Journal of Research Administration
Society of Research Administrators International

A CRITICAL STUDY OF CONTACT TRACING APPS IN INDIA VIS-À-VIS RIGHT TO PRIVACY

Dr. Payal Thaorey
Asst. Professor (Sr. Gr) & Head of the Department Post Graduate Teaching Department of Law, RTM Nagpur University, Nagpur, Maharashtra, India

Dr. Anjum Ajmeri Rabbani Ansari
Assistant Professor, Dr. D. Y. Patil Law college, Pimpri, Pune.

ABSTRACT

The quote "know more from less" has become possible in the digitalized world, by collecting the data of an individual for the sake of technology and digitization.

Data is becoming the most important unit for analyzing behavior, identifying preferences, and offering the most relevant product/service to the potential consumer. Furthermore, the intangible nature of data and its reusable productivity have allowed for its endless distribution, beyond the boundaries and worldwide. Traditional systems of collection of data, processing of data, analysis of that data and importantly protection of the data, for all these steps the available regulations governing the data control and access, is inadequate in light of this highly uncustomary change in the usage of data. Data is a raw form of information but the processing, organizing or structuring of the data so as to represent a given context, converts the data into information. When personal information of an individual is compromised, it would be infringement of the informational privacy of a person. Failure to address the invasion of informational privacy would not only violate the Fundamental Right of the person but it exposes the absence of significant Data Protection laws also. After the outbreak of COVID-19, the government of India launched a mobile app called Aarogya Setu. This app was launched with a good intention to seize the spread of the disease by ensuring the contact tracing of an infected person. For serving the purpose, the app collects personal data of a person for tracing the covid contacts. But an important concern is that whether the Aarogya Setu App complies with the condition of anonymity recognized by the Supreme Court, in the Puttaswamy judgment? Unfortunately, the answer is 'No'. Hence, it can be said that in the absence of appropriate laws, the compulsion of using the App might have violated the Right to Privacy of the people who are using the app "**Aarogya Setu - a bridge to health"**. Thus, in this research paper a detailed analysis will be carried out about the working of the Aarogya Setu app and how it violates the informational privacy of its users. In furtherance of the paper, researchers will also discuss the legal issues and concerns relating to this App.

I. INTRODUCTION

The Fourth industrial revolution is transforming the intrinsic value and usefulness of data, as it is very unprecedented and unpredicted, resulting in worldwide convergence of digital, physical, and biological technology. As more and more new technologies become digital, the volume of data processed grows, with the frequency approaching that of almost like surveillance. The data collection and processing are driven by the demand for the newer technologies and for fulfilling the requirement of globalization. The increasing interaction between the communities from different parts of the world has a considerable significance in the great leap taken by technological developments. The narrowing of distance between places and people resulted in frequent travelling of people from one part of the world to the other. Such interactions result in many good things but sometimes, these may lead to spreading of some deadly diseases too. The virus that causes serious acute respiratory syndrome (SARSCoV-2)[1] is one such instance. By the end of year 2019, Wuhan, a city in China recorded some cases of this disease and within one month, the disease got spread to almost the whole world and thus was declared as Pandemic by the WHO [2]. This pandemic has made a devastating effect on the world and has killed more than five million among over one hundred million infected people.[3]

Any such unprecedented and uncontrollable outbreak necessitates excessively large number of measures to check the stretch of the sickness. In the case of corona virus, the government and the health monitoring agencies followed the other countries and adopted measures like thermal scanning, contact tracing etc. However, probably because of the obvious priority given to the control of spread, the impact of such measures on the civil rights and liberties of the citizens could not be appropriately studied.

Hence, it is very important to ensure that sensitive information like personal health data of the subjects should not reach any one unauthorized or potential misuser.

However, before the vaccine can be administered to all, the widespread use of cellphones, the Internet, and data collection are the methods adopted to improve the efficacy of a key tool viz. Digital Contact Tracing which has a potential of slowing down the spread of the disease. The data collected by this tool aids the public health authorities in drafting and implementing appropriate policies.

II. CONCEPT OF DIGITAL CONTACT TRACING

---

[1] *Chih-Cheng Lai 1, Tzu-Ping Shih 2, Wen-Chien Ko 3, Hung-Jen Tang 4, Po-Ren Hsueh 5Severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) and coronavirus disease-2019 (COVID-19): The epidemic and the challenges, International Journal Antimicrobial Agents, 55(3), 1.*

[2] *Anastasios Apostolos, Konstantinos Apostolos, Tracking Applications: A Factor of Mithridatism of Personal Data and Privacy in the Post-COVID-19 Era, Society for Disaster Medicine and Public Health, Inc, (May 22, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7303466/*

[3] *Coronavirus Death Toll, Worldometer (Jan 02, 2022), https://www.worldometers.info/coronavirus/coronavirus-death-toll/*

The government has launched multiple apps which can be used by the people for different services in India. Many of these apps eased down some of the hardships during the shutdown implemented to control the widening of corona virus. Six apps are recommended by the government's Digital India Twitter account for users to acquire and utilise to help throughout the shutdown, namely, BHIM UPI, UMANG, Ayush Sanjivan, Jan Aushadhi Sugam, E-Gram Swaraj and Aarogya Setu App.

