SUPREMO AMICUS

VOLUME 30 | JUNE, 2022 ISSN 2456-9704

RIGHT TO PRIVACY AND DATA PROTECTION DURING COVID-19

By Dr. Amita Verma
Associate Professor, University Institute of Legal Studies, Panjab University

By Sanya Singh
LLM Scholar, University Institute of Legal Studies, Panjab University

"Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life"

Puttuswamy verdict

INTRODUCTION

21st century is the time when the world is witnessing fast moving technological advancements which are at one hand quite beneficial and utilitarian to the humanity while at the same time, they come at a cost of having a vigilance on us as well as seeking our data which has become the new currency. Right to privacy has become a major issue which has been characterised by large scale sophisticated and advanced technology in communications and other systems. We have become so lost in our race of development that technological development has allowed to take place and constantly evolve without fully considering its impact on the democratic political systems. This is not just an isolated fear but has become a dreadful reality as has been exemplified by events such as Cambridge Analytica which has shown us how our data is not safe and how privacy of individuals is violated and the end result is manipulation of human being towards the gains of big corporations and governments.

The concerns with respect to privacy are becoming more and more pressing because of widespread use of information systems to avail even the most basic services which are considered essential to one's well-being. Today, people search jobs, houses and other services by disclosing information about them on internet where the man is oblivious to how the data entered by him is ultimately being used and what all parties are able to have access over this information. This information input by us accumulates into files maintained by private and public institutions. This might seem trivial to the people who are not yet aware of the value of this data regarding them. This data is so priceless that corporations are after this only. Data is the new currency and the new gold.

In this background, a major cause of concern is the lack of any legislation and organisational rules which protect the right to privacy, ensures maintainability of confidentiality and due process to the computerised information. Privacy is a basic value in a democratic and civilised society, a guarantor of individual autonomy.[1] It is man's claim to human dignity which extends to protecting his own information – information which is an encyclopaedia of selfhood, which should be for the person to decide when and to what extent he wants to

[1] Brandeis Louis Dembitz and Warren Samuels Dennis; "*The Right to Privacy*"; (HLR); 2019; Pg 5

communicate.[2] Even where such information is divulged in order to obtain certain benefits, the individual does not actively consent for his information to be shared further and for purposes other than beyond the original disclosure. Therefore, a discussion into right to privacy is of utmost importance in the present times, which places focus on an individual and his rights to control the sharing of his information in a technological world. This is all the more urgent considering the fact that in a relationship between individuals and major companies/organisations, the scales of power are tilted in favour of the latter. The bitter and scary reality of today is that sharing of information is happening only one way where only the organisations are learning about the individuals while the individuals are getting as little information about the institutions as possible.[3] And not just this, but when the party infringing the privacy to collect data, is the government itself, then the concerns become graver creating an apprehension of an Orwellian society becoming true where each and every movement and activity of the citizen is being carefully monitored.

On top of this, 2020 has proved to be an unprecedented year where the world has been exposed to coronavirus which has wreaked havoc everywhere. With time, at a very fast speed only, it assumed an unsettling global position of pandemic, a crisis of its own kind which the modern world had barely imagined. With its rapid increase and sky rocketing number of fatalities, governments everywhere had to take prompt actions to curb the spread and to protect the people. Technology has been put to its beneficial uses, to contain the spread by using techniques such as contact tracing and documentation of people under quarantine. The government has placed heavy reliance on technology for this. However, difficult times may call for desperate measures, but this is no excuse to put unconstitutional means to use.

HISTORICAL DEVELOPMENT OF RIGHT TO PRIVACY

The history of privacy can be delineated back to the phrase "the right to be let alone" in 1834 in the renowned case of *Wheaton v. Peters*,[4] wherein the Supreme Court of U.S.A stated that "defendant asks nothing – wants nothing, but to be let alone until it can be shown that he has violated the rights of another". Later on, the phrase, "right to be let alone", was used in Cooley's book[5] as a corresponding duty to "not to inflict injury" on another. This argument was further advocated and expanded by Warren and Louis Brandeis,[6] in their well-known work which discussed the right of privacy. It is this

[2] Nishant Singh; "*Right to Privacy and Internet*"; (Createspace Independent Pub, New Delhi, 2015); Pg 15

