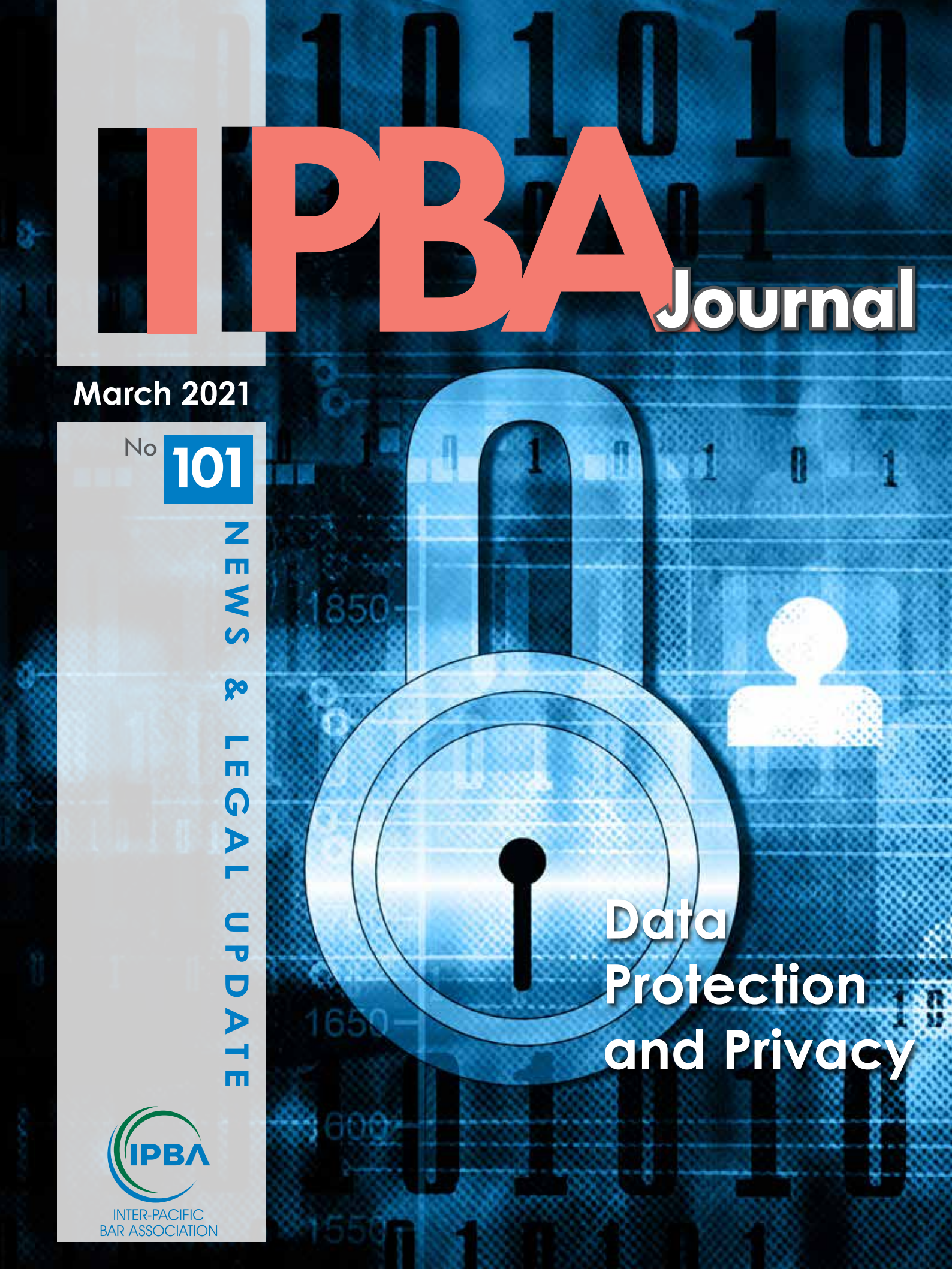
IPBA Journal

March 2021

No 101

NEWS & LEGAL UPDATE



Data Protection and Privacy

IPBA
INTER-PACIFIC BAR ASSOCIATION

IPBA
Legal
Update

Cross-Border Data Transfer in India: One Step Forward and Two Steps Back?

