PAKISTAN'S DATA PRIVACY BILL: DPA WILL HAVE POWERS, BUT LACK INDEPENDENCE

GRAHAM GREENLEAF

(2020) (165) Privacy Laws & Business International Report, 20-23
[2021] *UNSWLRS* 6

UNSW Law
UNSW Sydney NSW 2052 Australia

Pakistan's data privacy Bill: DPA will have powers, but lack independence

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

(2020) 165 *Privacy Laws & Business International Report* 20-23

Pakistan is the world's fifth most populous country, with a population exceeding 210 million, and a rapidly expanding middle class. It is the most economically significant Asian country not to have a data privacy law. As a South Asian country and member State of SAARC (South Asian Area of Regional Cooperation), it is part of a sub-region which is in the midst of developing modern, GDPR-influenced data privacy laws, as can be seen the current Bills before the legislatures of India[1] and of Sri Lanka.[2] Pakistan has few privacy protections at present.[3]

Pakistan's Ministry of Information Technology and Telecommunications (MOITT) released a new *Personal Data Protection Bill 2020* (PDPB)[4] on 9 April 2020, the latest in a series of draft Bills on which consultations have been held since 2017. It called for submissions on the draft Bill, by 30 May 2020, stating that privacy of personal data was more relevant than ever in the current pandemic.'[5] Pakistan pledged to enact data protection and privacy legislation as a part of Open Government Partnership commitments in 2017.[6] Pakistan's Ministry of Commerce published a revised version of the country's e-commerce policy[7] as recently as 13 November 2019, referring to a data protection law which would provide for data sovereignty and data localization and address issues relating to e-Commerce, including requiring all e-commerce platforms to make full disclosures regarding data protection provisions on their websites and apps. It appears that there may be some competition between Ministries for influence over the final shape of the legislation.

This article considers the main features of the MOITT's Bill, and in particular the extent to which it is influenced by the EU's GDPR.

Scope

The Bill is largely comprehensive, but with capacity for more exceptions to be created. The definitions of key terms (cl. 2) contain few surprises: 'personal data', 'data controller', and 'consent' are given broad definitions.

---

[1] G. Greenleaf 'India's data privacy Bill: Progressive principles, uncertain enforceability' [SSRN copy] (2020) 163 *Privacy Laws & Business International Report* 1, 6-9.

[2] G. Greenleaf 'Advances in South Asian DP laws: Sri Lanka, Pakistan and Nepal'[SSRN copy] (2019) 162 *Privacy Laws & Business International Report* 22-25.

[3] See G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 451-6 'Pakistan'.

[4] Personal Data Protection Bill 2020 (Pakistan)

[5] MOITT Press Release 'Draft Personal Data Protection Bill', undated.

[6] Hija Kamran 'Ministry of IT opens new draft legislation on data protection for public consultation' Digital Rights Monitor, 14 April 2020.

[7] *e*-Commerce Policy of Pakistan, October 2019

Comprehensiveness

The Bill extends to 'the whole of Pakistan' (cl. 1.2), both private sector and federal public sector (the definition of 'data controller' says 'or the government'). The public sectors of the four provinces and two territories are generally not covered.[8] The law will come into force one year after promulgation, unless extended by Gazette notice up to two years (cl. 1.3).

Processing for 'personal, family or household affairs' is exempt from the whole Bill (cl. 30.1), but other exemptions (cl. 30.2) are only from specified sections (generally, need for legitimate grounds for processing, notice requirements, disclosure limits, and some security obligations), and are fairly standard (if sometimes regrettable) exemptions. However, the government, on the advice of the Personal Data Protection Authority of Pakistan (PDPAP), may exempt other classes of controllers from specific obligations (cl. 31). Digital rights groups are very apprehensive of the exemption power.[9] The Bill's provisions take effect despite anything to the contrary in other laws (cl. 49), but this does not affect future inconsistent laws. The scope of the Bill is therefore quite comprehensive at present, but with capacity for exemptions to appear in future.

