UPDATES

Technology, Media & Telecommunications Law – Legal Milestones in 2019 and a Look Ahead

28 February 2020

This update covers:

1 The Year that Was

2019 was a busy year for this sector as the Government of India introduced several regulatory measures and policy initiatives which is likely to have a long-term impact on the sector. This update summarises some of the major developments in the past year and gives a brief overview of what can be expected in 2020.

The year 2019 saw many changes in terms of regulatory and legislative measures by the Government as well as judgments by the Supreme Court. The introduction of the Personal Data Protection Bill, 2019 before Parliament was a watershed moment in the history of privacy rights in India. Further, as a direct result of the Supreme Court's ruling on Aadhaar, the Government introduced changes to the legislative scheme surrounding Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Aadhaar Act) to put in place more robust mechanisms for identity verification. Additionally, the Government rolled out regulatory initiatives relating to e-commerce, regulation of information technology intermediaries, and consumer protection.

The year 2019 also saw the introduction of a foreign direct investment (FDI) cap of 26% for circulation of news and current affairs through digital media. While it is not yet clear how this will affect news aggregators and intermediaries, it nevertheless is an important development in the regulation of online news media by the Government.

Government bodies also undertook consultation processes in various fields such as artificial intelligence, non-personal data, provision of cloud services, and other service providers (OSP) whose potential impact remains to be seen. The involvement of stakeholders in formulating recommendations on these subjects is a step forward in policymaking in the technology and telecommunication sector in India.

2 Major Developments in 2019

2.1 Technology and Data Protection

2.1.1 Personal Data Protection Bill 2019

The existing legislative framework in India to address issues of privacy of citizens' data comprises of the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. It covers some basic tenets for the collection, storage and processing of information about certain identified categories of 'sensitive personal data or information' of natural persons such as financial information and health data.

However, after the Supreme Court recognised the privacy of individuals as a fundamental right under the Constitution of India and highlighted the need for privacy legislation in 2017, the Government set up a committee of experts (Committee) to look into the contours of such a law. The Committee came up with a draft Personal Data Protection Bill (2018 Bill) after expansive consultations in 2018. The 2018 Bill introduced the concepts of '*data fiduciaries*' and '*data principals*', as opposed to the more commonly used terms '*data controller*' and '*data subject*'. It envisages a fiduciary relationship between the data fiduciary and data principal wherein the data fiduciary must act in the best interest of the data principal. Any natural person whose

personal data is collected was referred to as the '*data principal*' and the entity that determines the purpose or means of processing this data was referred to as the '*data fiduciary*'.

After the 2018 Bill, the Government conducted a series of consultations and a revised Bill (2019 Bill) was released in December 2019 and is currently placed before a joint parliamentary committee for examination and stakeholder consultation is underway. The 2019 Bill introduced several important changes to the 2018 Bill, as follows.

- Data Localisation

  The 2018 Bill required the storage of a serving copy (which can be interpreted as a live copy) of all personal data (PD) covered by the Bill, on a server or data centre located in India. It also mandated the processing of 'critical personal data' (CPD) only in India. Further, even data that did not fall within this category could only be transferred outside India subject to satisfaction of specific conditions. However, the 2019 Bill does not mandate localisation of PD that does not qualify as sensitive personal data (SPD) or CPD. Moreover, it provides that with the explicit consent of the data principal and the satisfaction of specific conditions, SPD may be transferred outside India for processing. However, such SPD will have to be stored in India as well.

- Significant Data Fiduciaries

  A regulatory body called the Data Protection Authority (DPA) is envisaged under the 2019 Bill. The DPA is required to notify certain data fiduciaries (or classes of data fiduciaries) as '*significant data fiduciaries*' based on factors such as the volume of personal data processed, sensitivity of the data processed, annual turnover of the data fiduciary, the risk of harm from any processing undertaken by the data fiduciary, use of new technologies, and any other factor that may cause harm to any data principal as a result of any processing. These significant data fiduciaries are required to register themselves with the DPA.

  The 2019 Bill introduces the construct of *'social media intermediaries'*, which are entities that primarily or solely enable online interactions between users and allow information exchange between them. The Central Government can notify those social media intermediaries that have a specified number of users, and whose actions are likely to have a significant impact on electoral democracy, security of the state, public order, or the sovereignty of India, as significant data fiduciaries. In addition to the general obligations of significant data fiduciaries, these social media intermediaries will also be required to enable voluntary verification of accounts of their Indian users. This appears to be a measure to curb the spread of fake news through social media platforms.