Informational privacy is recognised as a fundamental right in India, and a new data protection law is underway. The Personal Data Protection Bill, 2019 seeks to regulate cross-border data transfer through data export restrictions and localisation norms. The article compares the existing legal regime with the proposed law, delves into the rationale for data flow restrictions outside India, and analyses its potential impact for organisations.

Introduction

Governments regulate cross-border data flow through data export restrictions, and in some cases, impose data localisation measures that mandate some or all aspects of processing to be carried out within its territorial limits.[1] Currently, Indian data protection rules are far from adequate and permit free flow of data across borders. However, a robust data protection legislation is in the pipeline. The proposed Personal Data Protection Bill, 2019 ('PDP Bill') contemplates a mix of data export restrictions and localisation for certain data sets. This article aims to explain the insufficiency of the existing data processing regime, provide an overview of the PDP Bill and specifically analyse the proposed cross-border restrictions to understand its potential impact.

Existing law—The Information Technology Act and Rules

Personal data processing is regulated under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('IT Rules'),[2] notified under the Information Technology Act, 2000 . They primarily apply to Indian body corporates engaged in processing personal information ('PI') of a natural person located in India. PI is defined as information relating to a natural person, which directly or indirectly, either standalone or in combination with other information, is capable of identifying the natural person. Certain categories of PI such as passwords, financial information, physical, physiological or mental health data, sexual orientation and biometric information are classified as sensitive personal data ('SPD'). The IT Rules contain only eight provisions, do not provide detailed data protection regulations and are mostly aimed at regulating the processing of SPD.

Rule 7 of the IT Rules deals with cross-border data transfer. It states that SPD can be transferred to a third party outside India, provided: (1) the foreign recipient ensures the same level of data protection as is provided under the IT Rules which, as observed earlier, is minimal; and (2) the transfer is undertaken either on the basis of an individual's consent or for a lawful contract executed with the individual. Consequently, organisations, while seeking consent or executing e-contracts for goods and/or services, add suitable terms that permit seamless and unbridled cross-border data transfer. In essence, the IT Rules enable free flow of personal data across borders without stringent data export restrictions.

Puttaswamy Judgment—Genesis of the PDP Bill

In the Indian Supreme Court's ('SC') landmark decision of Justice KS Puttaswamy (Retd) v Union of India[3] ('Puttaswamy'), right to privacy was conclusively recognised as a fundamental right. In Puttaswamy, the constitutional validity of the AADHAAR (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ('AADHAAR Act') was questioned. The said law rolled out a system of unique citizen identification numbers for efficient delivery of government benefits and subsidies. The unique number, also called the AADHAAR number, is linked and authenticated with an individual's biometric identifiers that are stored on a central data repository controlled by a special regulator, the UIDAI. The petitioners contended that the AADHAAR Act was invasive of an individual's right to privacy as it compelled individuals to provide their biometric information for availing legal entitlements, thereby negating free consent. It was also argued that the biometric data

can be misused by third parties seeking to authenticate the AADHAAR number as well as by the state to profile citizens, track their movements and surveil them. The Government, defending the *vires* of the legislation, argued that privacy was not a fundamental right and as such there were sufficient technical measures that would maintain authenticity and confidentiality of processed personal data.

The SC ruled that privacy was a key facet of an individual's right to life and personal liberty under Article 21 of the Constitution and can only be suspended by following substantive and procedural due process of law, that is, there must be a law, the action must serve a legitimate state aim and the invasive measures must be proportionate to the goal sought to be achieved. Further, the SC expressly recognised informational privacy as inherent to individual's right to privacy. Furthermore, the SC urged the government to create a detailed data protection regime in India that marries an individual's privacy interests and legitimate state concerns such as protecting national security, preventing and investigating crimes, encouraging innovation and dissipation of social benefits. On the second question regarding constitutionality of the AADHAAR Act, the SC undertook a detailed evaluation of the privacy and data protection safeguards provided therein and upheld its constitutionality, barring few provisions which were held unconstitutional.