[3] Dr. Mandeep Kumar and Puja Kumari; "*Data Protection and Right to Privacy: Legislative Framework in India*"; (JCR), Vol 7, Issue 11, 2020; Available at https://www.bibliomed.org/mnsfulltext/197/197-1595669532.pdf?1634470639

[4] *Wheaton v. Peters*, 33 U.S. 591 (1834)

[5] Dorothy J. Glancy; "*The Invention of Right to Privacy*"; (ALR), Vol 21, 1979; Available at https://law.scu.edu/wp-content/uploads/Privacy.pdf

[6] Samuel D. Warren and Louis D. Brandies; "*The Right to Privacy*"; (HLR), Vol 4, No 5, December, 1890; Pg 193-220; Available at https://www.jstor.org/stable/1321160?refreqid=excelsior%3A00ac390393d20b5dcea951cd91a81468&seq=1#metadata_info_tab_contents

very article which is credited with being instrumental in starting discussion on right to privacy and leading to its ultimate acceptance by American States as a legal right within a relatively short period of its publication. According to Brandeis, privacy is the most cherished freedom in any democratic environment and therefore, deserves to be given due recognition in the Constitution itself. The authors emphasised on the advancements in rights of press and the scrutiny which has become possible due to the recent inventions such as photography and print media. Therefore, they drew attention to the intrusion into privacy of a person through public dissemination of private details of a person's private life.

The concept of right of privacy has always been connected to mankind, so the evolution of privacy can also be said to have its origin from the evolution of the humans itself. The entitlement to privacy is something which comes naturally to the mind of any person. A human being, although a member of society, has always claimed, total non-interference by other persons and by the State with respect to certain matters. In India, the notion of privacy finds its mention in the ancient law of *Dharamshastras* and the ancient Hindu texts such as *Hitopdesha*.[7] *Dharamshastras* along with their several commentaries expounded the law of privacy in Indian sub-continent. The text of *Hitopdesha* provides that in certain matters such as worship, sex and family matters among many others, protection against disclosure must be guaranteed.[8] The rule prevalent in ancient Indian society was "*Sarvas Swe Swe Grihe Raja*" i.e., everyone is a king in his own house.[9] Therefore, the natural corollary of this was that each person was entitled to certain level of privacy within the walls of his house. Privacy of information and communication has been largely confined by Hindu jurisprudence to the realm of the sovereign. Both the *Manusmriti* and the *Arthshastra* acknowledged the importance of a secret council that aided the king in deliberations and important decisions.[10] Such decision making was required to be performed in a reclusive place which remained well-guarded to ensure privacy. These decisions were revealed to public only on a need-to-know basis. Therefore, the private nature of information was well-guarded.

In modern India, the issue of privacy was discussed and debated by the Constituent Assembly while drafting the Constitution for independent India. It was K.S. Karimuddin who pressed upon the inclusion of right to privacy in the Constitution on the lines of Article 4 of the US Constitution, and Article 114 and 115 of the German Constitution which provided similar kinds of rights to their citizens in order to support his proposal.[11]

[7] M. Rama Jois; "*Legal and Constitutional History of India- Ancient Legal, Judicial and Constitutional System*"; (Universal Law Publishing Co, New Delhi, 2010); Pg 490

[8] Ibid

[9] Ashna Asheesh and Bhairav Acharya; "*Locating Constructs of Privacy within Classical Hindu Law*"; (The Centre for Internet Society); Available at https://cis-india.org/internet-governance/blog/loading-constructs-of-privacy-within-classical-hindu-law

[10] S.K. Purohit, "*Ancient Indian Legal Philosophy: Its Relevance to Contemporary Jurisprudential Thought*"; (Deep & Deep Publications, New Delhi, 1994) Pg 145

[11] Sargam Thapa; "*The Evolution of Right to Privacy in India*"; (IJHSSI), Volume 10 Issue 2, February 2021, Pg 53-58; Available at

However, this never materialised as the proposed amendment failed to garner requisite support. The Indian Constitution, therefore, failed to recognise right to privacy as a fundamental right conferred upon citizens of India.