- Mandatory sharing of non-personal data

  The 2019 Bill seeks to provide the Government with the ability to requisition personal data in anonymised manner. Further, it extends this right of the Government to non-personal data which is outside the scope of the 2019 Bill. Under the 2019 Bill, the Government in consultation with the DPA may direct any data fiduciary or data processor to provide any PD anonymised or other non-PD (i.e. data other than PD) to enable '*better targeting of delivery of services*' or '*formulation of evidence-based policies*'.

- Surveillance

  The 2019 Bill allows for surveillance activities by the Government. The Government may direct that any or all provisions of the 2019 Bill will not apply to any government agency. Unlike the 2018 Bill, such a direction by the Government under the 2019 Bill does not require the passing of a law by the Parliament.

- Regulatory Sandbox

  Regulatory sandboxes are crucial for innovation in technology. To this end, the 2019 Bill proposes to introduce a sandbox for data fiduciaries working with emerging technologies. During the period in which they are included in the sandbox, the compliance burden of data fiduciaries associated with their data-related activities would be relaxed to some extent. However, the extent of this regulatory relaxation will only become clear once the safeguards including terms and conditions specifying consent requirements, compensation and penalties are specified by the DPA.

2.1.2 Non-Personal Data

During its deliberation on the 2018 Bill, the Committee had recognised the need to protect non-personal data including community data and recommended a separate consultation process for this. The Government has also on several occasions, indicated its intentions to regulate use of non-personal data.

In the discussion paper on *National Strategy for Artificial Intelligence* (AI) by the Government's think tank NITI Aayog, it was indicated that the Government may make a large amount of data that it holds on climate, non-strategic remote sensing, regional language speech, soil health etc., freely available for public good. The draft National E-Commerce Policy and the National Economic Survey 2018-19 also recognised the economic value of non-personal data for public good and compared it to a national asset over which citizens can exercise an inherent sovereign right. The idea here is that data originating in India belongs to the Indian people as a collective and would be held in trust on their behalf by the Government.

Subsequently, in September 2019, the Ministry of Electronics and Information Technology established a committee of experts to devise a framework for regulation of non-personal data and highlighted the need to recognise the economic dimension of data in its various forms such as aggregate data, derived data, anonymous data, e-commerce data, AI training data, etc.

2.1.3 Intermediaries

Safe harbour protection is available to information technology intermediaries such as social media platforms under the IT Act and the Information Technology (Intermediary Guidelines) Rules, 2011 (Intermediary Guidelines). The Government has proposed changes to this regime through the new draft Information Technology (Intermediaries Guidelines) (Amendment) Rules, 2018 (Amendments). The Amendments seek to introduce new restrictions and obligations on intermediaries to avail protection against liability for any third party information hosted on their platform. One of the new requirements proposed by the Amendments is for intermediaries with more than 5 million users in India toincorporate a company in India. Other proposed changes include requiring intermediaries to enable the tracing of originators of information on its platform and deploy technology-based automated tools or mechanisms to proactively identify and remove or disable public access to unlawful information or content.

The Government had represented before the Supreme Court (which is hearing several petitions relating to encryption breaking and traceability) that it will notify the Amendments by 15 January 2020. However, this has not been done yet. The interpretation garnered by the Supreme Court in these cases will have far-reaching implications on analysing liabilities on intermediaries in India, given that the definition of 'intermediary' is very broad and includes any party receiving, transmitting, storing or processing any third party information or providing any service with respect to that information. Therefore, all kinds of service providers, search engines, online payment sites etc., will be covered within this definition.

2.1.4 Draft e-commerce Guidelines

To ensure protection for consumers transacting on e-commerce platforms, the Government has issued a draft Consumer Protection (e-Commerce) Guidelines, 2018 (Draft Guidelines) under the Consumer Protection Act, 2019. The Draft Guidelines define an '*e-commerce entity*' to include even an electronic service provider who may be merely providing technologies or processes to enable sellers to engage in advertising or selling of goods or services to a consumer. The Draft Guidelines, among other things,seek to require all e-commerce entities carrying on B2C e-commerce in India to register as a legal entity under Indian laws and impose several obligations on e-commerce entities to ensure consumer protection. The consultation process for the Draft Guidelines concluded in September and are expected to be finalised by early 2020.

2.1.5 Developments in relation to Aadhaar

Aadhaar is a unique 12-digit number issued to Indian residents, based on their biometric and demographic data and is managed by the Unique Identification Authority of India (UIDAI). From the time of its introduction, Aadhaar has been mired in controversy for its privacy implications, its constitutionality, the steps taken by the Government to enroll persons under the Aadhaar program etc. In September 2018, the Supreme Court, in a landmark judgment, upheld the constitutional validity of Aadhaar project. However, it read down provisions of the Aadhaar Act that enabled private parties to use Aadhaar authentication services offered by the UIDAI under a private contract. It also struck down the mandatory requirement of linking the Aadhaar number with bank accounts and mobile numbers.