The primary UPI app for internet transactions is called BHIM [4]. In actuality, it's the simplest and fastest method of transferring funds electronically. More than 600 services offered by the government, including Aadhaar, PAN, passports, driving licences, and more, are available via the UMANG app [5]. It provides operations for both the state and federal governments[6]. The Ministry of Ayush and MeiTY created the Ayush Sanjivani App[7], which is suitable for analysing population behaviour. The data obtained from this app aids in understanding the measures and steps which public has adopted as immunity boosters. While Aarogya Setu gained the highest popularity in terms of number of downloads and its usage. This is basically a contact tracing app. The software alerts customers whenever they come into contact with someone who has been affected by deadly viruses by using GPS and Bluetooth connections. The concept of contact tracing is not new[8] and similar operations were carried out in the past during such pandemic situations. The trend continues in the situation of COVID-19 as well. The significant difference between the past contact tracing and the present one may be the utilization of virtual contact tracing applications. This helped in slowing down the spreading of deadly virus, with the mobility and accessibility of Internet-connected cell phones.

In the center of the virus occurrence, nations all over the world have proposed contact tracing applications as a way to seamlessly navigate the current issue. India is the second largest country hit by the COVID-19. Despite the fact that privacy experts and legal professionals have voiced dissatisfaction with theabove-mentioned applications of contact tracing owing to potentiality of breach of right to privacies of the users, it appears that these apps have become the most discussed topics for the season. In this situation, India too has developed its own contact tracing app named, Aarogya Setu 'bridge to health'.

---

[4] National Payment Corporation of India, Government of India, https://www.bhimupi.org.in/

[5] Ministry of Electronics and Information Technology (MeitY) and National e-Governance Division (NeGD), Government of India, https://web.umang.gov.in/landing/

[6] HT Tech, Aarogya Setu to BHIM UPI: Govt suggests 6 apps to make life easier during lockdown, Hindustan Times, (May 20, 2020), https://tech.hindustantimes.com/tech/news/aarogya-setu-to-bhim-upi-govt-suggests-6-apps-to-make-life-easier-during-lockdown-71589946706028.html

[7] Ministry of Ayush, Government of India, https://ayushnext.ayush.gov.in/detail/news/ayush-minister-launches-accr-portal-and-3rd-version-of-ayush-sanjivani-app

[8] "Plague crosses, which were placed on buildings occupied by the victims of plague, served as a rudimentary mechanism for minimizing the risk of contagion in the seventeenth and eighteenth centuries. During the AIDS crisis in the 1980s, public health officials debated the balance between contact tracing and discrimination against the LGBTQ community." Christopher S. Yoo and Apratim Vidyarthi, Privacy in the Age of Contact Tracing: An Analysis of Contact Tracing Apps in Different Statutory and Disease Frameworks, 2.

However, like other Internet-connected apps and gadgets, this most recent generation of contact tracing Apps elevates issues regarding data confidentiality. Contact tracing applications must gather some sort of locality information and examination outcome information (Sensitive personal data) and uploading it into the government server in order to fulfill their objective of tracing the transmission of a disease. Both location data [9] and self-assessment data are intimate and confidential, providing precise details about where data subjects pass through, who they connect with and what feasible places may have sources them for testing positive[10].

So many questions have arisen linked to the usage of this app. These questions must be answered for fear-free use of the App. This research will focus on addressing the research questions mentioned below:

1) Are there enough guidelines for App developers to combine the necessity of safeguarding privacy with the requirement to fulfill vital society wellbeing responsibilities by means of development?

2) Are such policies or protocols released by government possess the capability of dealing with the rapidly varying requirements of specific society wellbeing situation?

3) And how does the App strike a compromise between the demands and rights about their personal data and the public's healthcare requirement of stopping the transmission of a fatal illness?

4) How legislation lacks for mandatory imposition of the Aarogya Setu? And what are the issues and concerns arise relating to lack of legislation?

Answer of these questions would be helpful to decide deficiency or efficiency of Aarogya Setu App to combat with the Pandemic corona virus in parallel to guard the Fundamental Rights to confidentiality of the person because failure to address this invasion of privacy would not only stifle these technologies' transformative potential, but will also exacerbate power disparities and global inequities [11].

III. OBJECT OF THE DIGITAL TRACING APP: AAROGYA SETU

Statistics collection is regarded as an essential task for many governments and organizations throughout the world. It is indicated that in order to create a sound policy and have it implemented effectively, the government must have a comprehensive understanding of the situation. In India

---

[9] Location Data means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communication service. UK's Directive 2002/58/EC

[10] Self-assessment data means the responses provided by that individual to the self-assessment test administered within the Aarogya Setu mobile application. Ministry of Electronics and Information Technology, Notification of the Aarogya Setu data access and knowledge sharing protocol, 2020 in light of the COVID-19 pandemic, (May 11, 2020), Government of India, https://www.meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf

[11] Ankit Kapoor, Operationalizing Privacy by Design: An Indian illustration, 1, Operationalizing Privacy by Design: An Indian illustration by Ankit Kapoor: SSRN

Covid Pandemic is not the first time the Government is collecting the data. After Independence we have legislations like Census Act, 1948[12] and Collection of Statistics Act, 2008 where the government has been collecting the data of persons which could fall under the category of definition of personal data under Data Protection Bill 2019. The Census Act gathers information on a variety of topics, including gender, age at previous birth anniversary, religion, identification of a scheduled caste or tribe, condition of impairment, distances and methods of transportation for the location of employment, and several more [13]. On the other hand, the federal, state, and local governments are authorised under the Collection of Statistics Act, 2008[14], to gather any sort of data, particularly personal information on people and families. The Collecting of Statistical Act, 2008, removes the restrictions of the Gathering of Statistical Act, 1953[15], while also expanding the purview of information collection. Following the rise of technology, the Aadhar Card [16] has begun collecting almost the same amount of information under the auspices of the Aadhaar ("Targeted Delivery of Financial and Other Subsidies, Benefits, and Services") Act, 2016. It gathers "personality data" about a person, such as his or her Aadhaar number, fingerprint data, and information on demographics. Next in line to gather, analyse, and assess user data is the Aarogya Setu App, which utilises applications for artificial intelligence, GPS, innovative Bluetooth networking, and analytics. Four types of information are gathered (referred to as "responses details")[17]: Bluetooth ID[18], GPS position, private indicators, and specifics of the self-examination exam. App can analyze the chances of Corona Virus infection using an algorithm that calculates the user's contact with others. The software identifies additional devices having Aarogya Setu installed in the vicinity of a smart phone once it has been installed through an easy and user-friendly method. If an examination is positive for any of these contacts, the program may use advanced metrics to determine the likelihood of infections[19].

