

AAROGYA SETU WITHIN THE CONTOURS OF PRIVACY LAW IN INDIA

Snigdha Gupta* & Mayuri Gupta**

INTRODUCTION

The COVID-19¹ pandemic has somewhat locked us inside our own houses, but would it not be strange to realise that every time we step out of our own house, someone has an eye on us and knows about our every movement?

When the coronavirus disease started spreading all over the world at a rate of knots, India, being a very populous country², found it very difficult to come up with any measure that immediately could address the situation at that point of time. On 24th March, 2020 a nationwide lockdown was imposed in India under the National Disaster Management Act, 2005³ which put the country to a standstill.

* *Student-B.A.LL.B.(H)* @ Amity Law School, Kolkata; Email: snigdha Gupta0@gmail.com

** *Research Scholar* @ Gujarat National Law University, Gandhinagar; Email: mayurigupta55@gmail.com

¹ International Committee on Taxonomy of Viruses (ICTV) on 11th February 2020 announced 'Severe Acute Respiratory Syndrome Coronavirus 2' (SARS-CoV-2) as the name of the novel coronavirus. The World Health Organization on 11th February 2020 announced 'COVID-19' as the name of the new disease caused by the SARS-CoV-2. Available at: [https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-\(covid-2019\)-and-the-virus-that-causes-it#:~:text=The%20International%20Committee%20on%20Taxonomy,two%20viruses%20are%20different](https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it#:~:text=The%20International%20Committee%20on%20Taxonomy,two%20viruses%20are%20different) (Accessed on: 09.01.2021).

² India has a population of 1,380,004,385 in 2020, according to UN data, which is equivalent to 17.7% of the total world population, that is almost 138 crores, Available at: <http://data.un.org/en/iso/in.html> (Accessed on: 09.01.2021)

³ Under Section 2(d) of the National Disaster Management Act, 2005 'Covid-19' was declared as a notified disaster by the Ministry of Home Affairs vide Letter No.33-4/2020/NDM-1 dated 14.03.2020 to chief secretaries of all States <https://www.mohfw.gov.in/pdf/RevisedItem&NormsforutilisationofSDRFdt14032020.pdf>, (Accessed on: 09.01.2021)

The Ministry of Home Affairs, acting through the Home Secretary in his capacity as Chairperson of the National Executive Committee, issued the order of lockdown under the Section 10(2)(l) of the National Disaster Management Act, 2005 vide Letter DO No. 40-3/2020-DM-I(A) dated 24.03.2020 w.e.f. 25.03.2020 till 14.04.2020, Available at:

With the rising number of cases, arose the need for the use of technology to develop tools for contact tracing to break the chain of human-to-human transmission of the disease. In line with the contact tracing tools developed by various countries across the world, on 2nd April 2020, the Government of India released a mobile application called “Aarogya Setu” for the very purpose of contact tracing of infected individuals, exposure notification and allow health departments to take effective actions in order to manage the COVID-19 pandemic and enhance their preparedness. Aarogya Setu could inform persons at risk of the precautions to be taken by them, identify individuals exposed to the infection, and help manage quarantining, follow up and effective treatment, resultantly.

This means, Aarogya Setu although could not stop the spread of COVID-19 completely but could somewhat control it. This app, on installing, would ask you to take a self-assessment test, i.e., it will ask for your name, your mobile number and then you have to give your Bluetooth and location information as well so that firstly, the government authority controlling this app would know about your movement and details regarding that and secondly, if you are infected with the virus, people coming in contact with you could be made aware of it. However, this brings us to a question “*Is Aarogya Setu app contrary to the Right of Privacy in India?*”

Right to Privacy is a fundamental right given to every individual in India under Article 21⁴ as a part of the freedoms guaranteed by Part III of the Constitution. This basically includes that every individual in India has a legal right to enjoy their private life without any involvement of the rest of the world and the government of the country as far as any illegal activity is not seen.

