#NAMA: Issues around surveillance 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 I of our notes from the session on government access to data, read Part II here.

"The *Puttaswamy* judgement and the discourse around data protection in India arose in the context of Aadhaar, where the State was seen as the chief privacy violator. The Personal Data Protection Bill was an opportunity to correct that, but the State wants to exempt itself from all the obligations instead," a speaker said.

Sections 35 and Section 36 emerged as the crux of issues of the Bill as they grant government agencies too much power with respect to processing citizens' personal data. Section 35 empowers the central government to exempt any government agency from the provisions of the Act for purposes of pubic order, national security, etc. Under Section 36, certain provisions of the Bill are not applicable for purposes of law enforcement, and court orders.

The State needs to be a model actor given the asymmetry of power between State and citizen: Unlike data that is collected by private companies such as Facebook, it is more concerning when the State does it, a speaker said. **This is because the State has the power of law behind it and a monopoly over violence**. **"The State is the only actor that is sanctioned to commit violence or force of law, in a way private actors cannot**," they explained. As a result, centralisation of power in the State can make citizens vulnerable to extreme harassment, blackmail or coercion, they said.

CHAPTER VIII

EXEMPTIONS

35. Where the Central Government is satisfied that it is necessary or expedient,—

(*i*) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or

(*ii*) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order,

it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency, as may be prescribed.

Explanation.—For the purposes of this section,—

(*i*) the term "cognizable offence" means the offence as defined in clause (*c*) of section 2 of the Code of Criminal Procedure, 1973;

(*ii*) the expression "processing of such personal data" includes sharing by or sharing with such agency of the Government by any data fiduciary, data processor or data principal.

36. The provisions of Chapter II except section 4, Chapters III to V, Chapter VI except section 24, and Chapter VII shall not apply where—

(*a*) personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force;

(*b*) disclosure of personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding;

(*c*) processing of personal data by any court or tribunal in India is necessary for the exercise of any judicial function;

(*d*) personal data is processed by a natural person for any personal or domestic purpose, except where such processing involves disclosure to the public, or is undertaken in connection with any professional or commercial activity; or

(*e*) processing of personal data is necessary for or relevant to a journalistic purpose, by any person and is in compliance with any code of ethics issued by the Press Council of India, or by any media self-regulatory organisation.

Personal Data Protection Bill, 2019 – Section 36

2019 Bill widens government's powers and exemptions

"The 2018 version of the Bill said that processing of personal data by the State for security of the state is exempt from most obligations provided that it is in accordance with law, is necessary, and is proportionate. So the classic proportionality elements, mandated by *Puttaswamy* were introduced. Those in itself were not adequate and the Bill had not gone far enough to address structural and procedural elements, or embed safeguards for this type of access," a panelist explained.

> **Proportionality standard:** The *Puttaswamy* judgement established that the right to privacy can be curtailed only if it passes the four-fold proportionality standard, that is, it gave
>
> 1. Legitimate state aim

2. Legal basis in law
3. Least restrictive means used
4. No disproportionate impact on the right holder

The 2019 Bill, the speaker continued, reduced the already inadequate safeguards on government exemptions even further. This is problematic because:

- **Agency-specific exemption rather than function-specific:** The government can now exempt *entire agencies* from *all* provisions of the Bill, irrespective of whether it is performing the function of security, the speaker said.
- **Increased number of reasons for granting exemption to agencies:** Earlier, the exemption could be granted only for national security reasons, but now four more grounds have been added — sovereignty, integrity, friendly relations, and public order. "While these grounds have a constitutional basis in Article 19(2), this is still a widening of what the 2018 Bill said, something that needs to be examined," they said.
- **Government agencies can be exempted from *all* provisions of the Bill:** "The 2018 Bill was narrowly tailored wherein even State agencies that accessed personal data for security of state had to deploy security measures, process it in a fair and reasonable manner, and be regulated by the DPA," they said. In the 2019 Bill, it means that the exempted agencies would not be regulated by the DPA.

