Page 1902 - 1911 **DOI:** *http://doi.one/10.1732/IJLMH.25951*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 1

2021

Aarogya Setu: The Right to have Rights?

ARYAN PURI[1] AND SANYA RAWLANI[2]

ABSTRACT

With the Covid-19 crisis creating immense dismay, the government of India came up with an initiative of wellbeing and goodwill for its citizens- a Bluetooth based contact tracing application called the 'Aarogya Setu'. By the end of May 2020, a staggering 114 million people had not only registered, but also provided the application with sensitive and private information. Several lapses have been identified with regard to the security of this information. It further went on to breach several privacy protocols before mandating its use. One of the biggest problems was the lack of a transparent and verifiable framework with a chance of sensitive data being exposed. The risk was further increased by the fact that the application is not backed by a legislative aid, as directed by the Puttaswamy Judgement. The privacy policy of this application lacks a set protocol for the accessibility and shareability of the data or a predetermined penalty for the misuse of the data. Thus far the application has been sacrificing the right to privacy in favour of right to health. Here the courts should apply the rule of harmonious construction. The government has backed the legality of this application only with the Disaster Management Act, 2005. The authors seek to analyse and elucidate the flaws with the 'Aarogya Setu' application and provide viable solutions for the same.

I. INTRODUCTION

Privacy is not a liberty given to a few, but a right given to all. In today's age where technology controls most aspects of our lives, privacy has become a major concern. Not just for the elite who believe that they have something to lose, but also for the common folk who generally disregard the concerns of their own privacy. With the Covid-19 crisis creating immense dismay, the government of India tried to come up with a quick but viable solution for the problem. While Singapore has launched TraceTogether[3] and Australia has come out with COVIDSafe[4] for developing a contact tracing system, working towards a similar goal, the Indian government has launched a contact tracing application called 'Aarogya Setu'. The mobile application works on a Bluetooth based contact tracing model that ascertains the users'

[1] Author is a student at MIT - WPU, School of Law, India.
[2] Author is a student at MIT - WPU, School of Law, India.
[3] "TraceTogether." TraceTogether, 2020, www.tracetogether.gov.sg.
[4] "COVIDSafe App." Australian government Department of Health, 28 July 2020, www.health.gov.au/resources/ apps-and-tools/covidsafe-app.

 [ISSN 2581-5369]

live location and gives information about the mapping of likely hotspots and dissemination of relevant information about Covid-19.[5] Although the initiative taken by the government was intended to be a gesture towards the well-being of its citizenry, it was very ill-informed and has had several drawbacks, which included but were not limited to, the lack of a transparent verifiable framework, and the lack of a legislation or an ordinance that can legally make the use of the application mandatory.

A month after the launch of the application, over 94 million[6] people registered and by the end of May 2020 over 114 million people had provided the application with sensitive information including but not limited to their gender, mobile number, age and any pre-existing health conditions, if prevalent. In addition to that, they also gave the application permission to track their location. Most people who provided the application with their data were completely unaware of what the data will be used for, and whether the application has enough security systems in place to keep their data secure. The mobile application breached several privacy protocols even before the government mandated its use. Even though the application has been made mandatory in the times of dire need, it still cannot be given the complete freedom to use the private information of individuals at the government's leisure. This application needs to have a transparent and a verifiable framework so that it becomes clear that it is not a surveillance application in its essence. It is pertinent to note, that in times like these where the legal system is vulnerable, it becomes more important for the government to harmoniously protect the fundamental rights of the individuals as their infringement could have long term effects consequently. One of the major issues that Aarogya Setu faced is the lack of legislation backing the use of this application. It does not have an Act, passed by the parliament, or even an ordinance passed by the President[7] that provides it, its legality. In the case of Justice *K.S. Puttaswamy (Retd.) v. Union of India*[8], if the centre seeks to curtail the right to privacy of an individual, they must do so under the canopy of a legislation that has a legitimate purpose, which clearly is not the case here. The judgement also lays down three key tests, to be used for testing the legitimacy of a law that seeks to abridge the right to privacy: Necessity, Legality, and Proportionality. Since India doesn't have its own data protection Laws, the government must stick to the guidelines provided in the Puttaswamy judgement so that they can strike a balance between maintaining public health and simultaneously not abridging the fundamental

[5] Government of India. Ministry of Electronics and Information Technology. Aarogya Setu is now open source. Ministry of Electronics and Information Technology, 26 May 2020

[6]Sankalp Phartiyal, *Indian court seeks government reply over challenge to mandatory coronavirus app* (May 8, 2020, 5:05 PM) https://in.reuters.com/article/idINKBN22K1GG.

