#NAMA: Issues with classification of data in the Personal Data Protection Bill, 2019

The Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019, and was referred to a 30-member Joint Parliamentary Committee for review. The Bill is the first legislation that focusses on privacy of citizens, and could potentially result in significant overhaul of digital businesses and companies. The Committee is expected to submit its report to the Parliament before the Budget Session concludes on April 3, 2020.

Earlier this month, MediaNama held discussions in Delhi and Bangalore on the main aspects and impact of the Bill with a wide set of stakeholders. The discussions were held with support from Facebook, Google, and STAR India in Delhi, and with support from Facebook and Google in Bangalore. The discussions were held under Chatham House Rule, so quotes have not been attributed. Quotes are not verbatim and have been edited for clarity and brevity. Read our full coverage of the discussions here: #NAMA India's Data Protection Law – January 2020.

The following is Part II of our notes from the session on cross border data flows, read Part I here.

Classification of data is complex

What can potentially be sensitive personal data: A lot of Indian names can actually reveal the caste of a person, so wouldn't names also be considered sensitive personal information, a speaker asked, and added that there is currently a lot of confusion on what exactly is personal data, and what is sensitive personal data. Another speaker highlighted the problem by giving the example of photographs collected for non-biometric purposes, for instance, for making an album, will those photographs be then considered personal data, or sensitive personal data?

- **Is there anything such as personal data?** From the definition of sensitive personal data, it appears as if there is no such thing as personal data, a lawyer noted. The person explained that if fiduciaries start processing any kind of data with sufficient depth and clarity, it might give away inferences to people's health information, sexual orientation, mental status etc.
- **Definition of personal data is contextual:** Another lawyer said that the definition of personal data in the current Bill is extremely contextual. "There is no possible way that we can create an exhaustive list of personal data, and there is good reason for it: That same data packet could be personal data in one context and not in another context. So this entire exercise of data segregation itself is extremely difficult," they noted.

What is really the objective behind this data classification exercise, a lawyer

asked. "So, sensitive personal data has to be localised, does that have an objective? Maybe, it is due to the fact that certain data types might need a heightened sense of security. However, to provide that security to localised data, it will have to be encrypted. With the entire section on government exceptions, it appears as if it wants to access some of that data. But, will it be possible when that data is encrypted?" the person said.

What about critical personal data? A person in the audience said that as a small business, they are very anxious over the uncertainty of collecting critical personal data since it hasn't been defined in the Bill. A speaker noted:

> "Critical personal data hasn't been defined in the Bill, and neither does it have a basis for classification. Neither does the Bill doesn't spell out any process by which critical personal data is going to be defined, nor will it involve the Data Protection Authority or the industry in the classification process. I don't know how we are even going to arrive at any business predictability around that."

What falls under financial information? Financial service providers need to collect people's names to provide them with financial services, will those names also be categorised as sensitive personal data, a person asked. "There is a lot of ambiguity in the way sensitive personal data has been classified in the current Bill," they added.

- Another speaker noted that the reason why financial data was classified under sensitive personal data is to comply with the RBI's data localisation mandate. "This classification legitimises the RBI directive and the clarification that came later on, which specifically said financial data has to be stored only in India, can be processed outside the country and deleted in some time and that's exactly how sensitive personal data under this new Bill is treated as well," the person added.

Illustrating the problem with the classification of sensitive personal data, with respect to processing it outside India, a lawyer said:

> "Imagine I email you my bank statement, which by definition is sensitive personal data because it has my financial data. Then in the next email I also send you a cat meme. In which world will a data fiduciary be able to save the financial data part of the email in India and process it outside while the cat meme can go anywhere in the world?" — a lawyer

"Just the semantics of this condition are so new that even the best data protection team in the world would not be able to decode it," the same person said. They also highlighted that only because personal data has been allowed to be processed outside India, doesn't mean that it isn't of much worth to businesses. "A lot of email providers actually process users' emails and attachments in order to target advertisements better. This processing largely happens on the server," the person said.