Both the decisions of the Hon’ble Supreme Court of India and the Government of India, i.e., giving the Right to Privacy a fundamental value by the Supreme Court in 2017, and launching the Aarogya Setu app by the Government of India in 2020 were in a good faith and in favour of the citizens. But soon after its launch, the Aarogya Setu app was surrounded by controversies claiming the infringement of the right to privacy and personal freedom guaranteed under the Constitution of India. Several points were put forward, on the one hand

https://www.mha.gov.in/sites/default/files/PR_MHAOrderDt14042020forextendingtheLockdownPeriodtill03052020_14042020.pdf (Accessed on: 09.01.2021). This lockdown was further extended.

⁴ Article 21- Protection of life and personal liberty- No person shall be deprived of his life or personal liberty except according to procedure established by law.

advocating the need and urgency of launching the Aarogya Setu app whereas the other, defending the need to secure the right of privacy protected by the Constitution. In this article, the authors will try to incorporate such debates and examine the legality of the Aarogya Setu app on the litmus paper of right to privacy in India.

THE IDEA OF RIGHT TO PRIVACY IN INDIAN CONSTITUTION:

On 24th August 2017, after a series of debates, discussions and decisions over past 60 years, the idea of giving right to privacy a fundamental value guaranteed by the Constitution was developed in the case of (*Retd.*) *Justice K.S. Puttaswamy v. Union of India*⁵.

In 2011, the central government introduced the Aadhaar card as a new identity document and established the Unique Identification Authority of India (UIDAI) to issue Aadhaar with 12 digit unique identity number. In 2012, Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court, filed a writ petition in the Supreme Court against the functioning of the Aadhaar Card introduced by the UPA government, stating that this scheme has no constitutional validity. He opposed the move of the government in making the Aadhaar Card mandatory for the welfare schemes like, Public Distribution System, Mid-Day Meal, MGNREGA⁶, asserting that welfare schemes are meant for every citizen of the country and it is their constitutional right to get it. He further mentioned that through this Aadhaar Card scheme the government is gathering the biometric data of the citizens of the country like fingerprint scan, iris scan, facial scan. The details collected would be stored in a central server by the government and if by any chance the data got leaked, then there would be a high chance that these data could be misused and hence petitioning that the right to privacy of the citizens was on stake.

On 11th August 2015, a Bench of three judges⁷ passed an order that a bench of adequate strength must examine the judgement passed in *M. P. Sharma v. Satish Chandra, District Magistrate, Delhi*⁸ and *Kharak Singh v. State of Uttar Pradesh*⁹. Primarily, the 3 Judges

⁵ (2017) 10 SCC 1

⁶ Mahatma Gandhi National Rural Employment Guarantee Act, 2005

⁷ Hon'ble Justices Chelameshwar, Bobde and C. Nagappan

⁸ 1954 AIR 300 (8 Judges Bench) Hon'ble CJ. Mehar Chand Mahajan, Hon'ble Justices B. Jagannadhadas, Ghulam Hasan, Natwarlal H. Bhagwati, T.L. Venkatarama Aiyar, B.K. Mukherjea, Sudhi Ranjan Das, Vivian Bose.

bench wanted a clear picture that whether the judgements given in these two cases denying any fundamental right of privacy was on the mark or not.

While the above mentioned cases stated that Indian Constitution does not guarantee right to privacy to its citizen, but in later cases like *Maneka Gandhi v. Union of India*¹⁰, *Govind v. State of Madhya Pradesh*¹¹ and *R. Rajgopal v. State of Tamil Nadu*¹², the Supreme Court benches started giving right to privacy a constitutional protection. These conflicting decisions created confusions that whether right to privacy has constitutional efficacy or not.

After this, the *Puttaswamy case* got divided into two parts.