PDP Bill—An Overview

In the wake of Puttaswamy, the Indian Government constituted a Committee of experts to propose a structured data protection law.[4] The Committee submitted a draft law to the Ministry of Electronics and Information Technology on 27 July 2018 and a revised PDP Bill was referred to a Joint Parliamentary Committee on 11 December 2019 for further deliberations. The Committee is at the final stages of its deliberations and it is anticipated that a final PDP Bill will be tabled before Parliament soon.

Overview and Key Concepts

The PDP Bill is structured as a sector agnostic law regulating the processing of personal data ('PD') and, *inter alia*, provides for core data processing principles, the permissible processing basis, individual rights, technical and organisational measures, special obligations for certain kinds of processing, cross-border data transfer mechanisms and penalties for breach. It contemplates establishing an independent regulator, the Data Protection Authority of India ('DPA') that will be vested with significant powers for regulating the data ecosystem. The PDP Bill will apply to government and private entities/persons. It will also apply extraterritorially to foreign entities or persons who are engaged in any business or systematic activity of offering goods or services to persons within India, or profile them. Some of the key concepts and requirements under the PDP Bill are captured below to understand the extent of change that the PDP Bill proposes:

1. 'Processing' is defined widely to include any and all operations performed on PD such as collection, recording, organisation, structuring, storage, alteration, retrieval, disclosure, erasure and destruction of PD. Processing must be as per the core data protection principles of purpose limitation, data minimisation, storage limitation, data accuracy, accountability and transparency.

2. PD is also provided a wide scope and will mean any data about or relating to a natural person who is directly or indirectly identifiable, whether online or offline, either standalone or in combination with other information and shall include any inference drawn from such data for the purpose of profiling. An expansive definition is essential for the law to evolve organically and cater to future technological advancements.

3. Certain categories of PD that may reveal, be related to or constitute financial data, health data, an official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation will be treated as SPD. Apart from the listed SPD, Clause 15 empowers the Central Government ('CG') to notify additional categories of SPD after consultation with the DPA and concerned sectoral regulators. The definition is wide and there is a possibility that most kinds of PD qualify as SPD. For instance, one's last name in India generally relates to a person's caste and thus, a name may also qualify as SPD.

4. The PDP Bill introduces the concept of a fiduciary or trust-based relationship between the entities processing PD and the individual. Accordingly, processing under the PDP Bill involves three

stakeholders, namely (a) the data principal as the concerned natural person whose PD is being processed (akin to a data subject); (b) the data fiduciary as the state entity or the natural or legal person that determines the purposes and means of processing (similar to a controller); and (c) the data processor as the one that processes the PD for the fiduciary strictly in accordance with the instructions of and authorisation from the fiduciary. The underlying theme is that the fiduciary is best suited to determine the impact of processing and owes a responsibility to ensure the principal's privacy.

5. Consent is the primary legal basis for processing and must be free, informed, specific, clear and capable of being withdrawn. This essentially requires the fiduciary to provide detailed information about the scope and purposes of processing, manner of processing, the stakeholders involved in the data processing cycle and available remedies and rights. Apart from consent, the PDP Bill also contemplates processing on other grounds such as performance of any state function, compliance with the law, responding to any medical emergency, a breakdown of public order, a threat to public health and for reasonable purposes as may be notified subsequently by the CG. A detailed consent mechanism is a significant improvement over the IT Rules, but critics have raised concerns about absence of other grounds for processing (such as legitimate interest, reasonable repurposing and lawful contract) and overreliance on consent that is well known to result in consent fatigue.

6. Elaborate data principal rights are provided for under the PDP Bill, including the right to confirmation and access for processed PD, correction and erasure, portability and the right to be forgotten. This is an important change as the IT Rules barely provided for individual data protection rights.

7. To bolster transparency and accountability, the PDP Bill mandates a data fiduciary to prepare a privacy by design policy, provide necessary information on processing activities, implement necessary security safeguards (such as de-identification and encryption) and report any data breach to the DPA. Additionally, based on factors such as the volume of PD processed, sensitivity of PD, turnover, risk of harm to the data principal and other factors, certain data fiduciaries can be classified as significant data fiduciaries. These fiduciaries will have to comply with

specific obligations around data audit, appointment of a data protection officer, conducting data protection impact assessments and maintaining processing records.

