Mitigating the Impact of COVID-19 Through Technological Interventions is India Legally Equipped: Aarogya App Case Study

Sukhpreet Kaur[1], Seerat Gill[2], Namita Bhardwaj[3], Rajinder Kaur[4]

[1]Assistant Professor, Department of Pharmacology, Dasmesh Institute of Research and Dental Sciences, Faridkot, [2]Law Student, Rajiv Gandhi National University of Law, Punjab, [3]Research Scholar, Department of Laws, Panjab University, Chandigarh, [4]Director, University Institute of Legal Studies, Panjab University, Chandigarh

Abstract

Tremendous utilisation of technology during lockdown and quarantine for COVD-19 pandemic has been observed. The health care agencies are making best possible efforts to fight the pandemic. The phone applications for tracing proximity to people to identify infection hotspots and possible transmission is also gaining popularity. Various countries have launched apps which can be installed in smartphone for contact tracing. Indian government has also launched Aarogya Setu app. The launch of this app fueled alot of discussion as compliance with patient privacy and human rightsissues. This app constantly monitors GPS location of an individual which is considered as an invasion of privacy by legal experts. Although Aarogya Setu app has many in built privacy features to protect sensitive data. In 2017 Supreme Court held privacy to be constitutionally protected right under Article 21 of the Indian Constitution. The same was followed by introduction of Personal Data Protection Bill in Parliament in year 2018 and again in 2019. However, it still remains in the form of bill only. Further, in *Puttaswammy Judgement* Supreme Court allowed states to collect data for certain legitimate purpose where there is state or public interest. COVID-19 has definitely accelerated the need to have stronger data protection legislation in India to protect patient privacy. Stronger data protection law will only add to the legitimate, efficient and careful processing of important data which is required to fight against the pandemic.

Keywords: *COVID-19, Aarogya Setu app, Data Protection, Digitalisation, Contact tracing.*

Introduction

COVID-19 originated from China in December 2019 which later became global pandemic. During COVID-19 pandemic technologies are playing crucial role in fulfilling day to day needs in time of lockdown and quarantine. Trends of online shopping, robot deliveries, digital and contactless payments, work from home, distance learning, telehealth, online entertainment and drones for sanitization are gaining popularity during pandemic. Apart from these, digital contact tracing is also being used totackle COVID-19 pandemic. These smart phone applications (apps) are being considered for tracing proximity of people to determine possible sources of transmission[1]. Such technical solution requires patient privacy protection otherwise benefits can be undermined due to low adoption. Various countries launch apps for contact tracing as manual contact tracing may require a lot of time and resources[2]. For instance, Australian Government launch COVIDSafe and Indian Government launch Aarogya Setu app. The launch of these apps has fueled a lot of discussion on complying with privacy and human rights frameworks, including whether this information can, in fact, ever be anonymized[3]. Fully effective anonymisation is not possible when collecting data as gross as regular interaction with others in addition to age, gender and pincode demographics, as has been

Corresponding Address:
Dr. Sukhpreet Kaur
Department of Pharmacology, Dasmesh Institute of Research and Dental Sciences, Talwandi Road, Faridkot, Punjab
e-mail: drsukhpreetchd@gmail.com

demonstrated by previous attempts to de-anonymise data[4]. If these data are unintentionally or purposely linked with other datasets part of cloud computing[5], anonymity is virtually impossible to guarantee. Civil society in the United Kingdom called for clear and comprehensive primary legislation to regulate data processing in symptom tracking and digital contact tracing applications, including with a strict purpose, access and time limitations[6]. Such regulation may improve trust.

Indian initiative in digital tracking: Aarogya app: As the COVID-19 pandemic gripped the country, a nation- wide lockdown was enforced in March, 2020. The health workers along with other government services embarked upon a process of controlling the spread of novel corona virus in the nation. Other than the efforts to ramp up the hospitals to curb the pandemic, the digital efforts by the Government of India included introduction of the Aarogya setu application to control the spread of the virus by digitally tracking COVID- 19 patients or people at- risk of getting the disease. The Prime Minister of India, in its address to nation urged the countrymen to download the application as it would help the Government identify the potential risks and provide immediate help.

