|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 2|JUNE 2020|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2019): 2.32|
|IMPACT FACTOR (2018): 2.527|

|LAW AUDIENCE JOURNAL®|

|VOLUME 2 & ISSUE 2|JUNE 2020|

|ISSN (O): 2581-6705|

EDITED BY:

LAW AUDIENCE JOURNAL'S

EDITORIAL BOARD

|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 2|JUNE 2020|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2019): 2.32|
|IMPACT FACTOR (2018): 2.527|

Email: lawjournal@lawaudience.com, info@lawaudience.com,

Phone: +91-8351033361,

Website: www.lawaudience.com.

Facebook: www.facebook.com/lawaudience

Instagram: www.instagram.com/lawaudienceofficial

Contact Timings: 5:00 PM to 9:00 PM.

|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 2|JUNE 2020|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2019): 2.32|
|IMPACT FACTOR (2018): 2.527|

DISCLAIMER:

Law Audience Journal (ISSN (O): 2581-6705) and Its Editorial Board Members do not guarantee that the material published in it is 100 percent reliable. You can rely upon it at your own risk. But, however, the Journal and Its Editorial Board Members have taken the proper steps to provide the readers with relevant material. Proper footnotes & references have been given to avoid any copyright or plagiarism issue. Articles published in ***Volume 2 & Issue 2*** *are the original work of the authors.*

Views or Opinions or Suggestions ***(if any)****, expressed or published in the Journal are the personal point of views of the Author(s) or Contributor(s) and the Journal & Its Editorial Board Members are not liable for the same.*

While every effort has been made to avoid any mistake or omission, this publication is published online on the condition and understanding that the publisher shall not be liable in any manner to any person by reason of any mistake or omission in this publication or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this work.

All disputes subject to the exclusive jurisdiction of Courts, Tribunals and Forums at Himachal Pradesh only.

|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 2|JUNE 2020|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2019): 2.32|
|IMPACT FACTOR (2018): 2.527|

"AAROGYA SETU A PERSONAL BODYGUARD OR A POTENTIAL SPY?"

AUTHORED BY: MS. ANAMIKA DUBEY & CO-AUTHORED BY: MR. ANKIT SINGH, K.L.E. SOCIETY'S LAW COLLEGE,
EMAIL IDS: ANAMIKAD162@GMAIL.COM,
HCLANKITSINGHRATHEE@GMAIL.COM,
PUBLISHED AT: WWW.LAWAUDIENCE.COM.

I. INTRODUCTION:

Today when the Novel coronavirus or the Covid-19 has created havoc worldwide, the world continues to see drastic changes since the pandemic took over; India is amongst the many other countries trying to fight it through this pandemic. In today's era, Mobile applications have a colossal effect and the role that they play is indispensable in everyday life. These applications can be highly influential as they have become so tremendously intertwined and hence are very convenient in shaping the society. There are applications for almost every need of an individual and as these platforms continue making lives of individuals a plain sailing even the government to a certain extent bank upon mobile applications for shaping the needs of the country. In today's time when the pandemic (COVID-19) continues to haunt us and has made it extremely burdensome to step outside, the Indian government has taken various steps towards the curtailment of the spread of the virus.

II. AAROGYA SETU APP:

Aarogya Setu is one such step taken by the government. It's a contact tracing app which keeps a track of the health status of the user. It's been designed by the National Informatics Centre and was launched on April 2, 2020. The main objective of the app is to encompass the

spread of the novel coronavirus or COVID-19 and break the chain of the novel coronavirus or COVID-19 as it is a highly contagious disease and can spread to host via plethora means whether it is sneeze or touch. Thus, the containment is requisite and thereby the app aids in keeping a track of the individual user's health, whether or not one has COVID-19 and secondly it scans or identifies all users who may have come in close contact with a COVID-19 positive user. The app continuously scans for active cases in the area so as to send an early warning signal to the user regarding the spread of the disease in the area and for this it makes use of Bluetooth and GPS to alert the person if they have come under the close proximity of Covid-19. The app upon downloading promotes its user to enter their personal details such as name, phone number, age, sex, profession and travel history. The information collected by the users is then transmitted and stored remotely with ***Central Governments National Informatics Centre (NIC)*** data storage facility. Every individual user of the app after filing the required data is given a unique ID. Data collected by the app will be stored only for 30 days (as per the latest revised policy of the app).

II.I WORKING OF THE AAROGYA SETU APP:

Now, coming to the ***working of the app*** the tracking of the individual's health and contact tracing takes place in two ways. Firstly, when the user is frequently asked to update their health status with the app with the help of a survey, it helps in tracking the health status of the individual on a regular basis. Secondly, with the help of location mapping the location of individual users is tracked via GPS, which makes contact tracing efficient. The app aids in identifying COVID-19 positive cases so that the concerned authority can take further actions such as quarantining and the areas which need to be sanitised or sealed.

II.II IS IT MANDATORY TO DOWNLOAD THE AAROGYA SETU APP?

The app since its launch has crossed the mark of 100million download. But ***is it mandatory to download it?*** The list of citizens who are mandatorily asked to download the app are

government and private sector employees, also all the citizens in the containment zones are required to download the app. Even the recently issued guidelines by the Airport Authority of India (AIA) for domestic flights make it mandatory to download the app. Thus indirectly a large chunk of the population will be required to download the app.

II.III IS THIS MOBILE APPLICATION A POTENTIAL SPY OR REALLY A PERSONAL BODYGUARD AGAINST THE DEADLY VIRUS?