Aarogya Setu app, designed by the Ministry of Electronics and Information Technology, GoI, is an open-source app[20]. The GoI introducted the Aarogya Setu app claiming it as a tool to trace the movements and contacts of a corona virus affected personnel and thus combating the COVID-19

---

[12] The Census Act, 1948, as amended in 1994, No. 37 of 1948, Acts of Parliament, 1948 (India)

[13] Office of the Registrar General & Census Commissioner, India, Ministry of Home Affairs, Government of India, Data Item collected in Census, (2011), https://censusindia.gov.in/census_and_you/data_item_collected_in_census.aspx

[14] The Collection of Statistics Act, 2008, No. 7 of 2009, Acts of Parliament, 2009 (India)

[15] The Collection of Statistics Act, 1953, No. 32 of 1953, Acts of Parliament, 1953 (India)

[16] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18 OF 2016, Acts of Parliament, 2016 (India)

[17] Ministry of Electronics and Information Technology, Government of India, Privacy Policy, Aarogya Setu Application, cl. 1(a), https://www.aarogyasetu.gov.in/privacy-policy/

[18] Ministry of Electronics and Information Technology, Government of India, Privacy Policy, Aarogya Setu Application, cl. 1(a), 1(b) and 1(c), https://www.aarogyasetu.gov.in/privacy-policy

[19] Ministry of Electronics and Information Technology, Government of India, Privacy Policy, Aarogya Setu Application, cl. 1(c) and 1(d), https://www.aarogyasetu.gov.in/privacy-policy

[20] Andrew Clarance, Aarogya Setu: Why India's Covid-19 contact tracing app is controversial, BBC (May 14, 2020), https://www.bbc.com/news/world-asia-india-52659520.

crisis[21]. In the initial phase of its launching, Aarogya Setu was made voluntary for installation but some orders released by some state governments and the Union government seems to be intended to mandate the setting up of the app at least for their workforce, if not for the general public[22]. After initial mandating and passing a phase of dilemma, the Ministry of Home Affairs (MHA) released fresh guidelines on lockdown on May 17, 2020, in which the instruction for using the app was changed from compulsory to a "best effort basis"[23]

The object behind the developing and launching the App for the people is to make them enable to assess the risk of getting in contact with the people who might be affected with Covid 19. Thus, the government considered the app to be significantly useful and ensured that the App is user friendly. Thus, for achieving the purpose of Aarogya Setu App individuals' personal information is at risk in the deficiency of any authorized paradigm and no responsibility clause.

Constitutional Aspect of Right to Privacy

The nine justices of the Supreme Court jointly acknowledged in the historic Puttaswamy suit ruling that the Indian Constitution's core right to private is the right to privacy[24].

The report submitted by the Justice Shrikrishna committee in July 2018 on data protection clearly specifies that "processing of personal data must only be undertaken for clear, specific and lawful purposes"[25]. The committee proposed that the data principal (the person whose personal data is gathered) have various rights, including the ability to revoke consent for data processing, report a breach, and have its wrongly developed data corrected by the establishment. In its decision, the SC recognized that "in the age of Big Data, the collecting and processing of personal data can disclose a lot about a person's lifestyle, choices, and preferences."[26]

Chandrachud J., who wrote the majority judgment, maintains that "the right to privacy is not independent of the other freedoms guaranteed by Part III of the Constitution. It is an element of human dignity and is an inalienable natural right[27]." He concentrates on the technological side of security and how it relates to human autonomy and integrity. The Court noted that the deployment of such technology could be permitted in certain instances when the objective pursued by the authority is legitimate. However, in spite of the legitimacy in the objectives behind the deployment of such technologies, it must be ensured that the situation necessitates the deployment and the deployment is being done in a proportionate manner. If we accumulate the test criterion given by

---

[21] *Aarogya Setu: A Multi-Dimensional Bridge, Press Information Bureau (02 April 2020, 04:21 PM), https://pib.gov.in/PressReleseDetailm.aspx?PRID=1610301.*

[22] *Ministry of Home Affairs, Order No. 40-3/2020-DM-I(A), 2020, Gen. S. R. & O.*

[23] *Vrinda Bhandari and Faiza Rahman, Constitutionalism During a Crisis: The Case of Aarogya Setu, 1.*

[24] *Puttaswamy v. Union of India, (2017) 10 SCC 1*

[25] *Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, (July 20, 2021, 07:31 AM), https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf*

[26] *Puttaswamy v. Union of India, (2012), Writ Petition (Civil) No. 494 of 2012.*

[27] *Vrinda Bhandari, Amba Kak, Smriti Parsheera and Faiza Rahman, An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict, IndraStra Global, 11, 1-5. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54766-2*

Justice Chandrachud and Justice Kaul. J "in order to satisfy the proportionality test adopted in Puttaswamy judgement, the use of any privacy infringing technology must satisfy five criteria."
1. It needs a legislative foundation first.
2. The second is the appropriateness of the goals in relation to the desired outcome.
3. Third, the need
4. Lastly, it ought to represent a sensible approach to achieving the desired result.
5. Lastly, formal safeguards against misuse of interfering with rights, which reiterate the fundamental need to maintain a "the procedures imposed by law" as stated in Article 21.
Before taking the Proportionality test, firstly researchers would take the functioning of Aarogya Setu.
In the case of health data, the Puttaswamy (Privacy) judgement (plurality opinion authored by Justice Chandrachud) emphasized the necessity for "data protection legislation to ensure that personal data was not used to discriminate against people based on their health state."