Extra-territoriality

The extra-territorial application of the Bill is as follows:

(i) If 'any of the data subject, controller or processor (either local or foreign) is located in Pakistan', the data controller and process (the person who 'processes; or has control over or authorizes the processing') must comply with the law (cl. 3.1).

(ii) A person is 'established' (or located) in Pakistan if physically present there for at least 180 days per calendar year; incorporated there; is a partnership or unincorporated association formed under Pakistan's written laws; or maintains in Pakistan an office, branch or agency, or 'a regular practice' (cl. 3.3).

A data controller or processor falling within (i) but not within (ii) must nominate 'a representative in Pakistan' (cl. 3.2), presumably to at least allow service of process, but it is not specified if there are consequence beyond that.[10]

This adds up to significant extra-territorial application, but is different from the EU GDPR test of 'marketing to or monitoring of'. If a data subject is located in Pakistan they will (in theory) be able to proceed under this law against any overseas processing of their data. Many types of 'connections with Pakistan' of controllers or processor will also mean compliance is necessary.

Data on foreigners

An unusual provision limits the applicability of the law to data about non-Pakistanis: 'Foreign data subject shall have all his rights, if any provided under the laws of the country or territory where the foreign data has been collected or data subject resides in so far as consistent with this Act' (cl. 26). For example, if medical records of a US citizen are sent to Pakistan for transcription, or a Karachi-based call centre collects data from US residents, then those parts of Pakistan's law which are also found in the relevant US laws (federal or state) will apply, but

---

[8] There are some exceptions for subjects that are 'federally-managed'. There are also proposals to repeal article 18 of the Constitution, which would return some subjects like education and health to federal control, and within the scope of this law.

[9] Ramsha Jahangir 'Govt seeks consultation on data protection bill' *Dawn* April 11, 2020.

[10] This may be related to other proposals in Pakistan concerning 'online harms', which would expose social media companies to substantial penalties.

if US law is minimal (as will often be the case), then the Pakistani law will give no protection. In contrast, in equivalent situations concerning a resident of a country in the EU, the whole of Pakistan's law will apply because the GDPR provides wider protections. This is a convenient result for Pakistan-based companies doing outsourced processing, because it may satisfy both US and EU customers. However, if a Pakistani processor is taking in content collected from data subjects in many countries, how will they know what are the 'rights, if any provided under the laws of the [foreign] country' or countries? Compliance is unlikely.

Content: EU influences, in part

The content of the rights and obligations in the Bill show many EU influences, though closer to the standards of the 1995 Directive than the stronger GDPR provisions. Chinese influence is also present in data localisation provisions.

Legitimate grounds for processing

Processing of personal data can only be done in compliance with the Bill (cl. 4), and shall not take place without the consent of the data subject (cl. 5.1). However, seven legitimate grounds for processing without consent are provided (cl. 5.2), including 'for legitimate interests pursued by the data controller' (but without any requirement to balance this against other essential interests). Personal data must not be processed except 'for a lawful purpose directly related to an activity of the data controller' and it is 'necessary for or directly related to that purpose' and 'adequate but not excessive' (cl. 3.3). This applies to both primary and secondary processing.

Notice must be given to the data subject (in the national and English languages) specifying such matters as the legal basis and purpose of the processing, its proposed duration, source of the data, data subject rights, proposed disclosures, options to limit processing, compulsion and consequences (cl. 6.1)

Rights of data subjects, and corresponding obligations

The Bill's rights and obligations are extensive, but only require brief mention:

- *Security standards* are to be prescribed by the PDPAP, but also to be implemented by 'practical steps' proportional to risk (cl 8.1, 8.2).
- *Processors* are independently liable to implement security standards, and controllers are liable to ensure that they do (cl 8.3, 8.4).
- *Deletion* of data is required, no longer than it is necessary for fulfilment of purpose (cl. 9).
- *Data integrity* requires 'reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date' relative to purposes (cl 10.1).
- *Rights of access and correction* are required for data subjects (cl. 10.2), and records must be maintained (cl. 11).
- *Data breach notification* must be given to PDPAP (cl. 13), but there is no obligation to notify data subjects.
- Data subject's right to *withdraw consent to processing* (cl 23).

