Personal Data Protection Bill, 2019: Looking at use of video recordings, facial recognition software and drones by police

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the sixth article in the series. Read our extensive coverage of the Bill here.

By Vaneesha Jain

In *Puttaswamy,* the Hon'ble Supreme Court of India gave a resounding recognition to the Fundamental Right to Privacy under the Indian Constitution, and stressed the urgent need for an overarching data protection law to protect this right to privacy. The Personal Data Protection Bill, 2019, which is applicable to both Government as well as private entities, does this by putting in place a framework for notice and consent to the data principal before their data is collected or processed, imposing obligations for data protection on the data fiduciary and data processor, and setting up a mechanism for regulation and penalties for contravention.

The PDP Bill lays a strong emphasis on the obligation of any entity processing personal data to do so only for the purpose consented to by the data principal or which is incidental to or connected with such purpose. However, it also provides for certain deviations from this rule mandating prior informed consent in all cases, and these are the 'Exception' situations where personal data may be processed *without* obtaining prior consent — such as, when personal data must be processed in order to comply with an order or judgment of any Court or Tribunal in India.

The Bill also provides for 'Exemptions', wherein certain provisions of the Bill (extending beyond the 'consent' provisions alone) have no applicability in the situations provided as exempted. The exempted situations would play out as if there were no data protection law in place at all. Given that the need for an overarching data protection law to uphold the fundamental right to privacy was so strongly emphasised by the Hon'ble Supreme Court in *Puttaswamy*, the 'Exemptions' chapter should ideally be narrowly tailored to suit very specific situations that merit the abandonment of the protective cover of this law. However, on examination, we see that this is not so. Instead, in addition to providing for specific scenarios for exemption, the PDP Bill also provides some extremely broad exemptions, especially in favour of the Government.

What situations are 'exempted' from the application of the PDP Bill?

1. Specific situations: The protective cover of the core provisions of the Bill, which impose obligations on data fiduciaries, mandate stringent requirements of consent, ensure data principal rights, transparency and accountability measures and provide for protections while transferring personal data outside India, has been removed in specific situations, such as where personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any existing law.

2. Blanket exemption: In addition, there is a blanket exemption which can apply *at the discretion* of the Central Government. This broader exemption power allows the Central Government to remove any or *all* of the protections provided by the data law, to the processing, by a government agency, of *any* personal data that it may decide. It can do so by exempting the application of this law to any agency of the Government. Further, there is nothing in the law that would prevent the Central Government from adding to the list of exempted agencies, from time to time. The exercise of this power is conditioned upon the Central Government being satisfied that it is expedient to do so

1. in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or
2. 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.

Could this blanket exemption be used to allow the police to record protesters and use the information to arrest them?

Yes. The police, as a Government agency, could be exempted from the application of the data protection law by the Central Government, under the blanket exemption, by stating that the recording of protestors and subsequent arrests are being done in the interest of 'public order'.

In addition, if the protestors are seen as threatening to commit any act of violence punishable by law, then the recording of their personal data may be exempted from the procedural requirements of the data protection law, under the specific exemption relating to prevention, detection, investigation and prosecution of any offence or any other contravention of any law.

Typically, under these exemptions, it would be possible for the police to use handheld devices to record protestors in an Indian city, process the footage through a facial recognition software, cross-reference the results from the software on a national database of citizens (the Aadhaar database, the NPR and the NRC are all such databases) to find their personal details such as phone numbers and addresses and arrest them from their homes. While challenges to such arrest would exist by claiming democratic freedoms, the PDP Bill itself may not provide any recourse.

In fact, reports have already surfaced confirming that the Delhi Police has started using Automated Facial Recognition Software (AFRS) on footage filmed from protest venues.

Abroad, in countries such as Hong Kong and the United States, the threat of technology-based surveillance during protests has been widely recognised and circumvented by using face-masks to prevent the collection of facial recognition data — and governments have responded by introducing 'mask bans'. Such mask bans have been challenged as being unconstitutional in those countries, with some success. As the intensity of protests and anti-protest measures increase, it is highly likely that these issues will crop up in the Indian context as well.

Interestingly, if AFRS is considered to be a 'new technology' under the PDP Bill, then its continued use by the police might necessitate them being notified as 'significant data fiduciaries' under the Bill, with additional obligations such as registration with the Data Protection Authority.