[7]INDIA CONST. art. 123.

[8]Justice K. S. Puttaswamy and another v Union of India and others. (2017) 10 SCC 1 (India).

rights of any individuals. The initiative taken by the government is a commendable one but to ensure its success, enough measures should be taken for the framework of the application to be within the bounds of the Privacy judgement.

II. LACK OF LEGISLATION FOR MANDATORY IMPOSITION OF THE APPLICATION

"*Legislation is one of the most important instruments of government in organising society and protecting citizens. It determines amongst others the rights and responsibilities of individuals and authorities to whom the legislation applies.*"[9]

A major drawback which has invited much criticism was the absence of a transparent and a verifiable framework for the application. At the time of the launch, the government made the source code private, and did not give any independent auditors a chance to check the viability of the application.[10] Another major concern is that the privacy policy does not state the purpose of the collection of data and it is still silent as to the shareability of the data stored on the government servers. More importantly, since the Source Code was inaccessible, it became impossible for the people to check if the encryption systems used for the application are sufficient. As Justice Madan B. Lokur explained,

"*The balance between transparency and confidentiality is very delicate and if some sensitive information about a particular person is made public, it can have a far-reaching impact on his/her reputation and dignity*."[11]

It is pertinent to note here that the government has since then made the source code public. On the 5th of May 2020, a French ethical hacker who goes by the twitter Handle 'Elliot Alderson', tweeted asking the India government to get in touch with him so that he could point out the flaws in the Aarogya Setu app.[12] The government deftly denies having any security breaches through their twitter handle, "*We are continuously testing and upgrading our systems. Team Aarogya Setu assures everyone that no data or security breach has been identified*," by a tweet that gives a point-by-point clarification on the red flags raised by the hacker.[13] The hacker's real name is 'Robert Baptiste', he was the person responsible for finding out the privacy flaws in the official 'Narendra Modi android application'[14]. Keeping that in mind, it is pertinent to

[9] De Jager, H 2000, 'Importance of legislation', Auditing SA, p. 3-4. [http://www.saiga.co.za/publications-auditingsa.htm]
[10] Andrew Clarance, *Aarogya Setu: Why India's Covid-19 contact tracing app is controversial* (May 14, 2020), https://www.bbc.com/news/world-asia-india-52659520
[11]ABC v. The State (NCT of Delhi), 2015 SCC Online SC 609 (India).
[12] Krishnan Revathi, *Govt 'thanks' French Ethical Hacker Who Flagged Aarogya Setu, but Dismisses Security Concern* (May 6, 202012:20 PM), theprint.in/india/govt-thanks-french-ethical-hacker-who-flagged-aarogya-setu-but-dismisses-security-concern/415348.
[13] Aarogya Setu (@SetuAarogya), Twitter (May 6, 2020, 1:03 AM)https://twitter.com/SetuAarogya/statu s/1257755315614801921?s=20.
[14] Elliot Alderson (@fs0c131y), Twitter (Mar 24, 2018, 1:04 AM) https://twitter.com/fs0c131y/statu s/977267255309463554.

 [ISSN 2581-5369]

note that he exposed the vulnerability of the application on twitter, a public platform on which he has a following of over 226,000 people. A number far larger than that saw the tweet, who is to say that no one used the vulnerability of the application to their benefit?