8. For breach of the PDP Bill, the DPA is vested with wide inquiry and directive powers. It also proposes significant penalties that could range from between two to four per cent of an organisation's global turnover[5] and entitles the principal to seek compensation for harm suffered. Thus, upon implementation of the PDP Bill, organisations have to transition from a self-regulatory approach that exists under the IT Rules to a 'comply or face the consequences' approach.

Cross-border Transfer Under the PDP Bill

The PDP Bill at Chapter VII elaborates on cross-border data transfer mechanisms and mandates data localisation for certain kinds of data. Clause 33 permits the transfer of PD freely, as long as PD is not SPD or critical PD as may be notified by the CG. The PDP Bill does not provide any guidance on what will constitute critical PD, but it is speculated that this may include data that has a bearing on Indian sovereignty, state security, defence and the economy. Where it is SPD or critical PD, fiduciaries must take into account the data localisation principles and transfer mechanisms as explained below:

The PDP Bill at Chapter VII elaborates on cross-border data transfer mechanisms and mandates data localisation for certain kinds of data.

1. SPD can be transferred provided it is continually stored in India, that is, partially localised. Further, transfer can only take place with the principal's explicit consent and the DPA's approval, unless it complies with any one of the following data export restrictions. The first condition requires the transfer to be made pursuant to a contract or intra-group scheme approved by the DPA. For approval, the contract or intra-group scheme must include provisions for effective protection of the data principal's rights and liability of the fiduciary for harm caused due to non-compliance of the contract or scheme. The second condition mandates that transfer is undertaken to a country, entity or class of entity in a country or an international organisation on the basis of an adequacy decision of the CG in consultation with the DPA. An adequacy finding shall take into account the level of protection that is afforded to the transferred SPD having regard to the applicable laws and international agreements of the recipient and whether such transfer will prejudice enforcement of relevant Indian laws.

2. Critical PD can only be processed in India and cannot be transferred outside. The limited exceptions to this absolute localisation are where critical PD needs to be transferred for prompt action during health or emergency services or to a foreign recipient whom the CG has confirmed through an adequacy decision, provided that the transfer in the opinion of the CG is not prejudicially affecting security and the strategic interest of the state. If any critical PD is transferred, such transfer must be notified to the DPA within such timeline as may be prescribed.

Where the fiduciary fails to comply with cross-border data transfer regulations, the fiduciary could be penalised up to INR150 million or four per cent of the total worldwide turnover in the preceding fiscal (that is, 1 April to 31 March), whichever is higher. However, prior to imposing penalties, adjudicating officers shall provide a reasonable opportunity of hearing and the orders passed can be preferred in appeal to the appellate tribunal as may be notified.

To summarise, SPD can be processed abroad subject to partial localisation, explicit consent of the principal and either with the regulator's approval or subject to compliance with data export restrictions in the nature of a contract, intra-group scheme or adequacy decision. Critical PD is subject to absolute localisation and cannot be transferred abroad, except at the discretion of the CG. In light of these conditions, organisations have to plan, strategize and invest substantial resources for physically processing data only in India and implementing adequate data protection measures. Since there are no precedents in the context of cross-border data transfer under the IT Rules, there is ambiguity around implementation. Consequently, it is expected that the government, DPA as well as courts are likely to refer to other jurisdictions and foreign jurisprudence to interpret and enforce the requirements.

Cross-border Data Transfer Under the EU GDPR

In order to understand the impact of the PDP Bill's data localisation and export restrictions, it is helpful to take a quick look at cross-border data transfer regulations under the European Union General Data Protection Regulations ('EU GDPR'). The general principle is that PD can be transferred outside the EU only if the recipient complies with all of the applicable EU GDPR provisions, so that the data subject's interests are safeguarded. Alongside this, the controller or processor must comply with the data export restrictions as explained below:

1. PD is transferred outside based on an adequacy decision from the European Commission ('EC') or concerned supervisory authority. An adequacy decision will, *inter alia*, evaluate the recipient's state of law including its legislation and judicial redressal mechanisms, the existence and effective functioning of an independent data protection regulator and the recipient's international commitments/stance regarding personal data protection. As of date, the EC has recognised 12 jurisdictions as being adequate.[6]

