Technology Law Analysis

June 03, 2020

INDIAN JUDICIARY'S TAKE ON STORAGE OF COVID-19 PATIENT DATA OUTSIDE INDIA

- Case filed challenging the actions of the State of Kerala in outsourcing the processing of Covid-19 patient data to a non-Indian IT service provider.
- The Ministry of Electronics and Information Technology ("**MeitY**") expressed to the Court that sensitive personal data should always be in control of the State and stored in India.
- The Kerala High Court held that all data must be anonymised before it is shared with third party IT service provider, though no specific standards for anonymization set.
- The Kerala State Government subsequently issued guidelines for the collection and processing of Covid-19 related citizen data.

BACKGROUND

The Kerala High Court in the case of *Balu Gopalakrishnan v. State of Kerala,*[1] passed an interim order[2] focused on the protection of the personal data of individuals who tested positive / are suspected to have Covid-19 in the State of Kerala ("**State**"). This case arose due to concerns raised by the petitioner regarding the State contracting with Sprinklr Inc. ("**Sprinklr**"), a company based in the US, for the processing, analysis and storage of Covid-19 patient data outside India.

Sprinklr offers an online platform for the processing and analysis of Covid-19 data,[3] and has a specific *"Sprinklr for Government: Citizen Experience Management"* product aimed at assisting governments with their Covid-19 management efforts. As per the submissions of the petitioner, the State collects data of individuals who have tested positive / suspected to have Covid-19 and uploads it to Sprinklr's servers. Sprinklr then analyses the data and gives the State analysed data for their handling of the pandemic.

ARGUMENTS OF THE PARTIES

The petitioner (a lawyer) filed the case against the State, the Union of India ("**UOI**"), and Sprinklr. While this order captures the arguments of the petitioner, the State and UOI, Sprinklr's arguments appear to be pending. The arguments on record are as follows:

Arguments of the petitioner

The petitioner submitted that:

1. There was no need for the State to engage a foreign entity such as Sprinklr for storing such sensitive information, when government agencies like the 'C-DIT' and 'NIC' are well equipped to deal with the storage of data.
2. The safety of the sensitive medical data collected and stored by Sprinklr was in question and whether such data can be exploited by Sprinklr for monetary gains would need to be examined.
3. The State should inform and obtain consent from the persons from whom the data is collected.
4. As per the holding of the Supreme Court of India in the case of *Justice K.S Puttaswamy (Retd.) & Anr. V. UOI*[4] ("**Puttaswamy Case**"), the contract with Sprinklr qualified as a misuse of the arbitrary power of the State.
5. The contract with Sprinklr had been entered into without proper reference to applicable procedure and that it is in conflict with Article 299(1) of the Constitution of India[5] (which mandates that all contracts made in the exercise of the executive power of a State had to be entered into by the Governor or a person that he may authorise).
6. By submitting to the jurisdiction of New York courts, the State had made it impossible for both the State and its citizens to claim recourse to law in the event of a breach of contract by Sprinklr.

Arguments of the State of Kerala (Respondent 1)

The State submitted that:

1. The disclosure of Covid-19 data to Sprinklr was done as the State felt it essential that a *"scalable information technology system"* be employed due to the possible requirement of tracing over 80,00,000 citizens. It was further submitted that Government owned/controlled entities like 'C-DIT' and the 'Information Kerala Mission' are not technically equipped to manage large volume of data, and that there were no viable alternatives.

Research Papers

FAQs on Setting Up of Offices in India
December 13, 2024

FAQs on Downstream Investment
December 13, 2024

Gaming Law 2024
December 12, 2024

Research Articles

The Revolution Realized: Bitcoin's Triumph
December 05, 2024

The Bitcoin Effect
November 14, 2024

Acquirers Beware: Indian Merger Control Regime Revamped!
September 15, 2024

Audio

Securities Market Regulator's Continued Quest Against "Unfiltered" Financial Advice
December 18, 2024

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I
August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

"Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FII8 event in Riyadh
October 31, 2024

Analysing SEBI's Consultation Paper on Simplification of registration for FPIs

2. The Government had satisfied itself as to Sprinklr's credentials.
3. The State firmly believed that the confidentiality of the data of citizens was guaranteed as per the terms of the contract, and that the Government took full responsibility for the protection of data.
4. On the issue of the jurisdiction for dispute resolution being the Courts of New York, that the State had signed a standard form contract on the account of urgency. However, the State submitted that as "*the data resides in India (…) the breach of its confidentiality would expose Sprinklr to action in India.*"
5. The State would anonymise all personal data before it is disclosed to Sprinklr.