The app has received several criticisms from the opposition political parties and some even come to the conclusion of calling it a spy and according to the others the app violated the right to freedom of privacy. The legal alibis that the State employs to justify its infringement of our privacy are numerous, and range from 'public interest' to 'security of the state' to the "maintenance of law and order". But, the constitution of India does not expressly safeguard the right to privacy as stated in ***Kharak Singh V. State of U.P.***[1]. In ***PUCL v. Union of India***[2], the court held that Right to privacy was not identified in the constitution. It stated that a telephonic conversation without any sort of interference can be certainly claimed as a right to privacy. *"When a person is talking on telephone, he is exercising his right to freedom of speech and expression",* the court observed, and therefore *"telephone-tapping unless it comes within the grounds of restrictions under art. 19(2) would infract Art. 19(1) (a) of the Constitution*[3]*."*

Thus, the concept of Right to privacy is limited in India and not absolute. The Supreme Court of U.S. in a case[4] where the GPS system installed on a car was challenged held that installing a Global Positioning System (GPS) tracking device on a vehicle and using the device to monitor the vehicle's movements constitutes an unlawful search thereby breaching the right to privacy of an individual. The judge also further stated that GPS can reveal the entire

[1]AIR 1963 SC 1295.
[2] AIR 1997 SC 568, (1997) 1 SCC 301.
[3] AIR 1997 SC 568.
[4] U.S. v. Jones132 S.Ct. 945 (2012).

profile of a person by keeping a track on the places he/she visits and the government can make the most out of this data in the future. "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. Disclosed GPS data will be trips to the psychiatrist, plastic surgeon, abortion clinic, AIDS treatment centre, strip club, criminal defence attorney. The government can store such records and efficiently mine them for information years into the future doing so by the government may alter the relationship between citizen and government in a way that is inimical to a democratic society. In the current situation, the question that arises is whether the data stored with the government can be misused?

The only Act which provides for data protection is the Information Technology Act, 2000. Sec. 43 A of the act provides[5] for the compensation in case of failure to protect data but only takes into consideration the private companies and the government seems to have been immune from the application of this Sec. Sec 72 of the Act provides penalty for Breach of confidentiality and privacy Further, Sec. 72(A) provides, Punishment for disclosure of information in breach of lawful contract. The act as stated above only takes into consideration private companies and not the Government, now in the present scenario how does an individual seek protection against the data which it has provided to the government? In a landmark judgement ***K.S Puttaswami & another v. Union of India[6]***, the Supreme Court had held that right to privacy is a fundamental right. "Informational privacy" has been recognised as being a facet of the right to privacy and the court held that such information about the

[5]Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.
Explanation.–For the purposes of this sec.,– (i) ―**body corporate**‖ means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities; (ii) ―reasonable security **practices and procedures**‖ means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit; (iii) ―**sensitive personal data or information**‖ means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

[6] (2017) 10 SCC 1

person and the right to access this information also needs to be given the protection of privacy.

The ***Data Protection Bill (hereinafter referred to as bill)*** is the first attempt towards protection of personal data. The Bill is aimed to endow security of data to all the Indian citizens. The reading of preamble makes it crystal clear that this bill is the by-product of Aadhaar judgement[7]. The bill in its preamble also contains a mention that this bill provides for regulation of personal data with respect to cross-border transmission and also to provide remedies for unauthorised and harmful processing, and to establish a ***Data Protection Authority*** for overseeing processing activities.

Sec. 4 of the bill states that anyone who collects the data is responsible for its safe keeping. Similarly, Sec. 10 cl. (1) provides that data shall only be retained for the period which is reasonably necessary to satisfy the purpose for which it is processed. cl. (2) provides an exception to this rule as it states that the data can be hold on for a longer period if such retention is mandatory or is necessary to comply with any obligation under a law. Further, Sec. 12 cl. (1) provides that data shall be processed on the basis of consent of data principal i.e. person to whom data in point of fact belongs. Sec. 12 cl. (2)(a) makes it obligatory upon the data retrieving entity to make sure that the data is taken from any person based upon his free consent and meets all the concomitants required under sec. 14 of the Indian Contract Act, 1872 (9 of 1872).

Further, Sec. 19 provides that any data may be processed by the state under two circumstances mentioned under Sec. 19 (a) i.e. for any function of Parliament or State Legislature and (b) for exercising any function of the State authorised by law for the provision of any service or data benefit to the data principal. Sec. 96 provides for data mishandling offences by the state and central government cl. (1) provides that in case of data breach the head of the department or the authority shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly. However, as per Sec.

[7] Justice KS Puttaswamy v. Union of India, (2017) 10 SCC 1.

42 exemptions may be granted for the security of the state. Thus, we see ***Data Protection bill*** is a step towards the protection of personal data.

III. CONCLUSION:

Today when the government is taking various measures to curb the spread of the deadly virus, contact tracing applications like the Aarogya Setu has helped in aiding the present situation by giving them the early mover advantage. The app has more importantly been a great help to the frontline workers mainly those in delivery sectors, doctors and other employees. The app as of now has done more good than cause any harm.

But despite the present-day situation, the data would remain available to the government in the long term and if not handled with care will infringe privacy. Contact tracing apps make use of sensitive personal data and the use of such data raises serious questions. Despite the fact that these apps are created considering the good of the people but in no way shall they take away the basic constitutional rights of the people and violate one's privacy. In the end, it all comes down to the proverb that technology is a useful servant but a dangerous master.