IV. AAROGYA SETU: THE ASSESSMENT OF PRIVACY FACTORS

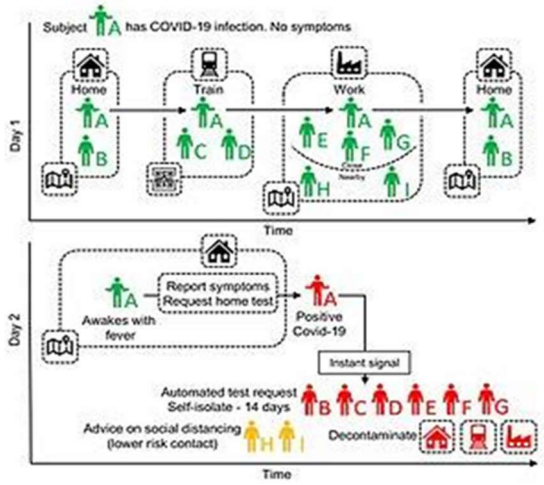
There is a lot of contact tracking applications[28] available nowadays, and a lot of them were created, established, and launched quickly. Such apps are generally helpful in that they let people keep track of nearby indicators and notify them immediately in the event that someone gets into touch with a coronavirus-positive instance[29]. But these advancements also bring confidentiality and moral difficulties. The World Health Organisation (WHO) released temporary guidance on May 28, 2020, outlining the fundamental moral precepts and conditions necessary to ensure the fair and proper adoption of electronic contact tracking technologies [30] .
An app's confidentiality agreement is a declaration, or regulatory document, that details how the app provider gathers, utilises, reveals, and handles information from users. Legal requirements force vendors of services, particularly app developers, to offer all relevant information concerning their procedures for collecting[31], exchanging, and organising data, as well as the manner in which they adhere to the law. Furthermore, customers may learn the way app builders and operators manage their private information primarily via their privacy terms[32].

In this part of the paper researchers will work on th,e assessment of privacy factors of Aarogya Setu in line with WHO principles and its privacy policy.

---

[28] *Hatamian, M., Wairimu, S., Momen, N. et al. A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps. Empir Software Eng 26, 36 (2021)*
[29] *Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Abeler-Dörner L, Parker M, Bonsall D, Fraser C, Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing. Science, 368, 6491 (2020)*
[30] *Ethical considerations to guide the use of digital proximity tracking technologies for covid-19 contact tracing (2020). WHO. https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1*
[31] *Hatamian M, Engineering privacy in smartphone apps: A technical guideline catalog for app developers, IEEE Access, 8, 35429, (2020)*
[32] Reidenberg JR, Breaux T, Carnor LF, French B, Disagreeable privacy policies: Mismatches between meaning and users' understanding, Berkely Technol Law J 30(1), 39, (2015)

Individuals must establish a profile and submit their cell phone number, gender, age, career, journey details, and how often they smoke in order to become eligible for the Aarogya Setu app. This information is maintained in an official database using a special digital identification (DiD). The authorities will use the information to generate compiled, anonymized statistics for managing COVID-19, notify people of their likelihood of contracting the virus, and offer healthcare workers the knowledge that is required to perform treatments[33]. The program utilises GPS and Bluetooth signals to transfer identification and capture time and position whenever an individual falls within reach of an additional application user. The date and time, as well as the location, are then saved on the individual's smartphone. The program records the geographical information of users remotely, approximately every fifteen minutes. Customers of the app have the opportunity to take self-evaluate exams that combine geographic information with questions regarding indicators, illnesses that underlie previous travel, and behaviour suspected that may have contributed to exposures[34]. If a user's self-evaluation test results indicate a probable illness or they test positive, the program will transmit the user's position and surrounding information into the server's memory. The data will be used by the federal government to identify hotspots for epidemics, which will need more investigation and medical intervention. In addition, the authorities will alert any other users that the individual who confirmed positive has had frequent interactions with[35]. All those who work in both the public and private industries, as well as individuals residing in COVID-19 confinement zones, have to download the app.



[33] Government of India, Aarogya Setu Privacy Policy, (July 20, 2021, 08:40 AM), https://web.swaraksha.gov.in/ncv19/privacy/

[34] India Today Web Desk, Aarogya Setu App: Follow these simple steps to do a self-assessment test, (May 02, 2020, 03:41 PM) https://www.indiatoday.in/information/story/aarogya-setu-app-follow-these-simple-steps-to-do-a-self-assessment-test-1673656-2020-05-02

[35] https://www.aarogyasetu.gov.in/terms-conditions/(July 20, 2021, 08:40 AM)

Fig. 1 A case study of a geographically based COVID-19 tracking of contacts application concept[36]

How Aarogya Setu works and what kind of data it generates?