- Validity of Aadhaar Card
- If right to privacy is fundamental or not

A Constitution bench of 5 judges¹³ was set up which modified the order dated 11th August 2015 passed by a 3 Judges bench¹⁴. The 5 Judges Bench after considering the matter as to the recognition of right to privacy as fundamental right referred the same to a 9 Judges Bench for an authoritative resolution of the dispute.¹⁵ The bench came up with the decision that the judgements given under the *M.P Sharma case* and *Kharak Singh case* were inaccurate and the foundation of right to privacy could be seen under *Article 14*, *Article 19*, *Article 20*, *Article 21* and *Article 25* of the Constitution of India. Opposing this decision the Attorney

⁹ AIR 1963 SC 1295 (6 Judges Bench) Hon'ble CJ. Bhuvneshwar P. Sinha, Hon'ble Justices N. Rajagopala Ayyangar, Syed Jaffer Imam, K. Subbarao, J.C. Shah, J.R. Mudholkar.

¹⁰ 1978 AIR 597 (7 Judges Bench) Hon'ble CJ M.H. Beg, Y.V. Chandrachud, V.R. Krishna Iyer, P.N. Bhagwati, N.L. Untwalia, S. Murtaza Fazal Ali and P.S Kailasam.

¹¹ 1975 AIR 1378 (3 Judges Bench) Hon'ble Justices Kuttayil Kurien Mathew, V.R. Krishnaiyer, P.K. Goswami

¹² 1995 AIR 264 (2 Judges Bench) , B.P. JEEVAN REDDY, S.C. SEN

¹³ Hon'ble Chief Justice H.L. Dattu and Hon'ble Justices M.Y. Eqbal, C. Nagappan, Arun Mishra and Amitava Roy

¹⁴ The order permitted the use of Aadhaar only for the PDS scheme and the LPG distribution scheme. Further, The Court said that if the Schemes like The Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS), National Social Assistance Programme (Old Age Pensions, Widow Pensions, Disability Pensions) Prime Minister's Jan Dhan Yojana (PMJDY) and Employees' Providend Fund Organisation (EPFO) are added to the P.D.S. Scheme and the L.P.G. Distribution Scheme as mentioned in the order dated 11.08.2015, it will not dilute the earlier order passed by this Court.

¹⁵ WP (C) 494/2012, (2017) 10 SCC 1 (Bench) Hon'ble CJ. Khehar and Hon'ble Justices, Jasti Chelameshwar, S.A Bobde, DY Chandrachud, Abdul Nazeer, R. Nariman, R.K. Agarwal, Abhay Manohar Sapre, And Sanjay Kishan Kaul

General of India said that there is no such concept of right to privacy in India and the Constitution makers deliberately didn't include such rights.

After hearing all the arguments, on 24th August 2017, the 9 Judges bench of Supreme Court unanimously came up with a landmark judgement overruling its own judgements in *M.P Sharma* and *Kharak Singh*, and declared the right to privacy a fundamental right under Article 21 of Part III of the Constitution. After this, on 26th September 2018 it was held that Aadhaar Act is also constitutionally valid and providing biometric data to the government is not the violation of any fundamental rights of the citizen.¹⁶

AAROGYA SETU AND ITS CONFLICT WITH PRIVACY

When you install any contact tracing App in your mobile, it asks you for some details regarding you and connects to your Bluetooth system of your device to work in accordance with it. This is exactly what the Aarogya Setu app does. Although the benefits of the app are clear, it is equally essential to protect the right to privacy of the users.

However, the working of the app is slightly unlike. On installing this app, the user needs to provide his name, gender, age, profession, travel history and telephone number. After this, the app will try to access the user's Bluetooth and location data. On acquiring all the details, the data gets saved in a centre based server. The users are required to keep their Bluetooth and location data switched on all the time because this app is designed to keep track of the app users who came in contact with each other or in Bluetooth proximity of each other's device. When any person starts registering their covid-19 symptoms then it gets uploaded in these central server and not only this, the other users of this app will also get to know about the number of registered users who are being infected nearby in their Bluetooth proximity and provide an approximate location of the user through their location data as well.

