TRILEGAL

Rewriting India's decades-old technology laws in 2023

By: Nikhil Narendran (Partner) and Karishma Sundara (Counsel)

India's technology law framework is set for a significant revamp in 2023. In March, the Government began the consultation process for the long-awaited Digital India Act (DIA). Representatives from the Ministry of Electronics and Information Technology met with stakeholders across the industry to unveil the rationale for replacing the two-decades-old Information Technology Act, 2000 (the IT Act). A draft of the DIA, though expected at the end of April, is yet to be released.

The decision to consult stakeholders on the DIA comes close on the heels of the Government's publication of the draft data protection law, the Digital Personal Data Protection Bill, 2022 (DPDP Bill), which was released for public consultation in November 2022. The DPDP Bill adopts a simpler approach to data protection as against its predecessors, which were more closely modelled on the General Data Protection Regulation. A revised draft of the DPDP Bill (whose final form remains unknown) is, however, expected to be introduced in Parliament this July or August. Both the DIA and the DPDP Bill are likely to considerably change how businesses reliant on the internet operate.

Out with the old and in with the new: what to expect as we move from the IT Act to the DIA

The DIA is expected to focus on:

1. ensuring an open internet
2. online safety and trust
3. accountability and quality of service
4. an adjudicatory mechanism for timely grievance redressal, and
5. a framework to address harms that may be caused by new technologies (such as, artificial intelligence).

The Government cited these changes as being necessary in view of the changing technology landscape, but provided limited information on how these goals will be implemented.

Challenges with replacing the IT Act

Replacing the IT Act with the DIA will be no mean feat. As the parent technology law statute, the IT Act specifies, among other things, the definition of an electronic record; preconditions for safe harbour immunity for intermediaries; lawful interception and content-blocking procedures; cyber offences; reporting and managing cyber security incidents; and protective conditions accruing to sensitive personal data. Dismantling the IT Act will also mean dismantling every piece of delegated legislation framed under the IT Act, from regulations prescribing critical procedural safeguards that government agencies must follow, to intermediaries' due diligence obligations.

Reframing cyber security incident response mechanisms

A lacuna that the DIA hopes to address is the absence of a coordinated cyber security incident response mechanism. The existing framework consists of certain rules that were prescribed under the IT Act in 2013 (2013 Rules), which (until 2022) solely governed the identification and reporting of cyber security incidents to the Indian Computer Emergency Response Team (CERT-In), the cybersecurity regulator. Now, certain more recent directions issued by CERT-In in 2022 (2022 Directions) govern this space alongside the 2013 Rules. One of the practical issues with this framework is that it creates a dual assessment procedure: prior to reporting an incident, entities must determine if the event constitutes a cyber incident and/or a cyber security incident (which are defined differently). This is complicated by the fact that the list of cyber security incidents accompanying the 2013 Rules and the list of cyber incidents accompanying the 2022 Directions identify an overlapping category of events. This complexity is furthered by the requirement to report certain cyber incidents within a shorter timeframe, while certain other kinds of cyber security incidents may be reported to CERT-In as soon as reasonably practicable. It is possible that the DIA will condense the identification and reporting mechanisms under both regimes into one, clarify the nature of incidents to be reported to CERT-In, and expand and strengthen CERT-In's powers and functions.

Reimagining intermediaries and safe harbour immunity

The Government intends to introduce certain new provisions and revisit other concepts that are central to the IT Act. For instance, the DIA will re-evaluate:

1. how intermediaries are classified, and identify separate classes of intermediaries based on the function they serve (eg, e-commerce; digital media; search engines; gaming; cloud services)

2. whether all intermediaries should be eligible for safe harbour immunity, and

3. the rules that should apply to each class of intermediary.

Other considerations

The DIA also aims to address other issues emanating from advancements in technology, such as:

1. the identification and adjudication of newer forms of online harms (eg, revenge porn, cyber-bullying, and doxxing), as well as a regulatory framework for enforcement

2. content regulation and monetisation

3. regulating high-risk artificial intelligence systems and associated user harms, and

4. preventing concentration of market power and gatekeeping to ensure non-discriminatory access to digital services.

Protecting digital personal data in India in 2023 - how novel is it?

Like the DIA, the DPDP Bill revisits and reconceptualises a segment of Indian technology law: data protection and data privacy. Today, the space is governed by a lean regulatory framework designed primarily to protect sensitive personal data: the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. While the law was not out of sync for the India of 2011, it lags behind considerably in 2023. India's much-anticipated data protection law, the finalised DPDP Bill, is expected to become law by the end of the year. Before this happens, though, it must be introduced in Parliament, where it will likely be debated and potentially amended, before it receives presidential assent. If it succeeds, it will mark the end of a 6-year journey to establishing a comprehensive legal framework to govern how personal data is handled in India.