A variety of information is gathered whenever an individual connects with the app: (i) identity; (ii) telephone number; (iii) DOB; (iv) gender; (v) occupation; and (vi) locations travelled in the past thirty days. The back-end server stores this data, which is encrypted and sent to the user-end app along with a distinct digital ID (DiD). The user's ID will then be linked to any information or data that is submitted from the app to the server and used for recognising them in any future app-related activities. People's geographic location is also taken upon registering and submitted to the website's server. The apps of two registered customers will consequently swap distinct digital IDs (DiDs) and log the GPS position and time of the interaction when they are in Bluetooth range of one another. The second enrolled user's smartphone or tablet will safely keep the data gathered from the user's app, and another individual will not be able to obtain it. This data will be safely transmitted from the authorised user's smartphone or tablet and kept on the computer in the event that the other person tests positive for COVID-19. The contact-tracing process is then continued using this data to identify any potential contacts of the individual who confirmed the coronavirus. Every fifteen minutes, the app gathers geographical data and safely saves it on your phone. This way, you'll have a history of all the locations you've visited. Only your DiD and this data will be posted to the database[37].

The GoI will solely use the private information gathered at the moment of enrollment in anonymous, collected records to produce status, heat maps, and other mathematical visualisations for the sole purpose of managing COVID-19 in the nation or to send out broad-term messages regarding COVID-19 as needed. DiD will only be linked to personal information in order to notify the individual of the likelihood that they have a Corona virus infection and/or to identify those who are performing administrative and clinical duties required in connection with COVID-19. AS collects information that is classified as personally identifiable data. Here, the issue of whether AS's current technological advancements are compatible with the Aarogya Setus privacy regulations emerges. What type of data protection technique is this organisation using? According to SriKrishna Committee report, "The issue of data protection is important both intrinsically and instrumentally. Intrinsically, a regime for data protection is synonymous with protection of informational privacy." Aarogya Setu was also made obligatory for the workforce of pvt. 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[38]. Failure to comply with the

[36] *Covid 19 apps, https://en.wikipedia.org/wiki/COVID-19_apps, May, 2020.*

[37] *Aarogya Setu: Information Collected and Manner of Collection, (May, 2020), https://www.aarogyasetu.gov.in/privacy-policy.*

[38] Aryan Puri and Sanya Rawlani, Aarogya Setu: The Right to have Rights, International Journal of Law, Management & Humanities, 4 (1), 1902, 1905-06 (2021)

guidelines would attract penal action under Sections 51 to 60 of the Disaster Management Act, 2005[39] and under Section 188 of the Indian Penal Code, 1860.

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[40]maximum punishment can be extended up to one year imprisonment, or with a fine of rupees one thousand, or both.

Since Aarogya Setu fails to derive its authority through a legal structure to oversee its activities and provide appropriate safeguards for procedures, it breaches the initial element of the rule of proportionality in this particular case. Private data regarding the wellness and whereabouts of freelancers, gathered via the Aarogya Setu app[41], may be utilised for widespread monitoring and characterization regardless of whether the COVID-19 epidemic has ended since there is no statutory assurance with an expiry provision. The court moved on to say that throughout pandemics, authorities may gather and use private medical information to create appropriate regulatory initiatives, but that information needs to be anonymized. The IT (reasonable security practices and procedures and sensitive personal data or information) Regulations, 2011 handle "health care documents" as personally identifiable data, despite the IT Act of 2000 having regulations that safeguard individuals' private data. These regulations, however, are insufficient to safeguard receptive private data. Detailed healthcare data is likewise classified as "receptive intimate information" under the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, which were promulgated under Section 43A of the Information Technology Act, 2000. These rules stipulate that health-related information may only be gathered and handled by organisations with permission from the user [Rule 5(1)]. Additionally, the regulations place on the corporations a number of requirements pertaining to notification [Rule 5(3)], storage restriction [Rule 5(4)], right of notice [Rule 5(2) and 5(5)], right to inspection and rectification [Rule 5(6)], and right of opt-out [Rule 5(7)][42]. Furthermore, the IT Act of 2000 only applies to businesses and does not apply to the federal government, making IT regulations a unique effort at safeguarding private information. The authorities must obtain the person's agreement before obtaining and disseminating their health information, as well as before determining the uses for which different organisations may use such information. Specifically, using electronic health

[39]The Disaster Management Act, 2005, No. 53 of 2005, Acts of Parliament, 2005 (India)

[40]The Indian Penal Code, Act No. 45 of 1860, 1860 (India)

[41] *"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", Ministry of Electronics and Information Technology, Government of India, Notification of the Aarogya Setu data access and knowledge sharing protocol, 2020 in light of the COVID-19 pandemic (May 11, 2020), https://www.aarogyasetu.gov.in/wp-content/uploads/2020/06/mygov-1000000000981057882.pdf*

[42] *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.*

information for combating epidemics only when anonymous or anonymized Because of this, even though India does not yet have comprehensive data privacy legislation, courts and the government have often acknowledged the need to protect personal health data.

Nearly every democratic industrialised nation has strong legal frameworks in place to shield their residents' personal information from violations of any kind. The fact that so many emerging nations have started down the same path is heartening. However, information on which governmental entity gets possession of the data and for how long is not included in the contract of agreement or privacy policy of the Aarogya Setu program. There are several instances when the authorities are monitoring Contact Tracing Apps' privacy policies. The Kenyan high court ruled that "GPS The coordinates and DNA specimens could not be gathered according to the heading of an overall law, but in a nutshell would necessitate establishing rules to gain an effect of law" in response to the constitutional challenge to NIIMS/Huduma Namba, the country's national biometric identity project[43]. The High Court of Justice in Israel ruled that the Shin Bet security agency could not keep monitoring verified carriers' cell phone numbers without the government's approval of this very controversial practice[44]. The court also said that the monitoring program "seriously breaches the basic right to confidentiality and ought not to be taken lightly."

