COVID-19: Implications on the Data Protection Framework in India

INTRODUCTION

The outbreak of COVID-19 and its development into a pandemic has led governments across the world to take extraordinary measures to protect their residents. The Central Government and various State Governments in India, along with public-health authorities, not-for-profit organizations and corporates, are collecting, tracking, and using information about individuals to slow down the spread of COVID-19; however, since a large proportion of such information could be categorized as 'personal data' or 'sensitive personal data' its use is subject to the data protection laws in India. It is, therefore, essential that a balance is struck between an individual's right to privacy and public interest at large. Separately, as a result of the COVID-19 pandemic, corporates are also required to implement aberrant measures to safeguard their employees and extended workforce. In this regard, the collection of personal data by corporates will need to be undertaken in compliance with the requirements of data protection laws in India.

This note discusses the use of technology platforms by the Government of India to curtail the spread of COVID-19 and the obligations of corporates in India in relation to their employees or business, in each case, in the context of the legal framework for data protection in India.

CURRENT LEGAL FRAMEWORK FOR DATA PROTECTION IN INDIA

The Information Technology Act, 2000 (the "**IT Act**") read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "**SPDI Rules**", together with the IT Act "**Data Protection Laws**") contain specific provisions governing protection of personal data in India. The SPDI Rules classify information related to physical, psychological and

mental health condition of a person as sensitive personal data or information ("**SPDI**") and any other information that relates to a natural personal which is capable of identifying such person as personal information ("**PI**").

The public-health authorities and corporates are able to collect personal information of an individual, such as medical records, data related to physical and mental health condition, body temperature, etc., however, such information is classified as SPDI under the Data Protection Laws and may only be collected subject to compliance with certain conditions specified under such laws (as described below). Further, information such as personal and official travel history of an individual or such individual's family members may not constitute SPDI but will be considered as PI.

SPDI is subject to greater protection under the Data Protection Laws. For example, such information may only be collected for a lawful purpose connected with a function or activity of the body corporate when such collection is necessary for that purpose; a person concerned must be aware of the fact that such information is being collected, intended recipients of the information, and the purpose for which the information is being collected; the provider of the information shall be given an option to not provide the information sought; and any organization or person holding such SPDI shall not retain that information for longer than is required for the purpose for which such information may lawfully be used. An organization collecting SPDI is required to obtain informed consent of the information provider prior to disclosing such information to any third party, except when such information is shared to government agencies in accordance with the Data Protection Laws. The SPDI Rules also specify that a corporate collecting personal data is required to comply with reasonable security practices and procedures such as the International Standard IS/ISO/IEC 27001 on "*Information Technology - Security Techniques - Information Security Management System – Requirements*".

Pursuant to the landmark decision of the Supreme Court of India in *KS Puttaswamy* v. *Union of India* (2017), the court held that right to privacy is a part of the right to life and personal liberty and is a fundamental right under the Constitution of India. The Supreme Court of India also observed that the right to privacy is not absolute; however, any restriction is required to be within the framework of law.

Proposal for change in Data Protection Laws in India

The Personal Data Protection Bill, 2019 (the "**PDP Bill**") was introduced in the lower house of the Indian Parliament in December 2019. The PDP Bill at large seeks to establish a robust data protection framework in India, including in relation to classification, collection and storage of personal data. For further details, please refer

to our analysis of the PDP Bill **here**.

The PDP Bill specifically describes 'health data' as the data related to the state of physical or mental health of the data principal (provider of such data) and includes, *inter alia*, records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services. The PDP Bill requires the informed consent of the data provider at the time of processing such information but also contemplates certain situations where such personal data may be processed without the consent of the data principal including to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual and to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health. The implications of such provisions will need to be analysed further once the PDP Bill is enacted and the relevant rules and regulations are in place.

DATA PRIVACY AND LOCATION TRACKING APPLICATIONS

On account of the lack of a vaccine for COVID-19, countries across the world have placed a lot of onus on the value of social distancing and containment to fight the pandemic. The World Health Organization also considers testing, isolation, and contact-tracing as the backbone of the fight against the virus. In this regard, countries are taking help of technology driven measures such as thermal screening, mass surveillance, location tracking, etc. to contain the spread of the virus. A number of countries, including India, have announced the launch of smartphone applications with different functionalities aimed at supporting the fight against COVID-19. While such applications could prove to be effective in containing the spread of the virus, they have started a debate on privacy concerns in relation to the misuse of data collected by the applications.

Position in India

The Government of India launched the *Aarogya Setu* application on April 2, 2020 which, *inter alia*, tracks the location of an infected individual and notifies the application users of their proximity to such individuals. The Data Protection Laws only provide a basic framework on data protection and not specifically contemplate measures to be taken by the public authorities in relation to protection of data during public health emergencies. Pursuant to *KS Puttaswamy*, the Supreme Court of India has observed that if the state preserves the anonymity of an individual it could legitimately assert a valid state interest in preservation of public health to design appropriate policy interventions on the basis of the data available to it. The *Aarogya Setu* application

requires its users to switch the GPS and Bluetooth tracking on at all times and has been criticized on the grounds that it could violate its users' privacy and could act as a surveillance tool in the hands of the government.