The app aims at providing users information as to whether they are prone to a COVID-19 infection by analysing their proximity to COVID-19 positive persons. The app requires the user to submit the user's geodata. It also uses bluetooth to connect to other registered users and from the network thus formed, analyse whether the user has come in contact with anyone who has been tested positive. The app, as per its terms of service is intended to "notify, trace, and suitably support" a registered user regarding COVID-19 infection[7].

Working model of Aarogya setu application: The application uses the location and Bluetooth information of the phone in order to analyse if an individual has been in close proximity to a person who had been infected by the virus by comparing with the database already prepared by the Government. The application calculates the risk of infection based on how recent it was, the proximity and recommends measures. The registration of the application is voluntary. The user needs to provide name, gender, age, profession and information about foreign travel in the past 30 days in addition to the mobile number. A unique device identity number (hereinafter referred DID) is allotted to the mobile number provided at the time of registration. It is this DID that is used for future interactions with other devices. The whole information including personal information and details of interaction with other devices is encrypted and stored on Aarogya Setu servers[8].

Privacy concerns: The application constantly monitors the GPS location of an individual which is considered as an invasion of privacy by legal experts. Many other countries have also utilized contract tracing applications to keep a track on virus spread. Though the objective of all these apps is similar they somewhat differ in the process. For instance, the Trace Together application used by Singapore does not collect GPS information and the data can only be used by health ministry officials. Similarly, U.K. has the data centrally stored with National Health Service (NHS) servers. The data stored on servers can be utilised by the health workers as well as law enforcement agencies in U.K. to identify the hot spots based on GPS data[9]. Thus, practically the government can obtain the information on individuals who are sick and obtain their location as well. India does not have stringent data privacy laws as such which makes the medical data vulnerable because of the lack of regulation process of the data.

Privacy features: The medical data is considered as personal sensitive data. The Aarogya setu application has many in built privacy features to protect the sensitive data. The personal information is anonymized by assigning a DID to the mobile number and using the same for future reference. The whole information is encrypted and stored. The location information and contact tracing information is stored locally on the mobile devices and uploaded on the server only of individual test positive. This information is permanently deleted from the device at every 30 days cycle if the individual does not test positive. The information which might have been uploaded to the server will be deleted at every 45 days cycle. If someone test positive the contact tracing info is deleted from the server after 60 days[8].

The government has taken a significant step in utilizing technology to check the spread the of novel coronavirus. Human contact tracing is a long and cumbersome process. In such a scenario, the application will definitely provide useful information to the agencies. The application has largely addressed the privacy issues by encrypting the stored data on the servers. With a total of 13.11 crore people enrolled (as on 19thJune 2020), the application would provide useful data to the

health workers. The host of facilities on the application like self-assessment test and helpline number will also provide easy help to patients to identify if they are at risk and obtain immediate medical help when required.

International Data Protection Regime: International Position in European Union (E.U.), privacy is considered as a Fundamental Right. The recently enacted General Data Protection Regime (GDPR) recognises the importance of Data privacy as a human right and thus provides a comprehensive law on data protection and privacy which its member states are bound to incorporate in their respective states. There is no law in E.U. which gives unbridled power to the member states for surveillance and data retention. In U.S.A., data privacy is not considered as a fundamental right. It is considered more of a consumer right and thus there is no comprehensive law on data protection; it is scattered in different laws. The surveillance practices of U.S.A. have been found covert and arbitrary. However, with the passing of new surveillance laws, these surveillance activities have been made legal. In Australia, the legislature and the Government has been the most active in passing legislations to deal with the legal issues arising from technological advancements. In U.K., the Data Protection Act, 2018 caters to the challenges of I.T. technological advancements. The recent law on surveillance Investigatory Powers Act, 2016 explicitly provides for tools that facilitate electronic surveillance for combating terrorism and anti- national activities. In China, the Government has laid down rules through law on protecting data privacy. However, the surveillance activities undertaken by the Chinese Government are so covert that the Law seems to be inadequate in protecting the data privacy of individuals[10].