Prior to 2018, the necessity to determine the status of right to privacy was not as pressing in light of its conflict with other laws, as the Courts were always in favour of upholding the validity of the laws which were under challenge. The importance of State surveillance and investigation techniques always prevailed over infringement of privacy. However, in the case of *Justice Puttuswamy v. Union of India*,[12] the need to resolve the status of privacy became increasingly relevant because of the claims of violation of privacy under the implementation of unique biometric identification scheme, commonly known as Aadhaar and also the global development occurring in contemporaneous world became a supplemental factor.[13] Ultimately, after extensive deliberations by the Hon'ble SC in its 685-page long verdict, the court laid the position to rest that Article 21 includes right to privacy. Therefore, any cloud over the status of privacy as a fundamental right has now been removed through this decision, with right to privacy being given the status of a fundamental right.

PRIVACY CONCERNS DURING COVID-19

Dire times call for clever, innovative and often, radical course of action. The COVID-19 pandemic is one such extraordinary and unfortunate event which has led to various actions being undertaken under the Epidemic Diseases Act, 1897 and the Disaster Management Act, 2005 in India. While governments and health workers all over the world are engaged in supressing and controlling the spread of this deadly disease, one of the measures taken to limit the spread is the surveillance of the affected persons in order to prevent and control the spread of the virus. For this purpose, data tracking and analysis have emerged as the unlikely hero.

INDIA'S CONTACT TRACING APP: AROGYA SETU

Social distancing has become the new normal for everyone today, as the presence of the virus has not completely disappeared. The threat of a new wave is still at large and the country has already witnessed the stressful, dreadful and anxious state in the first and the second wave. In such times, people need to stay updated regarding containment zones, virus hotspots and other related information. This is where the Indian application by the name of Arogya Setu comes in handy. It is a contact tracing, syndromic mapping and self-assessment digital service which has been developed by National Information Centre

https://www.ijhssi.org/papers/vol10(2)/Ser-1/J1002015358.pdf

[12] *Justice K.S. Puttaswamy (Retd) v. Union of India*, (2017) 10 SCC 1

[13] V. Bhandari, S. Parsheera and F. Rahman; "A*n Analysis of Puttuswamy: The Supreme Court's Privacy Verdict*"; (SSOAR), 2017; Available at https://www.ssoar.info/ssoar/bitstream/handle/document/54766/ssoar-indrastraglobal-2017-11-bhandari_et_al-An_Analysis_of_Puttaswamy_The.pdf?sequence=1

under the MeitY.[14] Through contact tracing, the app notifies a user of any hotspot or 'high-risk' areas near their residence.[15] In case, the app notifies that the person is present in a hotspot, the user is required to take standard precautionary measures against coronavirus as are prescribed by the medical community. The platform provides a test for self-diagnosis in case they start exhibiting symptoms close to the viral infection. It can then help in gauging whether there is a need to consult a doctor or not. However, in case the self-assessment on the app indicates a strong possibility of COVID-19 infection, the data gets uploaded on the government servers for inspection, use and control.

The application also uses contact tracing to keep a note of all individuals whom a user meets during this pandemic. If the persons in vicinity have contracted COVID-19 symptoms, the app immediately notifies the users of the presence of such person.[16] This is done with the help of GPS and Bluetooth. After installation, the app requires the users to permit Bluetooth and GPS access to the program. With the aid of Bluetooth function, the app will find out all nearby users of Arogya Setu. It will warn the user of the risk due to proximity with a COVID-19 infected person, by scanning through databases of known cases across India. Using the location information, it determines whether the area where the user is present is one where infected person are present. This is done on the basis of data available throughout the country. At the same times, GPS tagging helps in determining the location of the user with precision, every fifteen minutes.[17] All these records are then stored on the phone.

On May 1st, 2020, MHA made it mandatory for all local authorities to ensure 100% coverage of Aarogya Setu app among all the residents in containment zones. Soon, companies such as Swiggy, Zomato, Urban Company, Grofers among others also made it mandatory for their staff working as frontline workers to use the app. Amazon and Flipkart strongly recommended the use of the app for their works. The NCDC recommended the use of the app as mandatory for people entering Delhi. Thus, little choice now remained with the person whether to join the app or not. Joining the app was made synonymous with travelling and safe public dealing. The element of making an informed decision was taken away from the people and it would not be totally incorrect to say that people had to download the app separate from their individual will.