2. In absence of an adequacy decision, the controller or processor can transfer only if they have provided adequate safeguards. Adequate safeguards can be provided through a legally binding and enforceable instrument between public authorities, binding corporate rules (similar to intra-group schemes under the PDP Bill), standard data protection clauses adopted or approved by the EC, approved codes of conduct or certification mechanisms. In all of these options, it is fundamental that there are binding commitments on the recipient to apply appropriate data processing safeguards, including enforcing data subject rights under the EU GDPR.[7]

3. Where (1) or (2) are not fulfilled, the EU GDPR provides for other grounds of transfer. These include transfer with the data subject's explicit consent, performance of a contract or implementation of pre-contractual measures, public interest, legal claims or for protecting the vital interests of the data subject where the data subject is incapable of giving consent.

4. Additionally, cross-border data transfer is permissible if the transfer is not repetitive, concerns only a few data subjects, is necessary for compelling the legitimate interests of the controller that are not overridden by the data subject's rights and the controller has fully evaluated and provided suitable safeguards for protection of the transferred data.

In essence, there are no data localisation norms, although getting an adequacy finding or implementing approved adequate safeguards is an uphill task. A case in point is the decision of the European Court of Justice in the Schrems II case,[8] where it was ruled that the EU-U. S. Privacy Shield failed to provide adequate safeguards for EU data and invalidated it with immediate effect. This testifies to the high threshold that must be fulfilled for continuous adequacy determination. Despite a lapse of 18 months from the EU GDPR implementation, the EC has to still approve codes of conduct or certification mechanisms. Further, approval of binding corporate rules is a long-drawn process and can take several years. In such a scenario, organisations have relied on approved standard contract clauses and the data subject's consent as viable alternatives for data export.

Analysis of the PDP Bill Restrictions and Potential Impact

The PDP Bill's localisation and data export restrictions seem to be motivated by three main ideologies.

1. It is argued that localisation will prevent misuse of valuable and sensitive data in a foreign territory such as foreign government surveillance, unauthorised profiling and unlawful data trade. Foreign surveillance has been a big concern for India due to its geo-political relationships with neighbouring countries. The Indian Government's recent move to permanently ban 59 Chinese apps citing use of data for activities prejudicial to the sovereignty and integrity of India evidences the regulatory mindset towards foreign surveillance, which finds its reflection in the proposed localisation norms.

2. The Government believes that localisation will facilitate the exercise of territorial jurisdiction, which will in turn obligate foreign fiduciaries and processors to provide access to data when required, such as for prevention of crime, investigating breach scenarios and enforcing remedies in India. As early as 2008, the Indian Government in connection with the infamous 2008 Mumbai terror attacks (known as 26/11) engaged in a protracted struggle with

While cross-border data regulation is a necessary evil, localisation measures are archaic and opposed to the idea of data agility.

Blackberry. As the perpetrators used Blackberry devices for planning the attacks, the Government compelled Blackberry to locate its servers in India, so that law enforcement agencies could access encrypted data. Thus, data localisation appears to be an obvious choice for the regulator for law enforcement.

3. It is also presented that localisation will facilitate India's trillion-dollar digital economy. The Government believes that the current data-driven economy has a first-mover's advantage and if India is to emerge as a technology leader, data harnessing and harvesting are key, which calls for ramping up local data infrastructure. With mandatory data localisation, the Government hopes to increase foreign direct investment in digital infrastructure including more data centres, communication satellites and network connectivity, which will result in more employment and benefit the economy.

In light of the above justifications, it appears that the PDP Bill's data transfer restrictions are aimed at asserting data sovereignty and it is not solely aimed at protecting a principal's privacy. A by-product of data flow regulation is that it tends to distort trade by creating entry barriers for businesses and new technologies, segregates the Internet on geographical lines, weakens network security management and increases the cost of doing business. The PDP Bill's localisation and data export restrictions in its current form can be counter-productive for the following reasons:

1. There will be a direct cost impact. Since the scope of SPD is wide and can directly or indirectly cover large volumes of PD, the outcome may be that businesses end up storing all data in India. This will have a bearing on data management methods for organisations processing and storing huge volumes of data outside India. Migrating data from an existing location outside India to servers in India is likely to entail substantial costs. Combined with this, the uncertainty around what will qualify as critical PD will constantly require businesses to undertake data inventories on an ongoing basis in order to remain compliant, which again is likely to become a significant cost head.