- Data subjects' right to require *cessation of processing likely to cause unwarranted substantial damage or distress* (cl. 25).
- Data subject's right to *erasure of data* where (a) no longer necessary for purpose ('right to be forgotten'); (b) consent is withdrawn and there is no other legitimate ground; or (c) processing is unlawful (cl. 27).

Extensive though these are, many obligations and rights found in the GDPR are not present, including objections to automated processing; data portability; privacy by design and default; and demonstrable accountability.

Sensitive data

The definition of 'sensitive personal data' (cl. 2(k)) includes most subjects found in the EU, but not political beliefs or criminal records. It includes 'access control' information and 'financial information'. The categories may be expanded by rules made by the PDPAP with government approval (cl. 48). Processing of sensitive data requires explicit consent in most cases, plus a situation where processing is necessary (cl. 28.1). Local processing may also be required.

Cross-border transfers and data localisations

If personal data is to be transferred outside Pakistan 'it shall be ensured that the country where the data is being transferred offers personal data protection at least equivalent to the protection provided under this Act and the data so transferred shall be processed in accordance with this Act and, where applicable, the consent given by the data subject' (cl 14). Personal data exports may take place 'under a framework (on conditions) to be devised by the Authority' (PDPAP) (cl. 15.1), but it is unclear whether this 'framework' may provide additional methods for data exports, or whether transfers under clause 14 must comply with these conditions, or both. Also unclear is whether the government or the PDPAP decides which countries' laws are 'at least equivalent', but if it uses rules (rather than regulations) to do so, it must have government approval.

Two forms of 'data localisation' are required. First, the DPA must 'devise a mechanism for keeping a copy of personal data in Pakistan' (cl. 15.2): so a local copy must be kept of all data exported. Second, 'Critical personal data shall only be processed in a server or data centre located in Pakistan' (cl. 14.1), so data exports are not normally possible for 'critical' personal data, but the government can make exceptions on 'the grounds of necessity or strategic interests of the State' (cl. 14.2). It is possible that exceptions cannot be made for sensitive data, but unclear due to a drafting error (cl. 14.3). 'Critical personal data' is to be classified by the DPA with approval of the government (cl. 2). Such clauses have been proliferating in Asian laws and Bills since China's *Cybersecurity Law* of 2016, and are found in Vietnam's law, India's Bill and Sri Lanka's Bill.

A criticised DPA, modest enforcement

Civil society criticises the proposed DPA as too powerful and not independent enough.

The government is required to establish a Personal Data Protection Authority of Pakistan (PDPAP). It 'shall enjoy operational and administrative autonomy, except as specifically provided for under this Act' (cl 32.1). However, the government 'may, as and when it considers necessary, issue policy directives to the Authority, not inconsistent with the provisions of the Act … and the Authority shall comply with such directives' (cl. 38.1). Such clauses allowing government instructions to DPAs on policy matters are quite common in Asian jurisdictions (Malaysia, Singapore, Indian Bill, Sri Lankan Bill), but make it very difficult to argue that these

DPAs are 'independent' in the European usage of the term. The PDPAP also requires government approval to cooperate with international organisations, or other DPAs (cl. 39).

The PDPAP will consist of seven members, appointed by the government for a single non-renewable four-year term (cl. 34.2), although the government can increase the number of members (cl. 32.5). Three will be ex-officio appointments of representatives of each of the IT & Telecom, Defence and Interior ministries[11] (which further compromises independence), and four from the IT, financial, legal and civil society sectors (cl. 32.4). The government chooses which one will be Chairman, but the PDPAP will operate by majority vote. These are all full-time salaried positions, with protections against removal from office except for incapacity or misconduct. Civil society has argued that these full-time positions will not be independent, particularly with government being able to give policy instructions.[12]

The functions of the PDPAP are comprehensive, involving complaint investigation, advising government on legislation and law reform, monitoring technological and social developments, and education of the public, controllers etc on the law (cl. 33). It has all powers needed to exercise these functions, including by being deemed to be, and hold the powers of, a Civil Court. It can 'impose penalties for non-observance of data security practices and non-compliance of the provisions of this Act' (cl. 44(j)) and 'order a data controller to take such reasonable measures as it may deem necessary to remedy an applicant for any failure to implement the provisions of this Act' (cl. 44(k)). These powers seem sufficient for civil penalties and compensation payments to be ordered, but this is not specified.