Conflicts:

¹⁶ (2019) 1 SCC 1 (5 Judges Bench) Hon'ble CJ. D. Misra, Hon'ble Justices D.Y. Chandrachud, A Bhushan, AM Khanwilkar, A Sikri. Declared that the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 was valid and not violative of the fundamental right to privacy. The Court also held that Section 7 was the core provision of the Aadhaar Act and since it satisfied the condition of Article 110 of the Constitution, the Aadhaar Act was validly passed as Money Bill.

- 1) The critics who opposed this step of the government regarding the quick releasing of the Aarogya Setu app pointing over its illegal and unlawful nature towards the fundamental right of right to privacy in the country came up with several arguments. The foremost of them are the working of the app and its policies. It has been argued that on installing, the app acquires admin access through the Bluetooth setting of the user. This is a risk for the users as the app could get access to more than the required data through the setting which is against the rights of the individuals because nobody is entitled to access anybody's personal data without their consent according to Article 21 of the constitution. It is against the right of privacy given to every individual through the Constitution of the country.
- 2) On May 1 2020, the Ministry of Home Affairs under the National Disaster Management Act, 2005 passed an order stating that it is mandatory for all the people of the containment zones and private and public employees to install the Aarogya Setu app and gave the responsibility, in case of employees, to the head of the organization and, in case of containment zones, to the local authorities of the area, to make sure that everybody has registered themselves in this app and ensure a 100% coverage of the Aarogya Setu app.¹⁷ This order aroused several conflicts. Firstly, the National Disaster Management Act, 2005 comes under the concurrent list¹⁸ which the government had used to take the measure of launching an app and thus the central government could take decisions and request the states to follow it. But when it comes to the personal or sensitive information of the individuals, any decision taken by the government could not force them to share it unless they have not consented according to the right of privacy given to the individuals under Article 21 of the Indian Constitution. The National Disaster Management Act, 2005 specifies no such circumstance or situation under which the fundamental rights given to the individuals could be infringed. Secondly, the employers of the private organizations assert that it is not possible for them to keep a check on all of their employees all the time that

¹⁷ Ministry of Home Affairs, Government of India Order No. 40-3/2020-DM-I(A) dated 01 May 2020, Available at: <https://www.mha.gov.in/sites/default/files/MHA%20Order%20Dt.%201.5.2020%20to%20extend%20Lockdown%20period%20for%202%20weeks%20w.e.f.%204.5.2020%20with%20new%20guidelines.pdf> (Accessed on 31.01.2021)

¹⁸ Seventh Schedule Entry 23 List III Social security and social insurance; employment and unemployment.

whether they are using the Aarogya Setu app or not and even if they don't then they cannot force them to do so. According to the Personal Data Protection Bill, 2019 both the public and private employees need to give their consent before getting their personal data being shared to their employers other than those required for processing salaries.¹⁹ Moreover, the installation of the app was made advisory rather than mandatory by a subsequent government notification.²⁰

- 3) According to the Economic Survey of 2018-19, the government is considering the citizens' data as something to be used for public good and tends to use some parts of them for revenue making by providing them to private companies to ease the pressure on government finances.²¹ This idea of the government has created a concern among the people assuming that the data being acquired by the government through the Aarogya Setu app could be used by the government for further purposes of their benefit.
- 4) The Aarogya Setu app lacked transparency to its users. At first the app was not open source which meant that any third party could not review its methods and policies which leads to a lot of criticism regarding it and it was said that the app which was launched by the government is not transparent in its working to the citizens of the country and thus restricting the researchers to detect its vulnerabilities. But later the government came up with a decision declaring the Aarogya Setu app will now be an open source.²²
- 5) Another concern was raised with the fact that the guidelines and directives provided by the government regarding the application lacked the sunset clause. That means no

¹⁹ Personal Data Protection Bill, 2019, Available at: https://www.prindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf (Accessed on: 30.01.2021)

²⁰ The Ministry of Home Affairs, Government of India Order No. 40-3/2020-DM-I(A) dated 17.05.2020, Available at: <https://www.medianama.com/wp-content/uploads/MHA-Order-Dt.-17.5.2020-on-extension-of-lockdown-till-31.5.2020-with-guidelines-on-lockdown-measures.pdf> (Accessed on: 28.01.2021)