PRIVACY ISSUES UNDER AROGYA SETU

Though on the face of it, data sharing and contact tracing seem to be feasible remedies, privacy issues with respect to the utilisation,

[14] Meryl Sebastian; "*Aarogya Setu's 6 Major Privacy Issues Explained*"; Huffpost.com; Available at https://www.huffpost.com/archive/in/entry/aarogya-setu-app-privacy-issues_in_5eb26c9fc5b66d3bfcddd82f; Accessed on 24.9.2021 at 11.00 AM

[15] Rohin Dubey; "*Privacy in a Pandemic: Is the Aarogya Setu App legal*?"; (Bar&Bench.com); Available at https://www.barandbench.com/columns/privacy-in-a-pandemic-is-the-aarogya-setu-app-legal

[16] Supra Note 14

[17] Tripti Dhar; "*Aarogya Setu- Carrying your privacy in your hands*?"; (IJLTET) Vol 20, May, 2020; Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3614506

storage and sharing of such data remain a pressing concern which is largely unanswered. One of the State's crucial responses to the pandemic has been based on the intrusive use of technology, which seeks to access people's personal health data.[18] While the methods used sound reason, the means at work for implementing the programme ignore major privacy concerns which are intrinsically linked to human dignity. The most alarming among these measures is the use of contact-tracing app which keeps a constant check on the movement of COVID-19 carrier. The aim is obviously to ensure that a person who comes into contact with a carrier can quarantine himself.

Here what becomes even more pressing is that the app is not backed by any legislation like Aadhaar.[19] In such a scenario, the user is not sure to whom his data is going to or where is it being stored and who all can access it. Employers all over are making the use of the app compulsory and are compelling their employees to make use of the app. Thus, the app is becoming a tool of technological invasion into personal liberty as well as privacy of a person, albeit to achieve a greater social and public purpose. But this is without any statutory backing and without any data protection law existing in the country. Moreover, the reach of the application extends throughout the country. It is beyond imagination, the catastrophe which may emerge if the personal data so collected falls into wrong hands and the purposes to which it can be deployed.

- **Legality of making the app mandatory:** As per MIT Technology Review's Covid Tracking Tracker,[20] India is currently the only democratic country all over the world which has made the use of its covid-19 tracking app as mandatory for people.[21] However, this has been done vide executive orders of MHA without any law compelling the use of such app. A legal sanction behind the mandatory use of app is of utmost importance because then, the app will have to satisfy the tests of necessity and proportionality before invading the privacy of its users. It will further provide answers to questions as to all the purposes for which the data is being collected, the time frame for which the data will be stored and the others practices and protocols concerning such data. Such law will have to be clear, specific and unambiguous with respect to the privacy concerns of the users, the basis of infringement if any, the procedural safeguards and other rights of the users. It will have to stand the test of a reasonable and fair law.

Furthermore, in case the mandatory use of the app is made under the authority of law, it will inspire confidence among people, because

[18] Benjamin Boudreaux, Matthew A. DeNardo; "*Data Privacy During Pandemics*"; (Rand Corporation, 2020)

[19] Supra Note 12

[20] Eli Blumenthal; " MIT Tech Review is keeping tabs on coronavirus apps that are tracking you"; Cnet.com; Available at https://www.cnet.com/tech/mobile/mit-tech-review-is-keeping-tabs-on-coronavirus-apps-that-are-tracking-you/

[21] Priyam Jhudele, Shantanu Pachauri; "*Aarogya Setu: An analysis of the Data Access and Knowledge Sharing Protocol, 2020*"; Available at https://www.researchgate.net/publication/342504067_Aarogya_Setu_An_analysis_of_the_Data_Access_and_Knowledge_Sharing_Protocol_2020

then the data collection would have been allowed after following the course of parliamentary debate and discussions. It would have been authorised by the elected representatives of the people who have been given the task of looking after interests of the people who have chosen them. As of today, India lacks a comprehensive data protection law; the privacy bill having not yet been converted into an Act of Parliament. In such a background, such apps are bound to overlook privacy concerns and become a tool for movement control of users.