Keeping the privacy concerns and the fact that the application is not backed by legislation aside, the application fails to achieve its purpose: curbing the spread of the Novel Coronavirus. It failed because it generated a plethora of false positives, and the application once downloaded relied on a self-assessment test in which people are supposed to truthfully provide information about their travel history and if they have any symptoms. Some hospitality and food delivery services, like Zomato, Swiggy and Urban Company have also mandated the use of the application for their employees.[15] With the current drop in job opportunities, it is highly possible that an employee may falsify the voluntary self-assessment test, so as to avoid losing his job. There have been various instances where the government authorities have mandated the use of the Aarogya Setu app. In the guidelines given by the Ministry of Home Affairs on the 1st May, 2020, Section 3(iii) read that "*The local authorities shall ensure 100% coverage of Aarogya Setu application among the residents of containment zones.*"[16]. Even in the Privacy policy of the App the government absolves itself from all liabilities in case there is a data leak. This imposition does not have a legal standing and the only thing that it will do is open the government to a plethora of legal liabilities.

Aarogya Setu was also made mandatory for the employees of private as well as public sector offices by the order passed on the 1st of May. Hundred percent installation of this application within the containment zones was also mandated. Failure to comply with the guidelines would attract penal action under Sections 51 to 60 of the Disaster Management Act, 2005 and under Section 188 of the Indian Penal Code, 1860 will be taken[17]. Under section 51(b) of the Disaster and Management Act, 2005, if a person refuses to comply with the orders given by the authorities, the person shall be imprisoned for a period that may extend to one year, or with fine, or both and under Section 188 of the Indian Penal Code, 1860, maximum punishment can be extended up to one year imprisonment, or with a fine of rupees one thousand, or both.

[15]Alnoor Peermohamed& Aditi Shrivastava, *Some Startups Mandate AarogyaSetu, Others Remain Wary* (Apr. 24, 2020, 01:27 PM), economictimes.indiatimes.com/small-biz/startups/newsbuzz/some-startups-mandate-aarogya-setu-others-remain-wary/articleshow/75339322.cms? from=mdr.

[16] Ministry of home affairs, government of India. *New guidelines on the measures to be taken by ministries/ departments of the government of India state /UT governments and state/ UT authorities for containment of covid-19 in the country for the extended period of National lock down for a further period of two weeks with effect from 4 May 2020* (May 1 2020) https://prsindia.org/files/covid19/notifications/IND_Extension_Lockdown_May_1.pdf

[17]Ministry of Home Affairs, Government of India. Guidelines on the measures to be taken by ministries/ departments of Government of India, State/ UT governments and state/ UT Authorities for containment of COVID 19 in the country upto 31st May, 2020. (Last visited: Oct 25, 2020), https://mofpi.nic.in/sites/default/files/mha_order_dt._17.5.2020_on_extension_of_lockdown_till_31.5.2020_with_guidelines_on_lockdown_measures.pdf

 [ISSN 2581-5369]

The government is using Section 10(2)(l) of the Disaster Management Act, 2005 to justify the mandatory imposition of the application. The said section allows the government to formulate guidelines on any subject of law in response to any threatening disaster situation or disaster. It is hard to derive its legality from this provision as, according to entry number ninety-seven of list one of the Seventh Schedule of the Constitution of India, a legislation on the use and collection of data would be covered only by the Union list, thus, only the Parliament has the power to legislate on this subject matter. The National Executive Committee set up under Disaster Management Act, that issued the May 1, 2020 Guidelines directing the installation of Aarogya Setu, is not a statutory body as it is not established by an act of the parliament , and it is also pertinent to note that in the present case, there is no evidence of any specific parliamentary approval for directing the mandatory installation of the Aarogya Setu app. The order given by the government is predominantly ambiguous as to how these guidelines will be imposed on people who do not own smartphones. Only the guidelines from the Ministry of Home Affairs are not sufficient legal backing. Justice BN Srikrishna, the former judge who headed the committee of experts that made the first draft of the Personal Data Protection Bill, while talking about the legality of the mandatory imposition of the application in an interview said, "*Under what law do you mandate it on anyone? So far it is not backed by any law.*" He went to the extent of calling the mandatory use of this application "*Utterly Illegal*".[18]

The Aarogya Setu Data Access and Knowledge Sharing protocol was issued on the 11th May, 2020, and it was issued by way of an order by the Empowered Group on Technology and Data Management. It set principles for the data collection and the processing of data, but this is not enough to manifest legality of the mandatory use of the application. As there is no legislation for mandating the downloading of this application, the foreground subject here must be the health of the citizens and their fundamental rights. Non-compliance with the mandatory installation of this application comes with penal provisions which not only hampers the liberty of the citizens but also cues coercion and compulsion, eliminating fraternity and trust.