  > "Is the removal of *all* privacy safeguards the least restrictive way, as set forth by the *Puttaswamy* test, to justify the blanket exemption for an agency? Does it justify the wholesale exemption for, say, the Bangalore police to collect *everybody's* data without *any* application of the safeguards in this Bill?" — a speaker in Bangalore

- **Exemption for government from all offences:** Under Section 35, in effect, the government is exempted from the Offences chapter as well, a speaker pointed out, unlike the 2018 Bill. "Even if we find the government guilty of something, there is effectively no statutory remedy," they said.
- **'Reasoned' order is enough to exempt an agency:** The speaker highlighted that now the central government would only need a 'reasoned' order to exempt an agency as opposed to a legal/statutory mandate.
- **Lack of oversight over law enforcement agencies:** Section 36 allows the central government to exempt law enforcement agencies from certain provisions of the Bill for law enforcement purposes, a speaker said. As a result, while oversight by DPA and need for security safeguards remain, two safeguards that were there in the 2018 Bill have been removed, a speaker pointed out.
- **Removal of statutory basis for surveillance by intelligence agencies:** The 2018 Bill explicitly said that for law and order situations, you need a statute or law passed by the Parliament, a panelist said. This would have made it mandatory for the Parliament to actually deliberate on these issues before they exempted an agency. That has been done away

with in the latest draft.

- **Rights of victims, witnesses and suspects have been diluted as proportionality is undermined:** The 2018 Bill allowed law enforcement agencies to process data of a victim or a witness or a person related to a crime or offence that the agency was actively investigating or seeking to prevent, a speaker said. Agencies also had a limitation for how long such records could be kept. Now, it for general prevention and prosecution of offences and contraventions of law, and purpose limitation and limiting retention of data have been scrapped. Proportionality has been removed as a statutory obligation.

One panelist disagreed and said that **the 2019 Bill is an upgrade** as under the 2018 Bill, government agencies could process data without consent for any function of the state. But in the 2019 Bill, this non-consensual processing is limited to providing targeted benefits and certification.

Does the Bill pass muster of the proportionality standards?

***Puttaswamy* standards of necessity and proportionality are not part of a statute:** "Irrespective of that the State or the courts say, a regulator goes by the law. The regulator doesn't go by the precedent set in judgements," a speaker said. As a result, the requirements of necessity and proportionality should be a part of the act itself. This is visible in the case of sedition, a lawyer explained, wherein the police goes by the text of Section 124(A) of the IPC, which is very broad, instead of the Supreme Court judgement that *read down* the section and said that there has to be an incitement to violence.

> **Looking at the Pegasus scooping scandal:** "Installation of malware on somebody's phone for the purposes of surveillance does not have any legal basis. It conforms to no legitimate state aim, and is overly broad. The manner in which surveillance is carried out in India, and its institutional architecture, in my opinion, is completely and manifestly unconstitutional. Steps such as the Central Monitoring System, NATGRID, would not meet the proportionality standard at all." — a speaker

Some definitions are too broad under the bill: A number of terms in Section 35, such as "security of the State" and "public order", are very vague and have not been narrowly defined. "In a statute, you have to be much more precise; you can't have broad value statement like you have in the Constitution," a speaker said. "Public order" is a "term of wide latitude" that has been used for a lot of things, especially to impose Section 144 of the CrPC, remarked another speaker. "When use of administration or discretionary power is tailored so broadly, it inevitably provides a scope for misuse," a speaker said.

- **Delegating powers to private actors for public order?** "When the exemption allows you to take any measure to ensure safety of or provide

assistance or services to any individual during any disaster or any breakdown of public order, apart from the State, it also gives power to a person to determine what is a public order situation and then without consent process your data or seek your data. So, it's a very wide provision," a speaker argued. Letting private individuals determine when they can process personal data without consent when they see a breakdown of public order is a "disaster", another speaker said.

- **Does contravention of law include contractual breach?** Under Section 36, certain agencies of the State can be exempted for contraventions of law. "This is not just criminal offence or cognizable offence. It can even be a contractual breach," a speaker said. This is a really wide power that law enforcement agencies, and State agencies in general, will get.