Data Protection in India: In 2017, a ninejudge bench of the Supreme Court unanimously held privacy to be a constitutionally protected right under Article 21 of the Indian Constitution[11]. The court also laid down certain benchmarks which every governmental action had to suffice in case any infringement of privacy is sought for[11]. Following this, a Committee was constituted under the chairmanship of Justice B.N. Srikrishna for laying down the framework of data protection legislation in India[12]. The committee recommended identifiability of the data being processed to have a significant bearing on the definition of personal data and suggested bringing besides identifiable data, de-identified data and up to certain extent anonmyised data as well under the purview of the legislation[12]. The committee further categorizing health data under the category of sensitive personal data, acknowledged that the same is more prone to infringing privacy of the data principal[12]. The same was followed by introduction of a Personal Data Protection Bill in Parliament in the year 2018 and again in 2019. The preamble to the bill states that "the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy"[13]. However, the same is still in the stage of a bill and therefore, India as of now does not have a dedicated legislation on data protection and data privacy which makes its position very vulnerable. Certain provisions of IT Act, 2000 along with the Rules framed by the Government of India is the only legal protection for ensuring data privacy and against arbitrary surveillance by Government agencies; which are inadequate in the present day dependence of individuals on cloud enabled applications and insufficient to provide a strong legal platform for India's ambitious 'Digital India' and 'Make in India' projects.

Aarogya Setu and Contact Tracing- The lawful justification: In 1998, the Supreme Court held that right to privacy is not absolute and can be curtailed on the ground of protection of health of other individuals[14]. The same was reiterated in the 2017 judgment of the Supreme Court wherein Justice D.Y. Chandrachud held that "Like other rights which form part of the fundamental freedoms protected by Part III, including the right to life and personal liberty under Article 21, privacy is not an absolute right"[15]. The Court held "compelling state interest" or "public Interest" as one of the grounds where infringement of privacy can be allowed. The judgment repeatedly referred to the European Union's regulations of 2016 which have as well mentioned public interest as one of the restrictions on the right to privacy. The same was reiterated by Supreme Court in CPIO v. Subhash Chandra Agarwal (2019) wherein it was held that the personal information including medical records, treatment etc. is entitled to protection from unwarranted invasion of privacy of that individual however, conditional access may be guaranteed wherein larger state interest is justified by the government[15].

The Balance Test: The recent judicial pronouncements though allowing states to collect data for certain legitimate purposes have imposed strict checks to ensure careful and legitimate handling of the data. The Supreme Court in the Puttaswamy judgment held that in all the cases even where defense of state interest is taken to justify infringement of privacy,

a three-fold requirement has to be justified by the government. Primarily, there must be a law justifying the infringement, secondly there must be a legitimate state aim ensuring that the same fulfills the mandate of reasonableness under Article 14 of the Constitution and third, the means chosen to achieve the end should be proportionate[15]. Justice DY Chandrachud quoting Christina P. Mondis who stated that "information collection can be swiftest theft of all"[16] concluded that a delicate balance has to be drawn in the legitimate interests of the state and the individual interests of protecting one's privacy[14]. The Kerala High Court in April 2020[17] while deciding on a case concerning a contract signed by the Kerala government with Sprinklr Inc., to analyze the data of COVID 19 susceptible individuals, affixed responsibility on the state to ensure anonymisation of all the sensitive data and held that "controlling COVID-19 pandemic cannot lead to a data epidemic"[18]. The right of a state on account of public interest to collect the data cannot be an opportunity for absolute violation of right to privacy of individuals.