²¹ Chapter 4, *Data Of the People, By the People, For the People*, Economic Survey 2018-19 Volume 1 Pg 78-97, Available at: <https://www.indiabudget.gov.in/budget2019-20/economicsurvey/doc/echapter.pdf> (Accessed on: 28.01.2021)

²² Aarogya Setu is now open source, Ministry of Electronics and Information Technology (MeitY), Government of India posted on 26 May 2020 PIB Delhi, Available at: <https://pib.gov.in/PressReleasePage.aspx?PRID=1626979> (Accessed on: 28.01.2021)

definite time interval was mentioned about the working of Aarogya Setu app and how long it would keep collecting the data and store them. This further created distress among the citizens regarding their fundamental right of right to privacy.

- 6) A petition was filed in Karnataka High Court by Anivar Aravind claiming that the citizens cannot be restrained from any service for not installing the Aarogya Setu app.²³, advocating the petition, Senior Advocate Colin Gonsalves says that this application is not backed by any law. In any such circumstance where the privacy of the citizens are being infringed by any directive of the government, needs a proper legislation and mere executive orders are not enough. Further, it was claimed that Aarogya Setu app fails the test of proportionality and purpose limitation test. There is no need for Bluetooth and location data to be collected and stored in the central server. A data controller cannot collect the data without a clear and informed consent of the user and give its access to third parties.²⁴
- 7) Another petition was filed in Kerala High Court by John Daniel, General Secretary, Thrissur District Congress Committee in which he appealed to the court that the step taken by the government by launching the Aarogya Setu application is violating the fundamental rights of the citizens by collecting their information through the app and storing it in the cloud and there is a possibility of the data being misused.²⁵ The directives issued by the government has taken away the rights of the people to control their own personal information by releasing the guidelines that the private sector employers were compelled to ensure a 100% coverage of the app among their employees as per Section 58 of Disaster Management Act, 2005 leaving the employees in a situation where they were forced to share their data. Beside this the

²³ *Anivar A. Aravind v. Ministry of Home Affairs*, GM PIL WP (C) 7483 of 2020

²⁴ The High Court, on 25 January 2020, in its interim order declined to stay the Aarogya Setu app or use of data of the users already collected through the app while prima facie holding that there is “informed consent of the users” through the privacy policy” of the app regarding collection and manner of collection of information, use of information and retention while there is no informed consent of users for sharing of response data as provided in the protocol. However, the Court restrained the Central government and the National Informatics Centre (NOC) from sharing the data collected through the app with other government authorities and agencies as per the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 till further orders. See also, The Hindu dated 25 January 2021, Available at: <https://www.thehindu.com/news/national/karnataka/karnataka-hc-declines-to-stay-use-of-aarogya-setu-app/article33657589.ece> (Accessed on: 28.01.2021)

²⁵ *John Daniel v. Union of India & Anr* Writ Petition presented on 05 May 2020 Kerala HC

petitioner mentioned that, it was not specified in the guidelines released by the government that which department or ministry would be the one controlling the authority of accessing the data, questioning the transparency of the application and hence concluding that the guidelines and directives of the government regarding the Aarogya Setu app are completely unconstitutional.²⁶

THE AAROGYA SETU DATA ACCESS AND KNOWLEDGE SHARING PROTOCOL, 2020

After many such conflicts and questions regarding the sudden releasing of the Aarogya Setu app, on 11th May, 2020 a notification was issued by Empowered Group on Technology and Data Managements²⁷ under the Disaster Management Act, 2005²⁸ giving a clarity regarding the working of the app, its policies, its data accessibility and many such information for which there has been a lot of confusion and conflict in the country since the launch of the app which led to a lot of criticism against the policies, directives and guidelines of the central government regarding it. This notification was a protocol²⁹ regarding the policies of the Aarogya Setu app and the directives of the government, acting as a legal defence to the App.