How payments services will be affected: A lot of people store their credit card information, bank passwords on browsers which have a sync service. This means that if these people use their browser outside India, the stored data just gets synced to that particular browser instance, and is never generally stored on the server, a person explained. However, the classification of sensitive personal data with respect to processing outside India would mean that the same data fiduciary will have to consider those instances differently in different countries, which would essentially break the service, the person explained.

- The first speaker also said that just putting in place the architecture to segregate sensitive personal data from current datasets is going to be an egregious task, more so for industries that are just starting out, since they'll have to invest heavily in establishing this architecture. "This will create a bottleneck in their operations," the person added.

Health data being made part of sensitive personal data can also become a problem, a person said, and explained: "A lot of people come to India from around the world to get treated for certain health conditions, and hospitals here can also serve these people remotely. Similarly, what would happen if Indians travelling to other countries have to visit a hospital there unexpectedly which requires their health data? Will the current localisation norms for health data not affect that?"

- To that, a lawyer responded by saying that health data being part of sensitive personal data should not be looked at from the perspective of data localisation alone. Instead, we should discuss having separate laws that deal with the transfer of certain kinds of data, for instance, the the Health Insurance Portability and Accountability Act (HIPAA) in the US, the person added. They also said that we should not bat to remove certain kinds of data from the bracket of sensitive personal data, just because localising that would be a deterrent.

Read more: Personal Data Protection Bill, 2019: Considering data localisation and its effects on payments

Adequacy vs. data localisation: Which is the better approach?

Adequacy is better: Adequacy under EU's GDPR, is an indirect form of localisation, without any of the categorisation problems in the Personal Data Protection Bill, a speaker said. "It means you can either process data in a particular country, or not process it there at all, which makes compliance much easier," a lawyer said. Even though India doesn't have adequate status with the European Union yet, it is still possible for people in India to access someone's computer in the EU remotely, because technically, the processing is still happening in the EU, the person added. Another speaker noted that adequacy

is a better way of dealing with overseas processing of data, simply because data localisation will be unenforceable.

> "The reason why the EU chose adequacy over data localisation was because they did not want to get into an unsolvable problem." — a lawyer

If the EU says that its citizens' data can go to another country, only then can that data be taken overseas. Also, that data would enjoy the same level of protection as in the EU, and companies will have similar legal liabilities to ensure that that data remains safe and secure, another person added.

- If India were to choose ten countries where it would be fine to process Indians' health and financial data, none of the problems we have discussed thus far will arise. Most data fiduciaries will be happier to follow adequacy procedures than the localisation mandate, they added.
- A speaker pointed out that while adequacy is a much better option than data localisation, it still has its own share of problems, including the fact that it is an extremely bureaucratic exercise.

"When you open the Xiaomi Home app, it actually asks users on which server they want their account to be on. The options that pop up include India, China and the USA. What Xiaomi is doing at this point in time is basically giving users the ability to choose where they want their data to be stored and processed," a lawyer said, explaining what the adequacy procedure would look like.

Will India get adequacy under GDPR?

No. "With the current provisions in the bill, it's impossible to see how we would get adequacy status under GDPR," a lawyer said, and explained: There is a provision in the Data Protection Bill which says that data of non-Indians, when processed in India, might not enjoy the same level of protection that the Bill offers. This can be a potential hindrance in India getting adequacy status with the EU.

- With the kind of surveillance norms we have in India, along with the section of the Data Protection Bill which talks about government exceptions, India will not get adequacy with the EU, another person said. "Getting adequacy is a long process, and it takes a lot of negotiation with the EU to get adequacy. Our Bill won't give us enough power to negotiate with the EU," the person added.
- The section which deals with the restriction on cross border data flow in the PDP Bill, 2019, doesn't make it clear if it also applies to data of foreign nationals. Does that mean that even their sensitive personal data will have to be localised in India? If that were to happen, India will fail all adequacy requirements, a speaker said.

Read Part I of our notes on cross-border data flow here. Read our coverage of the discussions here: #NAMA – India's Data Protection Law – January 2020.