Standards of proportionality are undermined by security of the State: "In terms of application of the Bill, it means that an agency like the Delhi Police can be exempted from all provisions of the Bill, citing security of the State or public order," a speaker said. They further said that while this could be challenged in court and the government would have to prove that the step is proportionate, it was unlikely to happen. "Anybody who is a long time observer of Indian jurisprudence around national security would say that our courts have been extremely reluctant in seeking accountability or embedding safeguards on or limiting the national security exception," they said.

However, a speaker disagreed with this assessment and said that a nine-judge bench of the Supreme Court held that proportionality standards, which includes the standard of necessity, must be adhered to for any data processing and collection by the State. "**This has been subsequently reaffirmed and recast in different scenarios by the Aadhaar bench, the internet shutdowns order in Kashmir, and by the Bombay High Court in the Vinit Kumar v. CBI case**," they explained.

> **Lessons from the Vinit Kumar v. CBI case:** The Bombay High Court interpreted Section 5(2) of the Telegraph Act in light of the Puttaswamy judgement and actually ordered the destruction of evidence that was collected through surveillance since it did not comply with the parameters of the Telegraph Act. The Court concluded that evidence obtained unconstitutionally was not admissible in court. It applied the proportionality standards to the surveillance order and concluded that CBI didn't pass muster:
>
> 1. **Legal basis:** Public safety and emergency are very high standards. In this case, it was a question of corruption, and thus the surveillance was violative of Section 5(2) of the Telegraph Act and of Rule 419(A) of the Telegraph Rules.
> 2. **Least restrictive means:** The orders were overly broad and were thus not specific or proportional.

Lack of transparency and accountability for government agencies

Lack of Parliamentary or judicial oversight: "There is a big gaping hole in the PDP Bill as it doesn't talk about judicial or parliamentary oversight; it doesn't even actually have a review committee," bemoaned a speaker. Even under the *PUCL* judgement, the Telegraph Act, 1885, and the Information Technology Act, 2000, there is executive level oversight and a review committee that looks at all the decisions made about surveillance, they explained. A lawyer said that the rights to privacy judgement established that you need some semblance of oversight to give right to privacy its full meaning. Petitions challenging Section 5(2) of the Telegraph Act and Section 69 of the Information Technology Act are already pending before the Supreme Court as they don't mandate judicial or Parliamentary oversight, as directed by the Puttaswamy judgement.

Lack of transparency in the rule-making process: According to the PDP Bill, 2019, all safeguards and procedural obligations will be laid down by the regulator, that is, the Data Protection Authority, through a notification. This, as a speaker highlighted, means that there is no debate in the Parliament about these. Unlike the sections of the Bill which will be discussed in the Parliament, the rules and regulations, which will *actually* govern how the provisions are notified, will not be subjected to a debate. "Like the Aadhaar Act, much of what is laid down comes through regulations and is not laid down in the Act itself, and that is concerning," they said.

The Bill tries to create legal basis for private access to Aadhaar. A speaker explained that when Aadhaar was made mandatory for KYC for banks, the Supreme Court struck it down as it would not have been proportionate. However, the new Aadhaar amendments created a backdoor to the judgement because of which the amendments are now being challenged in the Supreme Court, they said. "**Sections of the PDP Bill effectively try to retrofit the Aadhaar ecosystem under the garb of public services.** They now want to include all private players in the Aadhaar ecosystem to be protected/given immunity under the Bill," they said.

A speaker went so far as to say that UIDAI doesn't even need to be exempted under Section 35 or Section 36 as the Bill has been written in a way "to accommodate Aadhaar's incursions into privacy". However, **another speaker said that commercial use of data collected for state purposes has been struck down as unconstitutional, citing the Supreme Court striking down Section 57 of the Aadhaar Act.** They argued that this will still largely be the case.

Read Part II of our notes on government access to data here. Read our coverage of the discussions here: #NAMA – India's Data Protection Law – January 2020.