On 3rd May, 2020, the Gautam Buddh Nagar District police in Uttar Pradesh passed a prohibitory order. In addition to the order, they also directed that the non-installation of the Aarogya Setu App will be treated as a violation of the order and attract criminal penalties. This imposition was challenged on three main grounds. Firstly, it is contrary to law because positive obligations cannot be imposed on a person to do certain acts under Section 144 of the Code of Criminal Procedure, 1973. It can only direct them to 'abstain from a certain act'. The Calcutta

[18]Daksha Fellowship, Data Governance & Democratic Ethos - Rahul Matthan, Justice BN Srikrishna with Dr.Ananth Padmanabhan, YouTube (May 11, 2020), https://youtu.be/WN3doA7W9Uk.

 [ISSN 2581-5369]

High Court noted that, "*The very reason why the section uses the language 'abstain from a certain act' is just because it is not intended to empower magistrates to make positive orders requiring people to do particular things.*"[19] Secondly, it is contrary to fact as already mentioned earlier. Hundred percent installation of this application was made mandatory within the containment zones by the Ministry of Home Affairs. As per the notifications by the State Government, the entire District Gautam Buddha Nagar was never declared a 'Containment Zone', but only a 'Red Zone'. On 20th May 2020, the Noida Authorities dropped the reference of Aarogya Setu and did not mention it at all in any subsequent orders. A number of cases have been filed against the various aspects of the application in the Hon'ble High Courts of and Kerala[20] and various other States. This goes on to prove that the order to mandate the use of this application falls foul of the law.

III. REASONS FOR THE FAILURE OF APPLICATION

The privacy policy and the terms of service of the application are completely silent as to which government authority has the access to the data and till what time will the authority have access to it. Information like live location is essentially very intrusive in nature and unless anonymised, sharing of any such data without, letting the individual know as to whom the data will do to is a breach of their Privacy. The users' data must be kept protected, and they should be informed as to who will have access to the data at the time of registering for the application, further, in case there is a change in the future, concerning the recipients of the data, the change should not be made without the consent of the users who have already registered.

When addressing the issue of access to the data, we also need to consider the question of the protocol established as to the shareability of data with the health professionals. The privacy policy of the application does not provide for a full-fledged protocol of the shareability of the data, and the user has no control over the same. In case a 'data set' is to be shared with a healthcare professional, clear guidelines should be established mentioning the penalty for the misuse of the data by the health professional who has access to it. In the Puttaswamy judgement, Justice Chandrachud, referred to the 'Stanford Encyclopaedia of Philosophy' and held, "*Behavioural privacy postulates that even when access is granted to others, the individual is entitled to control the extent of access and preserve to herself a measure of freedom from unwanted intrusion*".[21] Since the application does not use temporary IDs, but uses a unique

[19]B. N. Sasmal v Emperor, AIR 1931 CAL 263, (India).
[20] *John Daniel v. Union of India and ors.* (last visited Sept. 17, 2020) http://highcourtofkerala.nic.in/covid_files/WPC980620208052020.pdf.
[21]Cohen,J, "*What Privacy Is For*", HAR. LAW. REV.,2013, Vol. 126, at 1904.

permanent digital ID (DiD) to which a user's data is attached, any person who gets access to the DiD will essentially have access to their entire life. The right to give access of this data to anyone must still remain with the user.