The PDP Bill also categorically prohibits the processing of any sensitive personal data such as biometric data (which would be implicated by the use of AFRS) by a significant data fiduciary using new technologies, without first undertaking a data protection impact assessment, which must be reviewed by a data protection officer and submitted to the Data Protection Authority along with the review, and any subsequent directions/conditions imposed by the Authority for the use of such technology must be complied with.

Of course, these protective provisions, designed to further secure citizens against invasions of privacy using new technologies, may also be made inapplicable to a Government agency such as the police via a direction by the Central Government, if such a direction can be justified under one of the conditions for application of the blanket exemption provision.

Would the PDP Bill allow the sharing of drone-recorded information at a political rally for purposes of propaganda?

Assuming that the drones are used after complying with the extant domestic regulations for the use of drones in India, it may still have major implications for data privacy. In fact, in a recommendation for legislation around the use of drones, the Hungarian Data Protection Authority has emphasised that data processing with drone-mounted accessories has data protection implications. This is because even the proper use of drones can be very invasive into the privacy of people due to the ability and effect of the tool to collect data about everything that is in its field of vision, which is, compared to the use of similar technologies, unusually wide and can be changed very quickly.

The 'footage' recorded/collected by drones installed with cameras or other equipment to monitor or people would be 'personal data' within the meaning of the PDP Bill 2019 since the persons would be 'directly identifiable' with the footage recorded. It would further constitute 'sensitive personal data' as well: specifically, given the easy ability to process the drone-recorded footage on fa-

cial recognition software, the drone-recorded footage may constitute 'biometric data'; further, such footage recorded at a rally would also reveal 'political belief or affiliation' of a person, and can also be processed to further reveal religious belief, sexual orientation, transgender status, intersex status, caste or tribe, etc. Such categories of data are protected as sensitive personal data under the PDP Bill.

Recording of such data using drones, would constitute 'processing' as defined under the PDP Bill.

Now, the PDP Bill clearly provides that in case of processing of any sensitive personal data, the consent of the data principal must be explicitly obtained. 'Explicit consent' is the highest threshold for consent, and requires that in addition to the consent being free, informed, clear, specific and capable of being withdrawn, it must be obtained *after* informing the data principal the purpose of processing which is likely to cause significant harm, in clear terms without recourse to inference from conduct in a context and after giving her the choice of separately consenting to the use of different categories of sensitive personal data.

It would be practically impossible to meet this high threshold of obtaining 'explicit consent' from the people at the rally before recording them with drones. **Therefore, in view of the above, the police using drones to collect footage of people at a rally and then providing it to political parties for propaganda will be impermissible under the Bill.**

Thus, if the police still goes ahead and use drones to collect such data of people and provide it to political parties for purposes of political propaganda, they would attract penal liability under the PDP Bill, upto INR 15 crore.

Notably, when footage is recorded at a rally for purposes of use in spreading political propaganda/electoral campaigning, this is not exempted under the PDP Bill. This is because use of personal data/sensitive personal data for political propaganda cannot be legitimately justified as fulfilling any of the conditionalities required to trigger the exemption provisions — either the blanket provision as well as the specific exemptions. This is when the data protection provisions of the PDP Bill should kick into place to protect the privacy of individuals.

However, we cannot ignore the fact that the use of drones to capture footage during rallies and demonstrations is becoming increasingly normalised. In fact, in December 2019, there was a direction from the Madras High Court to the Police, as an interim measure, to videograph the entire area in which permission to carry out a demonstration, was sought — with specific permission for the use of drones, in order to identify leaders and hold them individually liable. The PDP Bill provides a specific exception to the need to obtain consent, when processing of personal data is done for compliance of any order of any Court in India.

Conclusion

In the first instance, the PDP Bill prohibits the recording of footage of protestors at demonstrations and rallies (given that the nature of recorded information constitutes personal data/sensitive personal data) without obtaining the highest threshold of consent from those being filmed, and provides strict penalties for doing so without obtaining prior consent.

However, these protective provisions may be easily circumvented by the police, by making use of the broad exemption provisions in favour of Government agencies, as provided under the Bill. Further, if such recording is done under direction of any Court or Tribunal in India, then the Bill provides an exception from the need to obtain consent in that case.

*

Vaneesha Jain *is an Associate Partner at Saikrishna & Associates, and works on Policy matters, in addition to advising clients in the fields of intellectual property, information technology and data privacy. She is currently based out of Bangalore. The views expressed in this article are solely the author's.*

Edited by Aditi Agrawal