- **Using GPS and Bluetooth:** Aarogya Setu app makes use of Bluetooth and GPS for the object of tracking a user's movement. This makes the application much more intrusive in comparison to many other apps on our phones. As per the new norms which are announced by the government from time to time, the app allows the government to collect demographic contact, self-assessment data and location data of infected persons or any person in close contact with such infected person.[22] Other apps just collect one data point which is later replaced with a scrubbed device identifies, but Aarogya Setu collects multiple data points for personal and sensitive personal information which increases the privacy risk manifold.[23] For this, the government has replied that the data remains anonymised and scrubbed of personally identifiable details,[24] but activists of privacy rights are pointing to the vague and ambiguous clauses in the privacy policy of the app which can lead to excessive collection and use of sensitive personal data. The concern is for government to prove that the data is anonymised properly. The government has expressed that the privacy policy of the app will not touch anything which falls under the category of anonymised data sets, however, it is not simply a matter of speech.[25] A simple response that something which has been anonymised is no longer personally identifiable will not suffice without showing the citizens as to how this is achieved. Certain level of transparency is required since the vulnerability attached to the amount of information collected through the app has the potential to expose citizens to greater risks.

The app does not specify as to which government departments will gain access to the information obtained through the app, but rather states that the database can be shared

[22] Ibid

[23] Nanen, Vikas Hasija; "*Privacy-Preserving and Incentivized Contact Tracing for COVID-19 Using Blockchain*"; (IEEEIoT) 4(3), April, 2021; Available at https://www.researchgate.net/publication/350601851_Privacy-Preserving_and_Incentivized_Contact_Tracing_for_COVID-19_Using_Blockchain

[24] Viral Nagori, "*Aarogya Setu": The mobile application that monitors and mitigates the risks of COVID-19 pandemic spread in India*"; (JITTC), Vol 11, Issue 2, April 2021; Available at https://journals.sagepub.com/doi/abs/10.1177/2043886920985863

[25] Saurav Basu; "*Effective Contact Tracing for COVID-19 Using Mobile Phones: An Ethical Analysis of the Mandatory Use of the Aarogya Setu Application in India*"; (CUP), November, 2020; Available at https://www.cambridge.org/core/journals/cambridge-quarterly-of-healthcare-ethics/article/effective-contact-tracing-for-covid19-using-mobile-phones-an-ethical-analysis-of-the-mandatory-use-of-the-aarogya-setu-application-in-india/8A902BBEF6722241E28458BB70FC1195

with the government of India and any other agency which is granted access to the data for specific purposes. However, the data sharing with other agencies will remain available only for 180 days after which the data will be deleted. NIC will be responsible for maintaining a list of agencies which will be granted access to such information. The chief executive of MyGovIndia which has developed the app have specified that the information through app will be utilised only for necessary medical interventions.[26] It shall not be used for any other purpose and no third party will be given access to it. However, in grave matters concerning privacy, mere verbal assurance cannot assuage the pangs of doubts that the masses have especially in the upcoming era of pervasive technology.

- **The lifespan of the app and its data systems:** The information collected through the app goes under regular deletion process on a rolling basis. After every 60 days, information of sick individuals and after every 30 days, information of healthy people is deleted. Personal information is removed from the serve after 45 days. Permanent deletion of data occurs after 180 days from the date on which it was collected.[27] Though these facts give some breath of relief to the users, the concerns of the activists is that a user has no means of ensuring if the government has actually deleted the personal information of the users, simply because there is no transparency and no way of inspecting the working of the app. Furthermore, a matter of grave concern is that the government has not stated any time period for which the app shall remain mandatory. There is no period when the government would review the need of the app or delete and ultimately destroy the data collected through the app. In such cases, rumours such as the server of the app might be linked with other government databases, play the role of fanning the flame. Such linking would ultimately increase the risk of a system of permanent surveillance over the masses which creates an image of Orwellian state in the minds of any reasonable person.

- **No liability:** The liability clause in the applications' T&C exempts the government from any form of liability in case of any unauthorised access to the data collected or modification of it takes place. Thus, the government will not be held responsible in case the personal information of the user is somehow leaked. Not only this, the government is immune from liability in case the app provides inaccurate information or shows false cases of COVID-19.[28] Therefore, what remains is that citizens cannot hold the government accountable in case of major breach of their privacy which contains crucial and intimate details. No judicial remedy shall be available against the government. Thus, in case of breach of privacy the fact that who will be responsible has remained unanswered.