Similar applications are being used by the State Governments of Goa, Karnataka, Maharashtra and Tamil Nadu. The use by the State Government of Kerala of the *Sprinklr* application has also been criticized on the ground that sensitive personal information is being accessed by entity that is not based in India. In a recent petition challenging the contract between the State Government of Kerala and *Sprinklr,* the High Court of Kerala has issued an interim order in April 2020 asking the State Government, *inter alia*, to anonymize all data collected with respect to COVID-19 before sharing it with *Sprinklr* and to inform all citizens from whom data is taken that such data can be shared with *Sprinklr* or any third party and obtain the consent of such citizens. Further, the High Court of Kerala has restrained *Sprinklr* from committing any act that may result in breach of confidentiality of data collected under the contract with the State Government of Kerala and exploiting such data directly or indirectly for commercial purposes or advertising or representing to any third party that they have access to data relating to COVID-19 cases. The court also ordered *Sprinklr* to return all data to the State Government of Kerala once the contractual obligations are over and delete any residual or secondary data in its possession.

Position in certain foreign jurisdictions

The location tracking applications are being used in many countries such as Singapore, China, the United States, and in various member countries of the European Union. However, unlike India, the legal framework in these countries for data protection is far more comprehensive and nuanced. The European Union's General Data Protection Regulation has released comprehensive guidance on the use of such applications and the data collected and stored by them. These guidelines provide, *inter alia*, that the personal data collected is required to be anonymized and will be used only for the specifically defined purposes, that the applications will not be used for mass surveillance, and that individuals will remain in control of their personal data. The United Kingdom's Information Commissioner Office ("**UK ICO**") has released a statement stating that the data protection laws in the country do not prevent processing of personal data where it is used for the purpose of protecting against threats to public interest. The UK ICO has also stated that the where the data is properly anonymized and aggregated, it does not fall under data protection law because no individual is identified and, in such circumstances, privacy laws are not breached as long as the appropriate safeguards are in place. It has been reported that the National Health Service of the United Kingdom is working on releasing a smartphone-based contact-tracing application. While the United States does not have a unified federal data

protection law, there are certain sector-specific privacy laws that have been adopted. In addition, certain states have passed state-specific data protection acts which set boundaries on the use of personal data. Reportedly, the U.S. government is obtaining personal data from mobile advertisement companies instead of telecom providers given that use of data by telecom providers is highly regulated. Any such data is being shared with the Centre for Disease Control and state and local governments. Further, the U.S. government is also working with various technology platforms such as Apple and Google to develop location-tracing tools. Conversely, Israel has adopted a controversial emergency law that allows Israel's security agency to track mobile phones of individuals and collect data without a court order.

COLLECTION OF INFORMATION BY CORPORATES – ISSUES TO CONSIDER

In response to the COVID-19 pandemic, corporates have been asking their employees and business associates to share their and their family members' professional/personal travel histories, symptoms of illnesses of themselves and their family members, medical records, etc. As indicated above, information relating to medical records will qualify as SPDI under the Data Protection Laws and will require the consent of the person disclosing such information. Additionally, prior to collecting such information, corporates will need to create and implement a privacy policy for handling of or dealing in PI and SPDI.

In view of the above, corporates in India will need to consider adopting a data privacy policy in compliance with the minimum technical standards prescribed under the Data Protection Laws. Corporates will also need to establish a procedure and format in which consent is obtained from individuals from whom personal data is collected and establish a framework for the categorization, storage and dissemination of the personal data that is collected. The COVID-19 pandemic has caused employees to work from home, and, accordingly, matters of data security (including in relation to information, personal or otherwise, of business associates) will have to be considered by corporates going forward.

CONCLUSION

The current situation on account of the COVID-19 pandemic is unprecedented. The health authorities, corporates and other stakeholders are taking steps to contain the spread of the virus and measures such as data tracking and mass surveillance could prove to be effective in curbing the spread of COVID-19. However, keeping in mind that such personal data will be available in the long-term, the Government of India will need to strike the right balance between protection of public interest and maintaining

the fundamental right to privacy. Once the COVID-19 enforced lockdown in India eases, corporates in India (regardless of size) will increasingly have to grapple with the processing of SPDI and other personal data to minimize the risk of COVD-19. To this end, corporates will need to process personal data in compliance with the requirements of the Data Protection Laws while keeping an eye out for potential change in the Indian legal framework on account of the PDP Bill.

*This insight has been authored by **Shivaji Bhattacharya** (Partner) and **Anindhya Shrivastava** (Associate). They can be reached on sbhattacharya@snrlaw.in and ashrivastava@snrlaw.in for any questions.*