A number of cases have been launched in the Kerala High Court challenging the legality of the MHA order, claiming that requiring the app to be completely covered at locations of employment and detention is discriminatory[45]. Its goal is "to prevent law enforcement from using coercive measures to enforce the obligatory installation of apps" in the short term. After that, on May 12, 2020, at a perception, the court spoke with the Centre directly on the need for the demand, taking into account that the nation's pace of adoption of smartphones does not lend itself well to its enforcement. Prima facie, the Court noted that the complainant has expressed "legitimate worries" about the directive's forceful character and requested a response from the Centre. The Centre was also requested by the court to address the objections made about the application's guarantees of privacy[46].

V. AAROGYA SETU: DEFICIENT TO FOLLOW PRIVACY PRINCIPLES

[43] *Anand Venkatanarayanan, Notes from a Foreign Field: Public Participation, Constitutional Rights, and Technological Design in the Kenyan High Court's Huduma Namba Judgment [Guest Post], (July 20, 2021, 08:21 AM), https://indconlawphil.wordpress.com/2020/02/19/notes-from-a-foreign-field-public-participation-constitutional-rights-and-technological-design-in-the-kenyan-high-courts-huduma-namba-judgment/*

[44] *Stuart Winer and Times of Israel staff, High Court: Shin Bet surveillance of virus carriers must be enshrined in law, (Apr.26, 2020, 11:50 PM), https://www.timesofisrael.com/high-court-shin-bet-surveillance-of-virus-carriers-must-be-enshrined-in-law/*

[45] *John Daniel v. Union of India and ors,(2020)*

[46] *Livelaw News Network, how 'Aarogya Setu' Can Be Made Mandatory When Many Workers Have No Smartphones, Kerala HC Asks Centre, (May 12, 2020, 5:51 PM), https://www.livelaw.in/news-updates/kerala-hc-to-centre-how-aarogya-setu-mandatory-when-workers-have-no-smartphones-156646*

The Aarogya Setu App, in addition to lacking a legal foundation, diverge from worldwide greatest practices for contact tracking applications and not succeed to meet data shielding requirements for the reason appended below:

a) Lack of Consent

Consent is a bedrock principle of privacy that informs data subjects about the kind of data the app would like to collect and asks them for consent to collect that data[47]. Consent entails giving customers the option of agreeing to have their data used in a certain way or not using the service or application at all. The usage of Aarogya Setu is no longer voluntary, since it was made voluntary-mandatory by a notification in order to make it an e-pass for public venues like for using any services of the government we have to download the App. As a result, there is no way for users to deny consent or opt out.

b) Lack of Data Minimization

At the time of Registration for the Aarogya Setu app, it requires sharing large amounts of personal data: name, phone number, age, sex, profession, countries visited in the last 30 days and smoking habits[48]. This is inconsistent with the principle of data minimization.

c) Lack of Transparency and Third-Party use

While it is stated that personal data gathered by Aarogya Setu is aggregated and anonymized, no publicly available information on the aggregation and anonymization procedures and methodologies is available. The Aarogya Setu protocol reads, "The anonymization standards to be used in this process shall be developed, reviewed and updated by an expert committee appointed by the Principal Scientific Advisor to the Government of India[49]." There seems to be a failure in developing a fully formalized anonymization process. Because there is a considerable threat of re-identification unless personal data is adequately anonymized, the app must undergo extensive security testing by governmental and independent authorities.

MyGov says "the app has been built with privacy as a core principle" and the processing of contact tracing and risk assessment is done in an "anonymized manner". Mr. Singh Abhishek Singh, CEO of MyGov at India's IT ministry which built the app, says when you register, the app assigns you a unique "anonymized" device ID. All interactions with the government server from your device are done through this ID only and no personal information is exchanged after registration. Experts in the subject, however, have cast doubt on the government's assertion. India has taken decades to

---

[47] *A privacy notice is a document or language that defines how an organization, software, or application collects, processes, and transmits user data, and what data protection principles are applied. (July 20, 2021, 10:04 AM), https://gdpr.eu/privacy-notice/*

[48] *However, the app does not provide an explanation for why it requests the demographic (age, sex, profession) and prior health data (such as whether the individual is a smoker), Government of India, Aarogya Setu Privacy Policy, (July 20, 2021, 10:09 AM), https://web.swaraksha.gov.in/ncv19/privacy/*

[49] *Government of India, Notification of the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 in light of the COVID-19 pandemic, (May 11, 2020), https://www.meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf*

recognize Right to Privacy as a fundamental Right and at many instances the data of users have been compromised. However, Mr. Pahwa points out that Aadhaar, the biggest and most contentious biometrics-based identification system in the world, has "a horrible history" of safeguarding personal information in India[50]. The push to force individuals to download the app, according to retired Supreme Court judge BN Srikrishna, was "completely illegal" in a conversation with The Indian Express daily. "Subject to what legislation is it required? It is not now supported by any laws," he informed the publication.

d) Cyber Security flaws (Claims of ethical hackers):

It was reported that a French cybersecurity analyst had claimed that the data of positive cases could be accessed by him through the Aarogya Setu app. According to him, Aarogya Setu has many privacy and security vulnerabilities. However, the government quickly reacted to the claims, saying that hacking the Aarogya Setu app was impossible, a claim that has since been debunked[51].