Rationale- The protocol begins with explaining the reason behind the launching of the app and its need to do so. With the increasing number of COVID-19 cases in the country, the central government issued some guidelines that are required to be followed by both the central as well as the state governments to take precautionary measures for those who are not

²⁶ *Ibid.*, Available at: <https://www.medianama.com/wp-content/uploads/John-Daniel-v.-UOI-Represented-Arogya-Setu-Writ.pdf> (Accessed on: 29.01.2021)

²⁷ Ministry of Home Affairs, Government of India Order No. 40-3/2020-DM-I(A) dated 29 March 2020 'Constitution of Empowered Group under the Disaster Management Act, 2005', Available at: <https://ndmindia.mha.gov.in/images/gallery/MHA%20Order%20on%20Constitution%20of%20Empowered%20Groups%20under%20the%20Disaster%20Management%20Act%202005-compressed.pdf> (Accessed on: 26.01.2021)

²⁸ Notification of Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 in the light of Covid-19 pandemic, Ministry of Electronics and Information Technology (MeitY), Government of India Order No. 2(10)/2020-CLeS dated 11 May 2020 https://www.meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf (Accessed on: 26.01.2021)

²⁹ Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020, Available at: <https://aarogyasetu.gov.in/wp-content/uploads/2020/06/mygov-1000000000981057882.pdf> (Accessed on: 26.01.2021)

infected yet and for the treatment of the individuals who are affected. In order to ensure the implementation of such measures there is a need of sharing the required data and information among the central and the state governments. The main focus should lie with protecting the health of the people in the country and in this concern a '*syndromic mapping and contact tracing*' of those who are being infected are urgently required to find those infected individuals and provide them with a proper treatment and make those individuals aware who are at risk. For this purpose Aarogya Setu app is being launched in the country to collect the required data of the individuals in this regard.

Process & Principle - specified that the purpose and the reason of collecting the data of the individuals through the Aarogya Setu app should be mentioned in the privacy policy of the app and only required data pertaining to the purposes mentioned should be collected and should be formulated and implemented for such purposes only. Contact and location data that are being collected should remain on the device on which the Aarogya Setu app has been installed and could only get uploaded on the central server for the formulation and implementation of the required purposes relating to the health of the individuals. The protocol has come up with a 'sunset clause' stating that it is in operation for 6 months from the date of its issuance and after that it will cease to exist, '*unless specifically extended by the Empowered Group on account of the continuation of the COVID-19 pandemic in India*'.³⁰ This aligns with the retention of the individual's data i.e., contact, location, self-assessment, not beyond 180 days from the date on which it is collected and to be deleted permanently. The demographic data of an individual could be retained in case of the protocol to be in force, but in the case of the user requests the deletion of the data it should get deleted after 30 days of such request being made. The data should be stored securely and should only be used in accordance with the protocol.

³⁰ Sunset Clause: The Empowered Group shall review this Protocol after a period of 6 months from the date of this notification or may do so, at such earlier time as it deems fit. Unless specifically extended by the Empowered Group on account of the continuation of the COVID-19 pandemic in India, this Protocol shall be in force for 6 months from the date on which it is issued. Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020, Available at: <https://aarogyasetu.gov.in/wp-content/uploads/2020/06/mygov-100000000981057882.pdf> (Accessed on: 26.01.2021). Notification of Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 in the light of Covid-19 pandemic, Ministry of Electronics and Information Technology (MeitY), Government of India Order No. 2(10)/2020-CLeS dated 10 November 2020 https://www.meity.gov.in/writereaddata/files/Order_Aarogya_Setu10112020.pdf (Accessed on: 26.01.2021)

The data of the individuals could be shared with the Ministry of Health and Family Welfare, Government of India, Departments of Health of the State/Union Territory Governments/ local governments or other such institutions of the government in a '*de-identified form*' where these data are strictly needed for the implementation of the mentioned purposes. Here, a randomly generated id is being placed, in place of the personal information of the individual. Apart from this, a list is to be maintained of the agencies and the institutions with whom such data are being shared, the timing at which the data sharing was initiated, the category of data that is being shared and the purpose for which the data is being shared.