In 2019, the Government introduced several amendments to the Aadhaar Act. The amendments allow Aadhaar holders to verify their identity through specified offline modes without authentication (that is, the querying of the biometric database to verify a person's identity). The voluntary use of the Aadhaar number in physical or electronic form for identity verification, by way of authentication or offline verification, has also been expressly permitted. The entities performing authentication and offline verification are now required to adhere to higher security standards while undertaking such processes. Further, a recent amendment to the Prevention of Money Laundering (Maintenance of Record) Rules, 2005 specifically authorises banks to carry out authentication using Aadhaar data available with UIDAI for KYC compliance purposes, if the bank's client has submitted Aadhaar number voluntarily. Notably, the civil penalties that can be imposed on non-compliant entities in the Aadhaar ecosystem may now extend up to Rs. 10 million for each contravention, and in the case of continuing violations, can lead to an additional penalty of Rs. 1 million per day.

2.1.6 FDI Policy for digital media

The Government has recently introduced the FDI policy pertaining to the uploading/streaming of news and current affairs through digital media. The Foreign Exchange Management (Non-debt Instruments) (Amendment) Rules, 2019 state that 26% FDI is allowed for digital media outlets involved in uploading/ streaming of news and current affairs. The restriction is similar to existing restrictions on print media.

However, '*digital media*' is yet to be defined and therefore it is not clear as to whether only entities which have direct relationships with online news publishers and which stream news and current affairs will fall under the ambit of the term or whether online aggregators and intermediaries, as well as applications that technically '*upload*' and '*stream*' news and current affairs only by providing links to other news websites will be covered by the amended policy.

2.1.7 Reserve Bank of India (RBI) Guidelines on Regulatory Sandbox

The RBI released the Guidelines on Regulatory Sandbox that will allow live testing of new products or services in a controlled or test regulatory environment. Such a regulatory sandbox allows the regulator, innovators, financial service providers and customers to conduct tests in live environment to collect evidence on the benefits and risks of new financial innovations, while monitoring and containing their risks. The Guidelines on Regulatory Sandbox provide for fintech companies such as start-ups, banks, financial institutions or any other company partnering with or providing support to financial service businesses to be potential applicants to participate in the regulatory sandbox.

In order to be eligible for participation, an entity must be either incorporated and registered in India or a bank licensed to operate in India; have a minimum net worth of Rs. 2.5 million as per its latest audited balance sheet; demonstrate that the products/services are technologically ready for deployment in the broader market; have adequate safeguards built into its IT systems to ensure that it is protected against unauthorised access, alteration, destruction, disclosure or dissemination of records and data; and have robust IT infrastructure and managerial resources. The entity must also highlight an existing gap in the financial ecosystem and demonstrate how it would address the problem in the proposal and certain other additional requirements specified in the Guidelines on Regulatory Sandbox.

However, the Guidelines are not clear on certain points such as the start and end date of the Regulatory Sandbox, its target customer type, limits on the number of customers involved, transaction ceilings and caps on customer losses. Further, in the event of discontinuation of the regulatory sandbox, it is unclear how the existing obligations to the customers of any financial service will be fulfilled or addressed.

Further, some of the products, services and technologies that are not currently accepted for testing are cryptocurrency or crypto assets services; credit information; trading, investing or settling in crypto-assets and initial coin offerings.

2.2 Telecommunications

2.2.1 Supreme Court's Judgment on Adjusted Gross Revenue

The Supreme Court in *Union of India vs Association of Unified Telecom Service Providers of India etc*. upheld the Telecom Disputes Settlement and Appellate Tribunal's order that certain non-telecom revenues like rent, profit on sale of fixed assets, dividend and treasury income would be included in the definition of Adjusted Gross Revenue, on which a proportionate license fee would have to be paid by telecom licensees to the Government. Thereafter, the Department of Telecommunication (DoT) had issued notices to all telecom operators directing them to pay their revenue share on a self-assessment basis and submit documents such as their revenue statements to ensure compliance in accordance with the order of the Supreme Court. Thereafter, the telecom operators filed review petitions in the Supreme Court that were also dismissed.

Subsequently, the Government has also stated that the applicability of this judgement will be extended to all licensees and not just to the telecom operators who were a part of the dispute. However, more clarity on this is awaited from the Government's end on how it will go about enforcing the judgement.