A Bengaluru-based software engineer has also managed to hack the app. It seems that the developers, Jay, were able to get past the app's security measures in just over four hours. This reveals gaping holes in the cyber security walls that are meant to protect personal sensitive data[52].

e) Functionality creep and the potential hazards of unauthorised sharing of information

Another problem with the app is external information distribution, which makes it simple for the governing body to transfer the data it has gathered on an individual to a "server" that is operated and owned by the GoI. For "essential clinical and procedural actions," the government may disclose this particular data to "other needed and pertinent persons." It is troublesome, according to the Software Freedom Law Centre, a group of attorneys, technologists, and pupils, since it allows the government to communicate its information with "literally everyone it wants." The sharing of personal data acquired by the Aarogya Setu app with third parties is not prohibited. The Aarogya Setu Privacy Policy does not clarify which government agencies would have access to the app's personal data. As a result, law enforcement authorities may utilise sensitive personal data acquired for contact tracing for punitive reasons[53].

VI. LACK OF LEGISLATION FOR MANDATORY IMPOSITION OF THE AAROGYA SETU APPLICATION: ISSUES AND CONCERNS

[50] *Andrew Clarence, Aarogya Setu: Why India's Covid-19 contact tracing app is controversial, BBC News, Delhi (May 15, 2020), https://www.bbc.com/news/world-asia-india-52659520*

[51] *Tripti Dhar, Aarogya Setu – Carrying your privacy in your hands? (June 25, 2020), Aarogya Setu - Carrying Your Privacy in Your Hands? by Tripti Dhar :: SSRN*

[52] *Money control News, (May 13, 2020, 08:21 PM), https://www.moneycontrol.com/news/technology/bengaluru-techie-hacks-covid-19-tracking-app-aarogya-setu-to-appear-safe-in-less-than-4-hours-5262771.html*

[53] *Anmol Dhindsa and Sashwat Kaushik, The Constitutional Case against Aarogya Setu, (May 26, 2020), The Constitutional Case against Aarogya Setu by Anmol Dhindsa, Sashwat Kaushik:SSRN*

"Legislation is one of the most important instruments of government in organizing society and protecting citizens. It determines amongst others the rights and responsibilities of individuals and authorities to whom the legislation applies. On the other hand, a law has little or no value if there is neither discipline nor enforcement[54]."

In this part of the research paper, researchers addressed the absence of legislative underpinnings as well as certain practical governance concerns linked to the app's rollout. We begin by debating the criteria for judging presidential action in a crisis and whether unusual circumstances actually necessitate extraordinary actions. To answer the question whether the 'Aarogya Setu Data Access and Knowledge Sharing Protocol 2020' has any legal value? Next, we discuss the significance of having a precise and unambiguous legal framework and the reasons why the Disaster Management Act and Section 144 of the Criminal Procedure Code do not provide a strong enough legal basis for the application[55].

In order to meet its mission of supporting the fight against COVID-19, the nation's government developed the "Aarogya Setu Data Access and Knowledge Sharing Protocol 2020," which aims to guarantee safe data collection by the tracing app and limit how such data may be disseminated.

The policy was created by 'Empowered Group 9' of the National Disaster Management Authority, which is also responsible for overseeing data and technological solutions in the case of a coronavirus epidemic. The purpose of the Protocol is to describe the procedures by which the National Informatics Centre (NIC) will collect and share the data produced by the Aarogya Setu app:

a) Demographic information, including name, age, occupation, gender, and past travel history.
b) Contact Information: people the user has recently interacted with.
c) Information from the user's evaluation about their well-being and emotions; and
d) Information about their location.

To answer the question whether The Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 has any legal value? Raman Chima, policy director at Access Now, explained "The protocol is not a binding legal regulation; it is in effect a voluntary declaration by one group set up by the Union Government,". "It does not even claim to be issued under the legal authority of the Disaster Management Act[56]."

Section 10(2)(l) of the Disaster Management Act of 2005 is being used by the government to justify the application's obligatory implementation. In response to any impending catastrophe scenario or disaster, the government can provide instructions on any topic of legislation under this provision.

---

[54] *Herman de Jager, Importance of Legislation, Auditing SA, (2000) https://repository.up.ac.za/handle/2263/14758*

[55] *Bhandari, Vrinda and Rahman, Faiza, Constitutionalism During a Crisis: The Case of Aarogya Setu (May 25, 2020). Coronavirus Pandemic: Lessons and Policy Responses, Uma Kapila ed. (Academic Foundation, New Delhi, 2020), Available at SSRN: https://ssrn.com/abstract=3774716 or http://dx.doi.org/10.2139/ssrn.3774716*

[56] *Vakesha Sachdev, Does Govt's New Data Protocol Address Concerns Over Aarogya Setu? (May, 13, 2020, 05:52 PM), https://www.thequint.com/news/india/govt-releases-new-aarogya-setu-app-data-access-protocol-experts-privacy-concerns*

It is challenging to infer the truthfulness of this provision from entry number 97 of the list of provisions in the Seventh Schedule of the Indian Constitution, which states that only the parliament has the authority to enact laws pertaining to the utilisation and gathering of data because such laws are only encompassed by the Union list. Since it was not created by a parliamentary act, the National Executive Committee established under the Disaster Management Act, which released the guidelines on May 1, 2020 mandating the setting up of Aarogya Setu, is not an official organisation. It is also important to note that, in this particular instance, there is no proof of any particular parliamentary approval for controlling the set-up of the Aarogya Setu app[57].