Further, these data could be made available to Indian universities and research institutions registered in India for research purposes as well. But there is a condition to it, mentioned under this protocol. The data would go under a series of '*hard anonymisation*' through which the identity of the individuals would not get disclosed. Any institution or university seeking access to the data need to file a request and the request would be accepted only if such access is sought for the purposes of statistical, epidemiological, scientific or any other form of academic research or such purposes should be in concern with the health reasons mentioned under this protocol. The research institution and university should not, whether knowingly or unknowingly re-identify the individuals through the provided data and if any such action is being made then any right granted to them under this protocol would be terminated and they would be liable to penalties under the applicable law in force, at that time. Further these anonymised data could be shared by the research institutions or universities to another institutions or universities registered in India only for the purpose for which it has been granted approval and not otherwise.

As per the protocol any violation of these directions may lead to penalties as per section 51 to 60 of the Disaster Management Act, 2005 and other legal provisions as may be applicable.

CONCLUSION

Before *Puttaswamy case*³¹, there was no substantial precedent guaranteeing right to privacy in India. With the welcome developments in the *Puttaswamy case* the Supreme Court of India in 2017, gave right to privacy a fundamental value by recognizing it under Article 21 of Indian Constitution guaranteeing that every individual in India would enjoy their fundamental

³¹ Supra note 5

right of privacy and the violation of which will amount to infringement of the right to life and personal liberty guaranteed under the Constitution.

As the coronavirus outbreak reached its peak in India in 2020, it became necessary for the government to come up with an instant measure to handle the health emergency. In view of this, the government launched a contact tracing app named Aarogya Setu for collecting the information of those who were infected to provide them with proper treatment and take precautionary measures for those who are at risks. But soon after its launch, the Central government found itself in troubled waters. Major section of citizens started criticizing the sudden launching of the app, its policies and the directives of the government stating that the app is infringing the right to privacy of the individuals that has been recognized under Article 21 of the Indian Constitution.

Considering the public opposition for the app, the government decided to issue a notification on 11th May 2020, holding a protocol to answer all the questions of the citizens which had till now created confusion and distress in the country. This protocol clearly mentioned that the data of the individuals are safe in the central server and these data would be used in a fair and non-discriminatory manner. The protocol further gave the assurance that no extra information would be collected through the app from users' device without their consent and the data would be used only for health purposes and not as a tool of surveillance once the pandemic is over. Another notification was also issued on 17th May, 2020 making Aarogya Setu rather advisory.

The concerns over data protection intensified in India following the government's stance on citizens' data in the Economic Survey of 2018-19. Although the protocol and government notifications addressed many public concerns, several concerns are yet to be addressed in respect of the Aarogya Setu app, its policies and government's directives. The absence of a parliamentary legislation and the authority of an executive to issue directions interfering with the fundamental right to privacy have been an area of strong debate among constitutional lawyers and advocates of human rights. Moreover, the absence of a strict sunset clause in the Protocol raises doubts. The Aarogya Setu app and the protocol while allow the users to de-register and thus withdraw consent, a concrete legal framework demanding erasure of collected personal data is absent. A provision for such legal framework is present in the Personal Data Protection Bill, 2019 but it has not yet been enacted as a law. Even though the decision to make Aarogya Setu open source and optional is praiseworthy, the transparency

and government's legal responsibility in case of breach of data still remains uncertain in the absence of a Personal Data Protection law. In view of these, the demand for the data protection law has amplified. The Personal Data Protection Bill, 2019 is currently being considered by the Joint Parliamentary Committee on Personal Data Protection Bill which is due to submit its report suggesting amendments by the second week of the Winter Session in 2021. Hopefully, 2021 will witness the transition of the Personal Data Protection Bill into an enacted law which will bring a statutory framework protecting the right to privacy in India.