2. Mandatory localisation can adversely affect privacy management measures. In order to localise, organisations may have to allocate budgets which could be otherwise used for ramping up their network security resources. This will not only result in lesser economies of scale, but also create additional threats for security failure. For instance,

it is a common practice for group entities to leverage intra-group network assets as part of a robust risk mitigation strategy. Where a data breach occurs, affected data is often transferred to a group entity's server irrespective of the physical location to minimise the potential harm. But, with localisation, cross-border data transfer as part of privacy protection measures is out of context and organisations will have to think about other alternatives.

3. There is also increased scepticism that localisation combined with the CG's wide powers under the PDP Bill can be a segue to increased state surveillance jeopaardising privacy. This is in clear derogation of Puttaswamy which requires balancing of an individual's privacy interests and legitimate state concerns. Further, if scepticism becomes a reality, it will be difficult for organisations to import data into India from jurisdictions such as the EU, United Kingdom and Switzerland, as an adequacy finding would be impossible on the grounds of heightened surveillance, lack of rule or law, and insufficient data protection and privacy measures.

4. The PDP Bill provides for very limited circumstances in which cross-border data transfer can be carried out. Unlike the EU GDPR, which provides for additional grounds such as approved codes of conduct, certification mechanisms, performance of a contract, implementation of pre-contractual measures, public interest, initiating and defending legal claims and protection of the data subject's interests, the PDP Bill heavily relies on an adequacy decision, intra-group schemes and standard contracts. From lessons learned under the EU GDPR, it will take quite some time for India to formulate details. Until such time, there will be business uncertainty and it is imperative to permit additional grounds for cross-border transfer to ensure business continuity.

Conclusion

While cross-border data regulation is a necessary evil, localisation measures are archaic and opposed to the idea of data agility. Instead, the government should focus on strengthening mutual legal assistance treaty mechanisms with other nations to meaningfully implement the PDP Bill in a global set-up. To this effect, the EU GDPR positively obligates the EC and supervisory authorities to take steps for developing international cooperation mechanisms and provide mutual international assistance for enforcement. There is no such provision under the PDP Bill and perhaps a similar provision is a better substitute to a physical localisation mandate. When the final text of the PDP Bill is tabled, it will be interesting to see if India manages to take a step forward for a truly progressive data protection law or retracts two steps to implement regressive localisation norms.

Notes

[1] Countries like Russia, Indonesia, Vietnam, Kazakhstan and China have localisation requirements and some others like Australia and South Korea have selective localisation requirements for certain kinds of data.
[2] There are specific processing requirements under sectoral laws which have not been analysed in this article.
[3] 2017 (10) S.C.A.L.E 1.
[4] The committee of experts was chaired by former Judge of the Supreme Court, Hon'ble Shri Justice BN Srikrishna.
[5] 'Worldwide turnover' is defined as gross revenue from the sale, supply or distribution of goods and/or services within and outside India. In the context of group entities, the revenue of a fiduciary will be added to the group entity(ies) revenue if it is connected with processing in India.
[6] These include Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay as providing adequate protection and talks are ongoing with South Korea; for details access https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last accessed on 25 January 2021).
[7] In these situations, there is no need to obtain prior permission from the concerned supervisory authority. Adequate safeguards can also be subjected to consent from the supervisory authority under the consistency mechanism, which are not captured in this article.
[8] European Court of Justice (Grand Chamber) ruling in case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, dated 16 July 2020.

Arya Tripathy
Partner, Priti Suri & Associates (PSA), India

Arya Tripathy is a Partner of Priti Suri & Associates (PSA), India. She practises in the areas of General Corporate, M&A, Employment and Data Protection laws and has closely worked with various domestic and international clients on diverse aspects of business law. She leads the firm's pro-bono practice and takes a keen interest in working alongside policy think tanks in the niche technology and privacy law space.