The DPDP Bill is slimmer than its predecessors (the Personal Data Protection Bill, 2019, and the draft Data Protection Bill, 2021) and other data protection regimes, leaving many asking whether it is simpler, or just simplistic. The DPDP Bill predictably features concepts that are central to global data protection frameworks like the GDPR, ie, placing data fiduciaries (the equivalent of data controllers); data principals (the equivalent of data subjects); and data processors at its core. Similarly, it also draws heavily on cross-jurisdictional precedents in other aspects (eg, cross-border transfers of personal data) with hybrid results. It does not, however, follow the pack in several significant ways. For instance, the DPDP Bill shrinks the ambit of 'personal data' and dispenses with segregating and protecting personal data based on how sensitive it is.

What processing activities will be governed under the proposed law?

Like the GDPR, the location of the processing is irrelevant. Under the DPDP Bill, as long as there is some nexus to India, the processing activity will likely fall within the Bill's ambit. Specifically, it will govern processing of personal data within India where personal data is collected from data principals online or collected offline and then digitized. Similarly, processing of personal data outside India will come within the Bill's purview provided it is in connection with any profiling of, or activity of offering goods or services to data principals within the territory of India. Personal data that is:

1. not processed using automated means (defined broadly to include any computer based processing)

2. offline in nature

3. processed by an individual for any personal or domestic purpose, or

4. about an individual and contained in a record that is at least 100 years old is excluded from the ambit of the DPDP Bill.

Notably, the DPDP Bill does apply to processing of personal data of non-resident data principals. Such processing is subject to limited compliance requirements ie, data fiduciaries and data processors are only required to undertake (currently undefined) reasonable security safeguards to prevent a personal data breach. Limiting their obligations in this way has positive implications for business process

outsourcing services in India. Non-resident data principals are not without a remedy in the event of a personal data breach. When a personal data breach occurs as a result of the resident data processor failing to take reasonable security safeguards, non-resident data principals can lodge complaints with the enforcement authority under the DPDP Bill (ie, the Data Protection Board, which will function more as an enforcement authority than a regulator). Significant non-compliance can attract penalties of up to INR 250 crores (USD 30 million).

Some key concepts: personal data, harm and personal data breach

Personal data

Unlike the GDPR, the DPDP Bill does not categorise data based on sensitivity or consequently subject certain categories of data to special protections. Instead, the DPDP Bill protects personal data, which is defined as "*any data about an individual who is identifiable by or in relation to such data*". This definition likely includes inferred data within its ambit. However, it probably does not include data that is not about an individual but could be combined with other data to create data *"about an individual who is indentifiable by or in relation to such data*". This is in contrast to the broader GDPR approach, which considers information to be personal data as long as it relates to an identified or identifiable natural person whether directly or indirectly.

Harm

Harm, which plays a pivotal role in determining whether a data fiduciary's processing activities are risky enough for it to qualify as a significant data fiduciary (and therefore, subject to additional obligations), is defined very narrowly. It includes a closed group of events (ie, actual bodily harm, distortion or theft of identity, harassment, or the prevention of lawful gain or causation of significant loss), which discounts other types of harms, like discriminatory treatment, denial or withdrawal of service, and psychological harms.

Personal data breaches

These are defined widely under the DPDP Bill as any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data that compromises the confidentiality, integrity or availability of personal data. This means that even unintended excessive processing that compromises the confidentiality of personal data would likely constitute a personal data breach, triggering reporting duties that (under the DPDP Bill) kick in immediately. Failing to comply could trigger penalties of INR 200 crores (USD 25 million) for not reporting personal data breaches, as well as other penalties for non-compliance with the DPDP Bill (eg, a general penalty of up to INR 50 crores (USD 6 million)).

Simplifying notice procedures and liberalising consent

The DPDP Bill dispenses with laborious notice and consent procedures, opting for more practical compliance structures.

Notice

Under the DPDP Bill, data fiduciaries are simply required to provide data principals with a notice stating:

1. what personal data is collected

2. the purposes for which such personal data will be processed, and

3. the contact details for the fiduciary's data protection officer or person responsible for responding to data principals' requests to exercise their rights under the DPDP Bill.

The notice must be clear, in plain language, and give data principals the option to access it in English, or one of the 22 Indic languages in the Eighth Schedule to the Constitution of India. Such notice obligations also apply to past processing. It is unclear how such notices will be delivered where personal data is not being collected directly from data principals (eg, where a person provides another person's name and address while placing an order to have groceries delivered to them).

Express consent

Consent to processing of personal data under the DPDP Bill can either be expressly provided or deemed as having been given. Unlike the GDPR, which requires express consent to be with regard to one or more specific purposes, the DPDP Bill understands consent in the context of a specified purpose, ie, as 'mentioned in the [corresponding] notice' presented to data principals. This enables informed data principals to consent to any and all kinds of processing of their personal data, provided they were notified of the same. Data principals have the right to withdraw their consent, which once withdrawn acts as a bar to continued processing: data fiduciaries must cease processing the associated personal data or remove the means by which it can be associated with a data principal within a reasonable time. The DPDP Bill also expressly bars data fiduciaries from making the continued provision of their services conditional upon consent to additional processing that is not necessary for a purpose.