The privacy policy and terms of use of the application do not indicate when the personal and anonymised data stored on the government servers will be purged and that it will not be used for any other purpose. There is no assurance that the data stored on the government servers will be deleted Post Covid-19 outbreak. Terms of limitation should be outlined through a legal framework to prevent the abuse of civil rights and liberties guaranteed under the Constitution of India. In the absence of a sunset clause, gathering of data can be carried out in relaxed terms and conditions. Destruction of servers and systems created as an output of the Aarogya Setu application cannot be backed by a sunset clause. This goes on to prove that the Aarogya Setu app can be used as a surveillance tool in the future by the government abridging the right to privacy of anyone who has downloaded the application.

The authors accept that the government has now scaled down the mandatory imposition of the application and has accepted their mistakes, although not publicly. Amitabh Kant, CEO of the government think-tank NITI Aayog, told a news conference "*Transparency, privacy and security have been the core design principles of Aarogya Setu since its inception. And opening the source code up to the developer community signifies the government of India's continuing commitment to these principles.*".[22] The citizens of the country would want to believe in what the government is saying, but until now all the evidence that has come forth says the contrary. The mere fact that they tried to impose something on the people that clearly violated their fundamental right to privacy, and tried to benefit from the fact that we do not have a Law for data privacy is inacceptable and outrageous.

IV. COEXISTENCE OF RIGHT TO HEALTH AND RIGHT TO PRIVACY UNDER ARTICLE 21

There is a very significant need to harmonise right to health and right to privacy under Article 21 of the Indian Constitution. In the present circumstances, these two rights are seen to be conflicting in nature. The rule of harmonious construction needs to be adopted when two or more parts of the fundamental rights are standing in conflict. This rule is carried out to ensure that each of the two conflicting parts have separate effects and neither is made redundant or nullified.[23] In the case of *Sultana Begum v. Premchand Jain*[24], it was observed that while

[22] Sankalp Phartiyal, *India Makes Source Code of Contact-Tracing App Public*, (27 May 2020, 7:10 AM) https://in.reuters.com/article/idINL4N2D83I6.
[23] Narayan Gopal Mhatre V. Shankar Sitaram Sontakke, 1967 SCC OnLine Bom 48, (India).
[24] Sultana Begum v. Premchand Jain, 1997 (1) SCC, page 373 (India).

interpreting two inconsistent provisions of an Act, the Courts should construe them so as to harmonise them so that the purpose of the Act may be given effect to. It was observed further that the statute had to be read as a whole to find out the real intention of the legislature.

There are a few principles that have been laid down by the Supreme Court of India with regards to harmonious construction. One of the principles states that the provision of one section should not be used to defeat the provision contained in another[25]. The Government, while maintaining the health of its citizens as their fundamental right, cannot defeat the purpose of protecting their personal data which is also their fundamental right. A balance needs to be considered between the two. Another principle states that to harmonise is not to destroy any statutory provision or to render it fruitless. Right to privacy should not be destroyed by the government just to preserve the right to health.

In order to harmonise right to health and right to privacy, the government should limit themselves to the extent necessary and proportional to ensure that the outcome of both the conflicting rights are achieved.

V. THE NEED FOR A DATA PROTECTION LAW

The Puttaswamy judgement, in 2017, declared the 'Right to Privacy' to be a fundamental right. Following which a committee headed by Justice B.N. Srikrishna was formed. It conducted various hearings all over the country and submitted a report in July 2018, wherein they mentioned the need to formulate a data privacy legislation. "*The issue of data protection is important both intrinsically and instrumentally. Intrinsically, a regime for data protection is synonymous with protection of informational privacy*."[26] The Puttaswamy judgement itself directed the centre to make a law for the protection of data. Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. "*We commend the Union government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state.*" The Information Technology Act, 2000, has certain provisions that intend to protect the private information of individuals, but the said provisions are not enough to safeguard the sensitive private information, as 'Medical records' which are treated as sensitive personal information within Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.[27] Moreover,

[25] CIT v. Hindustan Bulk Carriers, (2003) 3 SCC 57 (India).
[26] JUSTICE B.N. SRIKRISHNA ET AL., SRIKRISHNA COMMITTEE REPORT (2018).
[27] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules,

Information Technology rules were a novel attempt at data protection and the Information Technology Act, 2000, applies only to companies, not to the government.

