. The IT Rules 2021 are also applicable and provide mandatory guidelines covering posting of privacy policies and terms of use, taking reasonable steps to ensure that objectionable content is not made available on the service, and addressing user grievances. , Further, the SPDI Rules 2011 govern the collection and handling of personal data, and as discussed above, these will be replaced with the DPDPA in the near future. Cert-In Guidelines also kick in when issues of cyber security incidents get involved.
- **Foreign Direct Investment ('FDI') Policies –** Under the current framework, 100% FDI under automatic route is permitted in the marketplace model of e-commerce subject to certain conditions.
- **Central Goods and Services Tax Act, 2017 –** Nearly all transactions across search engines and marketplaces entail the collection of GST.
- **Payment and Settlements Systems Act, 2007**– This law regulates the payment and settlement systems in India, including those used by search engines and marketplaces.
- **Legal Metrology Act, 2009 & Legal Metrology (Packaged Commodity) Rules, 2011** – These regulate the manner of measuring and packaging of products in India, including through online means.
- **Drugs and Cosmetics Act, of 1940 –** This law has implications on online sale of drugs and cosmetics in the country and cover issues such as quality, labelling, etc.
- **Consumer Protection Act, 2019 & Consumer Protection (E-commerce) Rules, 2020** – These are consumer centric laws which regulate online marketplaces by providing rights of consumers, and duties and liabilities of platforms. These include mandating transparency in product information, establishing grievance redressal mechanisms, etc.
- **Competition Act, 2002** – This law deals with anti-competitive practices in the market and promotes fair competition among businesses.
- **Intellectual Property (IP) laws**: Various IP laws such

as the Copyright Act, 1957 and Trademark Act, 1999 also come into the picture and deal with creators' rights, prevent infringement, etc.

28. Please summarise the principal laws (present or impending), if any, that govern social media, including a brief explanation of the general purpose of those laws?

Many of the laws discussed in the preceding questions are applicable to social media to some extent. Amongst those, the principal law relevant to social media is the IT Rules 2021. The IT Act, SPDI Rules, Cert-In Guidelines and soon to implemented DPDPA would also apply.

The IT Rules 2021 provide definitions for 'social media intermediary' and 'significant social media intermediary'. These rules put various obligations on social media platforms including publishing of a privacy policy and terms of use, taking "reasonable efforts" to restrict certain categories of content, and govern issues such as collection and temporary storage of information, reporting of cyber security incidents, etc. The rules also provide for a grievance redressal mechanism and employing a Grievance Officer, whose contact details have to be prominently published on the website and/or mobile application.

On significant social media intermediaries (currently covering platforms with over 5 million users), the rules put additional obligations such as appointing a Chief Compliance Officer, a nodal contact person for 24×7 coordination with law enforcement agencies and officers as well as a Resident Grievance Officer, who would be an Indian resident employee of company. There are various other additional obligations as well such as publishing a monthly compliance report, implementing technology-based measures to filter objectionable content, etc.

29. What are your top 3 predictions for significant developments in technology law in the next 3 years?

India is going to see a lot of churns in its technology laws in the next 3 years as the government focuses on its Digital India Initiative. The top 3 expected changes in the near future are:

1. Implementation of the DPDPA along with its rules. Once implemented, the DPDPA will govern the Indian digital personal data regime and replace the currently applicable SPDI Rules 2011. It is expected that the industry would be given suitable time to adopt its provisions.
2. Replacement of the IT Act by the Digital India Act. It has been reported that the government has already held industry consultations on the Digital India Act, which will aim replace the two decades old IT Act and bring India's technology laws up to date.
3. Progress and regulations on artificial intelligence. With the growing use of AI and its impact on issues across the spectrum, the government is likely to undertake stricter measures to regulate AI and to ensure that necessary safeguards are put in place. It has also been reported that regulations governing AI use may be included within the Digital India Act.

30. Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Inclusion of provisions specifically addressing sustainability or net-zero obligations is not yet a widespread practice in technology contracts in India. However, there is a growing awareness and gradual integration of environmental commitments in business practices, driven by both global trends and regulatory developments. As such, companies have started introducing ESG commitments as part of their Corporate Social Responsibility obligations.

Contributors

Sherry Shukla
Associate
sherry.shukla@gnwlegal.com

Hardik Choudhary
Associate
hardik.choudhary@gnwlegal.com

Dhruv Singh
Counsel
dhruv@gnwlegal.com

Arjun Khurana
Partner
arjun@gnwlegal.com