Deemed consent

Non-express consent takes the centre stage under the DPDP Bill and is no longer simply a narrow exception to the rule. A bundle of circumstances - where the data principal is deemed to have provided consent - collectively constitute the 'deemed consent' bases for processing personal data. Some grounds (eg, for compliance with a judgment or order, medical emergencies, and employment-related purposes) are globally understood non-consensual grounds of processing (eg, under the GDPR). However, the manner in which certain grounds are framed, is particular to the DPDP Bill: ie,

- where the data principal voluntarily provides their personal data and is reasonably expected to provide their personal data (Ground 1), and

- where processing may be required in public interest (Ground 2).

In the case of Ground 1, data fiduciaries must demonstrate that the data principal voluntarily provided certain data that was reasonably expected to have been provided in this context. This is an easy standard to meet where the processing activity is obvious and inevitable (eg processing a phone number to enable a mobile phone top-up).

Ground 2 also has limited applicability, particularly for private entities. Although any processing in the public interest presumes consent of the data principal, (public interest only includes situations like the security of state and maintenance of public order; and also requires one of the other qualifying elements to be satisfied (eg, processing in the context of mergers and acquisitions, prevention and detection of fraud, credit scoring, and debt recovery).

Processing children's data

The data of a child (a person below the age of eighteen, unlike other data protection regimes that contemplate a lower digital age of consent, eg, under the GDPR) cannot be processed without verifiable parental consent (VPC). The DPDP Bill is silent on what will count as VPC, but it is possible that India will, as is the case under the USA's Children's Online Privacy Protection Act, 1998 (COPPA), adopt a non-exhaustive list of VPC mechanisms (eg, physically signing and posting/faxing a consent form; using a credit/debit card that notifies the account-holder of the transaction). However, it is likely that India's list will not be as prescriptive as COPPA's. This approach aligns with the GDPR stance, which does not prescribe a list of approved methods but points to methods endorsed in other jurisdictions (eg, by the Federal Trade Commission under COPPA) as a blueprint. Practically speaking, data fiduciaries must also account for age verification - a necessary step in determining whether a data principal is a child, and, accordingly, if verifiable parental consent is necessary.

Processing of children's data is also further limited by an express bar on tracking or behaviourally monitoring children and targeting advertisements at them. However, the Government can exempt certain processing activities from adhering to these restrictions in addition to complying with the VPC requirement. This and the manner of VPC will, however, be determined by delegated legislation.

Cross-border transfers

Cross-border transfers of all personal data are permitted under the DPDP Bill subject to:

- the transfer being made to a territory notified by the Government as a permissible one
- unspecified terms and conditions that may be prescribed by the Government.

The Government is expected to adopt a 'blacklist' approach, which will presumably identify unfriendly jurisdictions to which data transfers will not be permitted. This appears to be a comparatively simpler regime than those present in other jurisdictions (eg, being subject to adequacy decisions under the GDPR, or adherence to standard contractual clauses). However, the wild card here may well be the currently unspecified terms and conditions that may be prescribed by the Government.

Enforcement and penalties

The DPDP Bill opts for the carrot over the stick when it comes to enforcement, by electing to impose relatively lower penalties (ranging between USD 6 million and USD 30 million) for non-compliance, and capping such penalties at USD 60 million per instance. This is in stark contrast to other regimes (as well as prior iterations of the draft law), which adopt heftier penalty regimes that are described as a percentage of the non-compliant entity's turnover (eg, up to 2% or up to 4% of the worldwide annual turnover for the preceding year under the GDPR). Penalties are also only likely to be imposed in the case of significant non-compliance, and range from an INR 250 crore penalty (USD 30 million) for not implementing reasonable security measures to protect personal data against a data breach, to an INR 200 crore penalty (USD 25 million) for not reporting a personal data breach. Miscellaneous non-compliance is subject to a penalty of up to INR 50 Crore (USD 6 million). Such penalties can, however, be avoided if the non-compliant entity submits a 'voluntary undertaking' to comply in a certain manner.

Moving to a new approach

Although the final forms of the DIA and the DPDP Bill are yet to be made public, it is clear that the future technology law regime will be distinctly different from the present one. Much of the uncertainty, however, stems from the fact that the DIA proposes a rules-based approach like the DPDP Bill, which also leaves the specifics to delegated legislation. Both have a tough road ahead of them as they are intended to bridge the gap between a dated data and technology law framework and the complexities that accompany newer, emerging technologies. The extent to which they will achieve this goal remains to be seen.

Nikhil Narendran is a Partner and a part of the TMT practice at Trilegal, India's top-ranked full-service law firm. Karishma Sundara is a Counsel at Trilegal.

Views expressed are personal. This article was originally published on Taylor Wessing's Global Data Hub.