In this growing age of technology, for effective management of any unwarranted situations, we need to take desperate measures which will aid us in resolving any similar situations, the nation needs a data protection law to come into the picture as soon as possible although the Personal Data Protection Bill, 2019[28] was introduced in the Lok Sabha on December 11, 2019, but hasn't been passed as of yet. The preamble of the Bill states that its purpose is to, "*To provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed.*" The 2019 Bill seeks to protect the privacy of individuals with respect to their personal data, create a framework for processing such personal data, and establish a Data Protection Authority for these purposes.[29] The Bill lays out certain obligations for the data fiduciaries who decides the means and purposes of data processing. The processing of personal data is subject to certain purpose, collection and storage limitations. Certain transparent and accountability measures are to be taken by the data fiduciaries. Other than the tasks performed by the data fiduciaries, appropriate and necessary measures are taken by the Data Protection Authority to ensure that the interests of the individuals are protected and personal data is prevented from being misused. Data Protection Authority comprises members with expertise and the individuals who are not satisfied with the grievance redressal by the data fiduciaries can approach the Authority. The Bill categorises certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectoral regulator, most of which is collected by the Aarogya Setu application. Further, processing of personal data by the government, companies incorporated in India, foreign companies dealing with personal data of individuals, is governed by the Bill. This is exactly what was required at this time, we needed a Law to regulate any authority that has access to the data, so as to avoid the misuse of data.

VI. CONCLUSION

The application lost all of its capacity to succeed as soon as it became illegally imposed on people. Even if we assume that the application was not launched as a surveillance mechanism

2011, Rule 3.

[28]Personal data Protection Bill, 2019, No. 373 of 2019 (India).

[29] https://www.prsindia.org/node/845995/chapters-at-a-glance

by the government, it tried to take advantage of the fear in the minds of the people. The application was still unable to achieve any of its objectives as it could not gather a wide enough user base in India. The government even started pushing other services like the option for donation to the 'PM Cares Fund', which itself is under a lot of debate, on the application. We are not of the opinion that the initiative was substandard but to make the initiative work, the execution could have been improved. India is a country where the smartphone penetration rate is not as high, and it is even lower among women. Generally, in India, among families that cannot afford more than one phone, it is usually the men in the house who have a phone. If the movement of individuals is restricted on the basis of having the application on a smartphone, the government will indirectly be taking away the right to move freely[30] from the women who do not own smartphones, and the mandatory imposition becomes derogatory to women. By doing this, the government is implying that the people who do not own smartphones, do not have the right to have rights. To combat the pandemic, governments across the globe have tried to make contact tracing applications, but only some of these applications have been successful. Most countries which have made such applications have elaborate data privacy laws in operation. The contact tracing applications made by Singapore, Australia and the United Kingdom, all run on Bluetooth technology, but are successful because most of them are transparent, and provide for a data destruction clause. TraceTogether also used dynamic IDs[31] and not Static IDs[32] like in Aarogya Setu, which are exuberantly less private in comparison. As static ID is more easily amenable to de-anonymization i.e. identifying the owner, in case someone else gets hold of the DID, because there is only a single layer of encryption. Encryption in this regard is necessary as the data collected by the application is not anonymised also, there is no data destruction policy as of yet. The Aarogya Setu application has now lost public confidence, and no matter what steps the government takes, there is no scope for it to become successful. All things considered, the data already saved by the government has to be protected and the government must include a 'Sunset Clause' declaring when the data will be deleted. The systems should be designed in a manner where it automatically stops processing of data and meta-data, and deletes both of it. The legal order should subsist only till the circumstances warrant it. At the end of the day the governments are not chosen to discriminate among our fundamental rights, but are chosen to create a balance and protect them.

*****

[30]INDIA CONST. art. 19, cl. 1(d).
[31]Gov.Sg,*Help Speed up Contact Tracing with TraceTogether*., (2020), www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether.
[32] *Aarogya Setu - Privacy Policy*, https://web.swaraksha.gov.in/ncv19/privacy/ (last visited Sept. 16, 2020).