The government's directive is unclear in terms of how these recommendations will be implemented. how these guidelines will be imposed on people who do not own smartphones. Only the Ministry of the Home Affairs does not provide enough legal support. 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"[58].
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[59].
It established standards for data collecting and processing, but this is insufficient to demonstrate the legality of the application's obligatory usage. Because there is no law requiring the download of this software, it must be the primary focus of Citizens' health 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[60].
How could the administrative authorities keep these penal provisions when the App has no Legal validity? Again, this would be a violation of your fundamental Rights and showing the excessive use of arbitrary powers which violates the Natural rule of justice. The very recent example in Uttar Pradesh where the UP police issued new guidelines, action will be taken against people going

[57] *Aryan Puri and Sanya Rawlani, Aarogya Setu: The Right to have Rights, 4, International Journal of Law Management and Humanities, 1902, 1904 (2021)*
[58] *Ananth Padmanabhan, Data Governance & Democratic Ethos - Rahul Matthan, Justice BN Srikrishna with Dr.Ananth Padmanabhan, (11 May, 2020), Data Governance & Democratic Ethos - Rahul Matthan, Justice BN Srikrishna with Dr.Ananth Padmanabhan - YouTube*
[59] *Government of India, Notification of the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 in light of the COVID-19 pandemic, (May 11, 2020), https://www.meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf*
[60] *Aryan Puri and Sanya Rawlani, Aarogya Setu: The Right to have Rights? 4, International Journal of Law Management and Humanities, 1902, 1904 (2021)*

outdoors without installing the Aarogya Setu app in Gautam Buddha Nagar in western Uttar Pradesh[61].

"If smartphone users do not have the 'Aarogya Setu' app installed on their mobile phones, then that will be punishable and considered a violation of the lockdown directions," Additional Deputy Commissioner of Police, Law and Order, Ashutosh Dwivedi said. What could be the protective measures the machinery has, to prevent the abuse of such data and alleviate worries about surveillance?[62] This kind of statement in the media is a clear violation of fundamental Rights.

Aarogya Setu Information Accessibility and Knowledge Exchange Protocol, 2020[63], establishes guidelines for gathering, using, and disclosing sensitive information[64]. Nevertheless, neither the Disaster Management Act of 2005 nor any other official source may provide the Protocol with legal standing. More importantly, it is not trying to give the app any legal legitimacy. Therefore, it is not possible to interpret the terms of the Protocol as creating legal justification for using the Aarogya Setu app.

There are no legal procedures established if the agreement is broken and the data is misused. For instance, to comprehend the protocol's policy If your security is violated through the disclosure of your health information—which belongs to the umbrella term of sensitive personal data—with an outside entity despite your consent, or if a government organisation communicates data with an investigation organisation that hasn't correctly encrypted, or if a confidential business that obtained the data correctly forwards it on to other people, such as disclosing your medical and email address to an insurance provider or marketers, the challenges in lodging a grievance in the present situation would arise from: (a) The Liability clause (the government has effectively absolved itself of any legal liability in case of a breach).

(b) The use of Aarogya Setu is not restricted by any law or data protection legislation. The reality that the agreement has a "sunset clause" for the protocol itself in Paragraph 10 is another feature that has drawn a lot of criticism. As a result, after six months, the Empowering Committee will assess the Protocol's progress and determine if it needs to be extended; if not, it will stop working.

---

[61] *ET Government, COVID-19 Crisis: Not installing 'Aarogya Setu' app becomes a criminal offence in UP (May 06, 2020, 09:46 AM), https://government.economictimes.indiatimes.com/news/digital-india/covid-19-crisis-not-installing-aarogya-setu-app-becomes-criminal-offence-in-up/75566422*

[62] "Digital interoperability has generated large databases from otherwise isolated and meaningless information. Coupled with algorithmic ingenuity in successful predictions, it is now possible to know more from less." Ankit Kapoor, Operationalizing Privacy by Design: an Indian illustration, 1.

[63] *Digital interoperability has generated large databases from otherwise isolated and meaningless information. Coupled with algorithmic ingenuity in successful predictions, it is now possible to know more from less." Ankit Kapoor, Operationalizing Privacy by Design: an Indian illustration, 1.*

[64] *Government of India, Notification of the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 in light of the COVID-19 pandemic, (May 11, 2020), https://www.meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf*

Nonetheless, as Media Name's creator, Nikhil Pahwa, noted, "there is no sunset clause for the utilisation of the app itself." The protocol, but not the software, has a sunset date. Because the rule itself will not apply to any data obtained once it expires, this fosters even more mistrust.

VII. CONCLUSION

The government's poor track record on privacy, lack of transparency, and lack of data protection laws has raised serious concerns. The government must address the following primary issues: (a) where does the app get its legal legitimacy from, given that there are obvious reasons for the invasion of privacy? (b) Legal protections against data theft. The government must address this issue.

These concerns must be addressed openly by the government. Transparency, accountability, protecting individual rights, identifying organizational measures and compliances to be done, to mention a few guiding elements. It is all more vital to establish a data protection legislative framework in the current environment of contact tracing applications. At the end of the day, no amount of sophisticated technology will be able to save us from this unprecedented threat to our health and economic stability. At most, the most apparent technological solutions will be of little assistance. At the very least, it is the responsibility of their creators to guarantee that they cause no harm. However, under the App's privacy policy, registered users' access, correction, and erasure rights are limited to only the personal information that they have provided. As a result, in the absence of regulation, adherence to the privacy principles is insufficient.

Finally, the use of contact tracking applications will put the balance between government monitoring and consumer privacy to the test. The necessity for data protection laws is clear in India for protection of the fundamental right that is "Right to Privacy".