Privacy in Public Space

The book is a manual for privacy activists, advocates, IT professionals, business managers, law enforcement officers and the government for comprehending the complex issues of personal data usage. It not only explains the Act but discusses the different perspectives that make professionals draw inferences of the legal provisions. The author, Naavi, is a pioneer in cyber law, the author of several books on cyber law and cyber crimes and a visiting faculty at many premier law institutes in the country. We reproduce a chapter which concerns the objections raised over the Delhi Police identifying rioters, who unleashed communal clashes in northeast Delhi, through face recognition

PRIVACY enthusiasts sometimes claim that the Right to Privacy does not extinguish in a public space. Recently when the Delhi Police used the face recognition to identify people engaged in riot through a CCTV footage in a public space, objections were raised in some quarters.

This has brought "Privacy in Public space" into debate and whether PDPA recognises such a right from the perspective of data protection.

In the Supreme Court judgement on Privacy, a couple of references were made to the Privacy in public space but neither the final order nor the reflection of the judges indicates any recognition of Privacy in public space.

At one place, Justice Chandrachud wrote, "It is important to underscore that Privacy is not lost or surrendered merely because the individual is in a public place". But this was in a context and he had earlier quoted a specific example where he wrote, "So, for example, taking one or more persons aside to converse at a whisper even in a public place would clearly signal a claim to privacy".

This was an indication that a person may demonstrate his preference of Privacy in a public place by some specific action. This cannot however be construed as a blanket recognition that a person should not be watched on a CCTV and identified especially when the purpose is to maintain public order and prevent a crime or investigate a crime.

It is perfectly within the powers of the law enforcement if the CCTV footage is collected for the purpose of security reasons. It is only when the information so collected is misused say when one of the persons in the police force uses it to harass a person with the information that we may say that the Privacy is infringed. Here the infringement is not because of the collection of the CCTV footage but because the information gathered legitimately, was used for a purpose other than a permitted purpose.

When CCTV footages are collected from a public place there should be no reasonable expectation that there would be a privacy right and hence there should be no case for preventing such an activity. The permission should be considered as "deemed" also because it is in the interest of the security of the state. If any person wants to opt out of such legitimate observation through a public CCTV, the law enforcement is at liberty to deem it as a suspicious behaviour.

The right to privacy is not a right to hide oneself even when his activities are such that it affects other people around. When a person is in a public place, by definition whatever he does has an impact on other individuals and hence

Photos: UNI

LIMITATIONS TO PRIVACY RIGHTS
(Left) A CCTV camera unit being installed by the police in Hyderabad; nobody can demand privacy rights when CCTVs are installed to prevent crime

the right of privacy cannot be extended too far. If such a right were available, and a person streaks across a public place in nude, one cannot blame him for his action.

When a person shows his face in a public place it should be considered that he has placed his picture in public domain and hence the question of privacy does not arise.

It has been a point of abundant caution that some CCTV owners put out a notice similar to "This place is under Video surveillance". This is more a deterrence to mitigate the possibility of misbehaviour rather than a legal necessity.

Sometimes a person is found in the company of others and one of them may take a picture and publish it say on his social media profile. It is possible that in such cases others in the picture may have objection to such a disclosure. But if the person who has published has not tagged the name of the other persons, then the picture as a property should be considered as a joint and several property of all the persons there in and any one of them can use it without specifically disclosing the identity of the other persons.

Similarly in a telephone conversation, doubts are often expressed as to whether the recording of the conversation without the express permission of the other person would violate the privacy. Though some countries may support such a position, it is the author's opinion that the conversation belongs to both and any of them can record it with or without the notice. If however a third party makes a recording then it can be called a privacy infringement.

The Government of India has now formed an expert committee under the chairmanship of Mr. Kris Gopalakrishnan to study the Data Governance aspects related to the "Non Personal data" left out of PDPA. In this reference, Government has made a reference to "Community data" as data which belongs to the community.

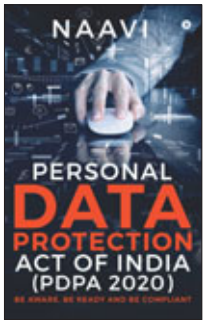
One example of this is when a group of persons travelling on a road contribute to traffic data captured by Google Maps. Though this could be aggregated anonymous data, it is a useful data belonging to the community. The committee may come up with its suggestions on how such data can be used.

Under Section 91 of PDPA, the Government may in consultation with the DPA direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulations of evidence based policies by the central Government.

This enabling provision is an indication that PDPA recognizes "Community data" which is collected by private companies on which the Government may demand a right for public good. There is a lobby which is currently trying to make the Government pay money for collection of such data.

However, since this data actually belongs to the community of people who have contributed to it, the Government may have its right to demand sharing of that data for the stated purposes which are for public good.

The Government and DPA may clarify this in due course when such an occasion to demand the information of that type arises. ■



Personal Data Protection Act of India (PDPA 2020)

Author: Naavi

Publisher: Notion Press

Pages: 334

Price: ₹600