Arguments of the Union of India (UOI) (Respondent 2)

The UOI submitted that:

1. MeitY is firm in their resolve that "*sensitive personal data of Indian citizens should always be in the control of the State and should necessarily be stored in the State Data Centres or in the National Data Centres.*"
2. Their singular concern was that the confidentiality of the data of citizens should be never breached. It was also submitted that the State ought not to have accepted the jurisdiction of the courts in New York, and that the contract did not have enough confidentiality clauses.
3. There was no need for the State have contracted with an entity outside India when there are several entities in India equally or more competent. It was further submitted that had the State approached the Central Government, they would've been able to give them the same or better support, and that they would be able to do so once the period of the contract is over.

COURT'S ORDER

At the outset, the Court stated that it was not willing to speak affirmatively on the various allegations made by the petitioners at this stage as the Respondents had not completed their arguments. Further, it was noted that the Court did not think it prudent to issue any orders that would impede the efforts of the State in fighting the pandemic. The Court also stated that it was their intent *"to ensure that there was no "data epidemic" after the Covid-19 epidemic is controlled."*

The Court therefore focused solely on the breach of confidentiality issue and issued the following interim directions in this order, which we have summarised below:

1. *Anonymisation of Data* - The State and its concerned departments to anonymise all the data that has been, and will be collected before allowing Sprinklr access.
2. *Obtaining Specific Consent* – All citizens need to be informed that the data collected from them is likely to be accessed by Sprinklr or other third party service providers, and their specific consent to such effect to be obtained in the necessary forms or formats.
3. *Breach of Confidentiality* – Sprinklr must not commit any act which will be, directly or indirectly, in breach of confidentiality of the data entrusted to them; and should not disclose or part with any such data to any third party/person/entity.
4. *Return of Data* – Once their contractual obligation ends, Sprinklr was directed to entrust back all such data to the State.
5. *Bar on advertisement* – Sprinklr was prohibited from advertising or representing to any third party/person/entity that they are in possession or have access to any data regarding COVID-19 patients or persons vulnerable/susceptible to it.
6. *No Commercial Exploitation* - Sprinklr was further barred from using / exploiting the data, or the name and the official logo of the Government of Kerala, directly or indirectly, for any commercial benefit.

GUIDELINES ON DATA COLLECTION AND PROCESSING

Post the passing of the Court's order, the State reportedly[6] submitted to the Court that it was in "full and exclusive ownership of the data" which will be analysed by the State-owned Centre for Development of Imaging Technology (CDIT), and not by Sprinklr. Further, the data is now stored in a cloud storage account owned by CDIT and that Sprinklr was asked to delete any residuary data with it, if any. Hence, there appears to be substantial changes made to the arrangement with Sprinklr by the State post receipt of directions from the Court.

Subsequently, the State released a circular[7] with certain guidelines to be followed in the collection of Covid-19 related personal information of citizens ("**Guidelines**"). These Guidelines include the following:

1. In the event that data collected will be shared with third party service providers for processing:

- The data collected in the past and to be collected going forward should be anonymised before it is shared; and
- Individuals need to be informed, and specific consent needs to be taken for the sharing of their data with such service providers.

2. The privacy policy is to be made available in English as well as **vernacular languages** in the app or website through which the data is collected.

3. Data Storage: To the extent possible:

- Data is to be stored in an encrypted form in the State Data Centre.
- If data is to be stored in a cloud, the cloud service provider ("**CSP**") used has to be approved by the Government of India as per guidelines issued by MeiTY, and
- If a third party system is used, the system be ISO 27000 enabled.

4. In the event data is collected in an involuntary manner via an automated device through GPS or Bluetooth, this must be done on prior explicit consent .

ANALYSIS

Some important takeaways from this case are as follows:

September 26, 2024

Scope of judicial interference and inquiry in an application for appointment of arbitrator under the (Indian) Arbitration and Conciliation Act, 1996

September 22, 2024

1. ***Public / private partnerships***

   These are challenging times, where the Central as well as various State governments are making efforts to monitor and detect the spread of Covid-19. An argument made by the UOI (which the Court did not comment on) was that there was no requirement for the State to have gone in search of foreign entities to handle the processing of Covid-19 data, when there are several companies in India who are equally or more competent.

   However, as the requirement for more novel data analytics arises for the better management of Covid-19, it is likely that we will see similar partnerships between private companies and the government in order to tackle this disease. Such partnerships may be more beneficial and efficient for contact tracing and data analysis and should not be discouraged Keeping in mind that handling the pandemic in the most efficient manner is in the interest of all, blanketly clamping down on any potential foreign partnerships may not always be the best solution. However, the key being building necessary safeguards to protect the data and minimize any risks which could arise from its usage.

   However, in light of the Court's interim order, it would be important for any future partnerships to take into account and abide by the six observations of the High Court, be it the need to have watertight confidentiality clauses, the requirement to adequately anonymise and protect data, and have adequate enforcement mechanisms. In the event private parties wish to contract with a Kerala Government department / agency for the processing of Covid-19 data, the Guidelines would also have to be followed.

