Smart cities mission risks ushering in Orwellian future

Source: India Business Law Journal

Authored by Rachika A Sahay, Partner along with Aakash Sharma, Associate, HSA Advocates

The Smart Cities Mission was launched by the government in June 2015 with a goal to develop 100 smart cities by 2020 (the deadline has been revised to 2023 now). Though a "smart city" is not defined under the mission statement and guidelines, it includes certain core infrastructure elements essential for a smart city.

It focuses on e-governance, information technology connectivity and digitalization. It envisages rapid exchange of information between citizens, government bodies and third-party service providers.

The computing infrastructure, which includes city data centres, gives rise to privacy concerns and the risk of increased surveillance under the guise of promoting safety. Most smart city proposals received by the government under the mission include extensive installation of closed-circuit television (CCTV) cameras across cities.

The creation of a consolidated electronic database of information could exponentially expand the potential for identity theft. The wide range of connected devices also raises cybersecurity risks, especially with hackers now capable of affecting city-scale infrastructure. The storage and transmission channels of data in smart cities are also vulnerable to cybercrimes.

Although not specifically mentioned in the Constitution of India, the right to privacy has been read into the fundamental right to life and personal liberty under article 21 of the constitution by the Supreme Court as early as 1964. The right to privacy can be understood to have been established in India over the preceding six decades by six major decisions given by the Supreme Court as "not being absolute". In a more recent judgment, in the case of KS Puttuswamy (2017), the constitution bench of the Supreme Court underlined the importance of privacy in a public place.

Eye on legislature: In view of the threats to privacy that arise out of the smart cities mission, it is the duty of the state to put in place a data protection framework, which, while protecting citizens from the dangers to privacy from state and non-state actors, serves the common good. Currently, the law does little to protect individuals against such harm in India.

The transfer of personal data is governed by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPD rules), issued under section 43A of the Information Technology Act, 2000. While the SPD rules are an attempt at data protection, the pace of development of the digital economy has made the definition of sensitive personal data unduly narrow leaving out several categories of personal data from their boundaries. Moreover, they can only protect an individual against a breach by a "body corporate", breaches by other individuals and the state being outside their scope.

Though the government has introduced various draft policies for the smooth transition to smart cities, these have yet to be implemented into laws that can govern the mission. The Personal Data Protection Bill, 2018, is one such vital legislation.

The bill categorizes data into three different categories – personal data, sensitive personal data and critical personal data. Each category of data is (subject to the degree of sensitivity) required to be treated, procured and processed with a higher level of caution.

However, "critical personal data" has not been defined under the bill and the Data Protection Authority (to be constituted under the bill) has been tasked with notifying certain categories as critical personal data. Though the bill proposes safeguards, including some that have extra-territorial applicability, it may have to be revisited to remove the wide discretionary powers of the state and include specific mechanisms and processes instead.

A report on data privacy released by a committee of experts under the chairmanship of BN Srikrishna has taken a vociferous stand against state surveillance. The committee identified a list of 50 statutes and regulations that have potential overlap with the proposed data protection framework. Involving the relevant ministries early on is important to ensure appropriate consultation and complementary amendments. At this stage, a more pragmatic approach would be to devote all focus on stakeholder consultations and subsequently revisit the bill with a more holistic outlook.

The balance between the right to privacy and ease of doing business would be a tightrope walk. The buck, however, stops at effective implementation.