2.2.2 Recommendations regarding OSPs

On 21 October 2019, the Telecom Regulatory Authority of India (TRAI) issued its recommendations for revising the framework for Other Service Providers (OSPs). OSPs are entities registered as Other Service Providers with the DoT. The TRAI recommends limiting the applicability of the OSP registration framework to providers of voice-based services on an outsourced basis, i.e. on behalf of another entity. Captive contact centres, i.e.,

entities that provide services to their own customers or employees, will be exempted from the registration requirement and OSPs providing services that are purely based on data/internet and involve no voice connectivity would be required to only go through an intimation process.

The TRAI also recommends the relaxation of registration requirements relating to OSPs, such that only OSPs providing voice-based services i.e. using voice call or voice-based applications, would have to register. Further, the requirement of getting multiple registrations for multiple OSP centres is recommended to be done away with, and a single registration for multiple OSP centres of one company will be introduced.

Another recommendation is with respect to contact centre service providers and hosted contact centre service providers. These are service providers who provide call centre infrastructure such as EPABX, IVR, call handling, customer relationship management etc., through their data centers or cloud facilities. The TRAI has recommended that these service providers must be Indian companies and registered as OSPs with the telecom department. Further, if the service providers are involved in the resale of telecom resources to OSPs they must obtain a virtual network operator telecom license from the department.

Another significant liberalisation is with respect to the work from home permission required for the agents of OSPs. OSPs were not permitted to allow agents to work from home unless the OSPs submitted a bank guarantee and obtained permission from the DoT. They were also required to ensure the availability of a provider-provisioned VPN to the home agent's location to get the permission in the first place. The cost and impractically of the provider-provisioned VPN deterred most OSPs from taking such a permission. Therefore, the TRAI has recommended doing away with the provider-provisioned VPN-requirement.

The current regime also requires OSPs to provide bank guarantees of up to Rs. 10 Million for permissions for sharing infrastructure and work from home permission. The TRAI has recommended doing away with the bank guarantee requirement. However, strict penalties for violation of conditions relating to work from home and infrastructure sharing are now proposed to be directly imposed under the OSP regime.

These recommendations will become law if and when implemented by the Government and it remains to be seen whether all the recommendations are adopted as law.

2.2.3 Mandatory Testing and Certification of Telecom Equipment (MTCTE)

The Indian Telegraph Rules, 1951 through a recent amendment provided that any telecom equipment which is used or capable of being used with any licensed telecommunication network must undergo prior mandatory testing and certification in respect of parameters as determined by the DoT. This process is the newly notified MTCTE, administered by the Telecommunications Engineering Centre under the Ministry of Communications. The Telecommunication Engineering Centre notified 1 October 2019, as the date from which all telecom equipment will be subject to certification under the MTCTE procedure and has launched a portal for facilitating this process.

2.2.4 Consultation Paper on Cloud Services

TRAI has released a Consultation Paper on Cloud Services as a follow up on its previous recommendations of 2017. This Consultation Paper focuses on the terms and conditions, eligibility, entry fee, etc. for registration of cloud service providers (CSPs).

TRAI had previously recommended that all CSPs above a threshold value should be required to become members of one of the registered industry bodies for cloud services (IBs) and accept the code of conduct prescribed by such body, which would include provisions for definitions, billing models, data security and dispute resolution frameworks. Such threshold may be based on either volume of buisness, revenue, number

of customers, etc. or a combination of all these. The Consultation Paper also deliberates on the frameworks surrounding IBs.

3 Looking Ahead

2019 was an important year for technology regulation and policy-making and 2020 is likely to continue this trend specifically in the area of e-commerce, intermediaries and data protection. The enactment of the Personal Data Protection Bill should put in place a data protection regime for India that is in line with global standards.

The amendments to the Intermediary Guidelines are also awaited by various business platforms operating in India because of its far-reaching consequences for social media companies. With India being host to one of the world's largest outsourcing industries, the recommendations for revising the OSP framework should lead to the removal of onerous compliances.

The Government is also undertaking a series of consultation in varied fields such as cloud computing, over-the-top media services as well as video, artificial intelligence and regulation of non-personal data. Further, we are likely to see legislation and policy statements around data localisation, local incorporation requirement and regulation of both personal and non-personal data.

For a round-up of some of the key legal developments across sectors in 2019 and a brief insight on what to expect in 2020, please read our sector-wise updates, which can be accessed at: https://trilegal.com/knowledge-repository/page/2/?title=milestone