Future Perspective: The need for Data Protection Legislation: COVID-19 has definitely accelerated the need to have a stronger data protection legislation in India. As of now, the privacy law in India is governed by multiple judicial pronouncements and legislations. This adds to the uncertainty in the legal sphere and consequently leads to a common man facing formidable hurdles while determining his rights and duties. To ensure a proper balance between the confidentiality of data and processing of personal data if mandated by the social circumstances, it has to be assured that none is favored at the very outset. This can only be ensured when a stronger data protection regime is in the place. Collection of data in a sensitive situation like this has definitely accentuated the spread of information and knowledge to control the novel coronavirus, however, it has to be ensured that no situation like present should be used as an opportunity for abhor infringement of a right which has been accorded the status of a natural and inalienable right. Stronger data protection law will only add to the legitimate, efficient and careful processing of important data which is required to fight against the pandemic.

Conflict of Interest: There is no conflict of interest

Funding: Self

Ethical Clearance: The study was approved by the Institutional Ethics Committee of Dasmesh Institute of Research and Dental Sciences, Faridkot

References

1. Servick K. Science (Internet). COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work? (cited 2020 July 10). Available from: https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how.
2. Leins K, Culnane C and Rubinstein B. Tracking, tracing, trust: contemplating mitigating the impact of COVID-19 through technological interventions. Med J Aust .2020;213(1): 6-8.
3. Culnane C, Leins K. Misconceptions in privacy protection and regulation. Law in Cont 2020; 36:1–12.
4. Narayanan A, Shi E, Rubinstein BIP. Link prediction by de-anonymization: how we won the Kaggle social network challenge. International Joint Conference on Neural Networks; 2011 July31–Aug5; San Jose (USA): IEEE Press, 2011.
5. Culnane C, Rubinstein BIP, Teague V (Internet). Stop the open data bus, we want to get off. (cited 2020 June 20). Available from: https://arxiv.org/abs/1908.05004.
6. Matrix Chambers (Internet). London: Legal advice on smartphone contract tracing published. (cited 2020 May 10). Available from: https://www.matrixlaw.co.uk/news/legal-advice-on-smartphone-contact-tracing-published/.
7. Our Concerns With TheAarogya Setu App (Internet). (cited 2020 July 7). Available at https://sflc.in/our-concerns-aarogya-setu-app.
8. Privacy policy of Aarogya setu application (Internet). (cited 2020, June 17). Available at: https://static.mygov.in/rest/s3fs-public/mygov_159051645651307401.pdf.
9. Alice Mollon. The Economist (Internet). The pandemic has spawned a new way to study medical records. (cited 2020 May 17).Available at: https://www.economist.com/science-and-technology/2020/05/14/the-pandemic-has-spawned-a-new-way-to-study-medical-records.
10. Schwartz PM, Peifer KN. Structuring International Data Privacy Law(Internet). (cited 2020, July 2). Available from : https://www.law.berkeley.edu/wp-content/uploads/2019/10/Schwartz-Intl-Data-

Privacy-Law-21.pdf.

11. Justice K.S. Puttaswamy (Retd.) v. Union of India, W.P. (C) No. 494 of 2012
12. Report of the Committee of Experts on a data protection framework for India under the chairmanship of (retd.) Justice B.N. Srikrishna (cited 2020 June20). Available from: https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
13. Personal Data Protection Bill, 2019, Preamble
14. Mr X v. Hospital Z, 1998, 8 SCC 296
15 Per J. D.Y. Chandarchud in K.S. Puttaswamy (Retd.) v. Union of India, 2017, pp 264
16. Christina P. Moniodis. Moving from Nixon to NASA: Privacy ‘s Second Strand- A Right to Informational Privacy. Yale Journal of Law and Technology, 2012;15 (1),:153.
17. Balu Gopalakrishnan v. State of Kerala, 2020, W.P. (C) 9498 of 2020
18. Anonymous, “Cases- Balu Gopalakrishnan v. State of Kerala” Columbia Global Freedom of Expression (cited 2020 July 9). Available from: https://globalfreedomofexpression.columbia.edu/cases/balu-gopalakrishnan-v-state-of-kerala-and-ors/