1. ***MeitY's preference for data localisation***

   UOI's submission on MeitY's resolve that "*sensitive personal data of Indian citizens should always be in the control of the State and should necessarily be stored in the State Data Centres or in the National Data Centres"* is an important indication of how MeitY wishes to treat sensitive data of individuals going forward. This intention is also reflected in the proposed *Personal Data Protection Bill, 2019* ("**PDP Bill**"), where a copy of all sensitive personal data[8] is required to be stored in India.[9]

1. ***Fundamental right to privacy***

   In the Puttaswamy Case, Article 21[10] of the Constitution was expanded to recognize privacy as a fundamental right, which can be claimed by individuals in India against the State. The Supreme Court clarified that like most other fundamental rights, the right to privacy is not an "absolute right", and is subject to the satisfaction of certain tests and reasonable restrictions. Therefore, the infringement of any fundamental rights will have to pass the basic tests under Articles 14[11] and 21 of the Constitution, i.e.: (1) the existence of law to justify an encroachment on privacy; (2) the requirement of a legitimate state aim; and (3) that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action. Protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge were cited as examples of legitimate state aim in the Puttaswamy Case.

   While the petitioner had argued that the State's actions were arbitrary and did not fulfil the above test, the Court in the last available order did not address this point. Going forward, state governments will have to keep in mind that the Supreme Court in the Puttaswamy case had recognised that individuals are within their rights to claim a fundamental right of privacy against the state. Any derogation from the privacy of individuals would necessarily have to fulfil the above test.

1. ***Standards of anonymisation***

   The High Court mandated that Covid-19 data be anonymised before it is shared, but does not prescribe recommended standards of anonymisation. In this day and age, where the re-identification of data is easily done, it is necessary for the Government to prescribe sufficient safeguards to ensure the irreversible anonymisation of data. The current data protection law and the PDP Bill also does not prescribe anonymisation standards.

1. ***Necessity for consent***

   The High Court mandates that informed consent and notice be taken from users for the transfer of the data to Sprinklr. However, where the State collects personal data from citizens, anonymises such data and only then discloses the anonymised data, there should be no legal obligation for obtaining consents in relation to the disclosure of the anonymised data – under both Current Law and in the PDP Bill. Consent and notice would be necessary only in the event that identifiable personal data is disclosed.

1. ***Enforcement in cross border arrangements***

   In this scenario, if the State were to initiate appropriate legal proceedings against Sprinklr, it could do so in the courts of New York. However, there may be practical difficulties involved in doing so, especially wherein obtaining relief by the State is time-sensitive. If the State were to seek certain reliefs from competent courts in India, enforcement of such court orders against Sprinklr may also be a challenge given the lack of reciprocity in enforcement of court decrees between US and India.

   In such cases, involving State Governments or the Central government engaging non-Indian service providers, it would be beneficial to have a more favourable mode of dispute resolution clauses incorporated in the contract. If there is no reciprocal arrangement between India and the jurisdiction of the service provider for enforcement of court orders, then alternate modes of dispute resolution should be considered basis its enforceability, such as arbitration.

– Inika Charles, Aaron Kamath & Huzefa Tavawalla
You can direct your queries or comments to the authors

[1] Kerala High Court, WP (C) Temp. no. 84 (2020), April 24, 2020.

[2] The Kerala High Court had clubbed related petitions filed against Sprinklr and passed a common order.

[3] More information is available at https://www.sprinklr.com/ (last accessed May 16, 2020).

[4] Supreme Court, Writ Petition (Civil) No 494 Of 2012.

[5] Article 299(1): *"All contracts made in the exercise of the executive power of the Union or of a State shall be expressed to be made by the President, or by the Governor of the State, as the case may be, and all such contracts and all assurances of property made in the exercise of that power shall be executed on behalf of the President or the Governor by such persons and in such manner as he may direct or authorise."*

[6] https://www.business-standard.com/article/pti-stories/sprinklr-will-have-no-role-in-analysing-covid-19-data-kerala-govt-informs-hc-120052101562_1.html & https://www.newindianexpress.com/states/kerala/2020/may/22/sprinklr-out-data-now-in-c-dit-cloud-kerala-govt-to-hc-2146379.html (last accessed May 29 2020).

[7] https://kerala.gov.in/documents/10180/11cd8afd-cc46-49d3-93e0-3eae847f686a (last accessed June 2 2020).

[8] Sensitive Personal Data under the PDP Bill has been defined to mean personal data revealing, related to, or constituting, as may be applicable: (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other category of data specified by the Data Protection Authority constituted under the PDP Bill.

[9] Section 33, PDP Bill.

[10] Article 21 states that: "*No person shall be deprived of his life or personal liberty except according to procedure established by law*".

[11] Article 14 states that "*the State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India*".