Other functions/powers of the PDPAP specified in the Bill include (cl. 34):

- 'Formulate compliance framework for monitoring and enforcement';
- 'Devise registration mechanism for Data Controllers and Data Processors';
- 'Formulate a Licensing Framework for Data Controllers and Data Processors';
- Identify categories of controllers/processors (for example 'large') 'and define special measures for compliance' (possible allowing simpler procedures for small controllers/processors, as in India).

The PDPAP can issue 'regulations for exercising its powers and performance of its functions' (cl. 47), and (with government approval), 'make rules to carry out the purposes of this Act' (cl. 48), including concerning codes of conduct and accreditation of security audits.

Civil society criticisms

The PDPAP's structure and powers are the most contentious aspect of the Bill. The organisation Media Matters for Democracy, a Pakistan-based not-for-profit working on communications issues, has condemned[13] what it sees as 'draconian and anti-democratic sections' in the draft Bill. Its criticisms include:

---

[11] Clause 32.4 is ambiguous, but the better interpretation (supported by civil society groups) is that all three Ministries will each have ex-officio representatives, not just one of them.

[12] Ramsha Jahangir 'Govt seeks consultation on data protection bill' *Dawn* April 11, 2020

[13] 'Media Matters for Democracy express concerns over the new draft of data protection law; warns it will create a dangerous precedent' 22 April 2020

- PDPAP 'should be independent from the involvement of existing government ministries'.
- 'The government has attempted to consolidate all powers, including the power of (delegated) legislation, investigation and the judiciary'.
- 'Giving the Authority powers to create definitions and rules that go well beyond general rule-making powers'.
- Clause 32.5 'allows the Federal Government to change the composition of the Authority at will'.
- 'Allowing the Authority to define Critical Personal Data'**.**
- **'**A licensing framework for data controllers and data processors … is an attempt to push for localisation of International Corporations'.

Enforcement – Complaints and offences

Any processing of personal data in breach of the Bill is liable to a fine of up to US$96,000, rising to US$160,000 for a repeat offence, or US$128,000 in relation to sensitive data (cl. 41). Failure to adopt necessary security measures can result in a fine up to US$32,000 (cl. 42). There can also be corporate liability for breaches, punished by a fine of US$192,000, or 1% of the company's annual gross revenue in Pakistan, whichever is higher (cl. 44). It is ambiguous whether the PDPAP may be able to both prosecute and 'punish' these matters, described as 'offences' (Chapter VIII is headed 'Complaint and Offences'), despite being classified as a 'Civil Court', or whether these matters must be heard by a court. The Bill needs to clarify whether these are criminal offences or civil penalties, and who is to have jurisdiction over them.

An individual can file a complaint with the PDPAP in relation to, in effect, any breach of the Bill by a data controller or processor (cl. 45.1). The remedies available should be the same as those from a Civil Court, which would include both injunctions and compensation. *Ex parte* orders may be made if necessary (cl. 45.6). Appeals against decisions of the PDPAP are to the High Court unless a separate appeal Tribunal is established (cl. 46.1). There is no right to 'judicial redress' in the sense of proceeding directly before a court.

Conclusions

This Bill has the ingredients to give Pakistan a data privacy law of medium strength (in both principles and enforcement) by international standards. However, these benefits are undermined by a data protection authority lacking some key elements of independence, and a combination of the government and the PDPAP having between them far too much discretionary power, in various forms of delegated legislation, to alter the meaning of the law fundamentally. This makes it uncertain whether the law will genuinely protect privacy and other civil liberties, or whether it will result in more authoritarian control over personal information and its use. Ambiguous drafting adds considerably to the uncertainties.

Information: Sadaf Khan of NGO 'Media Matters for Democracy' (MMfD) and another correspondent have provided valuable information for this article, but responsibility for content remains entirely with the author.