[26] Supra Note 62

[27] Rajan Gupta, Manan Bedi; "*Analysis of COVID-19 Tracking Tool in India: Case Study of Aarogya Setu Mobile Application*"; (Digital Government: Research and Practice), Vol. 1, No. 4, Article 28, August 2020; Available at https://dl.acm.org/doi/pdf/10.1145/3416088

[28] Rupali Bandhopadhyay, Arun Gupta; "*Data privacy & Aarogya Setu Covid-19 app*"; (The Times of India), April, 2020; Available at https://timesofindia.indiatimes.com/blogs/voices/data-privacy-aarogya-setu-covid-19-app/

PUBLICATION OF LIST OF PERSONS INFECTED WITH COVID-19

The COVID-19 pandemic exploded in a matter of days and the prevention of its spread left everyone baffled. This became a cause of grave concern because the incubation period of the virus spanned from 7 days to 14 days during which the virus showed no symptoms in the body. Thus, a person could be a covid-19 carrier without even feeling any signs of virus being present in his body. A person could have come in contact with an infected person and could roam around freely for 2 weeks without knowing of the risk to himself and others near him. Keeping this in view, another measure taken to prevent the spread has been to publish the list of infected persons in the area by the administration on their respective websites. For this, the State governments have made use of its powers under the Epidemic Diseases Act, 1897. Various orders have been issued in exercise of powers under the Act. However, this law does not give the State the authority to publicise this information.[29] The decision even though taken for noble purpose, has become a double-edged sword, as it has resulted into lesser people coming to the hospital on showcasing flu like symptoms due to the stigma attached to the disease and to prevent the information of their disease being put in public domain. This has somewhere slowed down the fight against covid.

State government have published list of District wise list of home quarantined people.[30] The list is prepared based on the travel history of individuals to the countries which are under special scanner. It contains information of place of origin of journey, place of final destination, date of arrival in India, date until the person is quarantined in house and the address of the individual. Details of person's name, address, mobile number, start date of quarantine as well as the police station having jurisdiction over the area is highlighted and openly mentioned. Similarly, notices have been pasted outside people's homes who are suspected of having come in contact with a covid-19 patient or if any member of the family has tested positive and who are under an order to remain in isolation.[31] At the very top of the posters, a huge caption of 'Do Not Visit' appears written in bold. This adds to the stigma attached to the disease, which somewhere discourages people with the disease to come forward for help.

[29] Apurva Vishwanath , Abantika Ghosh , Karishma Mehrotra; "*Lists of Covid names raise issues of public health vs private information*"; (The Indian Express), March, 2020; Available at https://indianexpress.com/article/india/coronavirus-names-private-information-privacy-home-quarantine-6336611/

[30] Sanya Kumar, Shrutanjaya Bhardwaj; "*The publication of COVID-19 quarantine lists violates the right to privacy*"; (The Caravan); April, 2020; Available at https://caravanmagazine.in/commentary/covid-19-pandemic-quarantine-lists-right-to-privacy

[31] Soutik Banerjee and Devika Tulsiani; "*Privacy In Times Of Corona : Problems With Publication Of Personal Data Of Covid-19 Victims*"; (The Live Law), March 2020; Available at https://www.livelaw.in/columns/privacy-in-times-of-corona-154360

District administrations are publishing the information of people under quarantine in the area on their websites, along with house addresses and phone numbers of individuals. This is personal data of the people which is being published and made known to everyone at large without their consent. The data which is made available is sufficient to identify and locate the individual. This not only leads to the patients being stigmatised but can also lead to their social boycott or even anti-social activities like lynching. This is highly possible in areas where relations between neighbours are already sensitive either due to caste or religious reasons. These measures are also in direct violation of medical ethics and patient's right to privacy and confidentiality of his medical details.

Any action of government which is infringing the right to privacy of citizens must necessarily pass the 'necessity' test. Thus, prior to publication of such information, the government is look for other possible means to undertake preventive measures which prove effective. Here, even though maintaining a record of persons who have been infected or at risk of infection is necessary to curtail the spread of the virus, but at the same time, publication of details of individuals quarantines does not appear proportionate to the object for which it is being done. It is an executive act without the support of any law and therefore, becomes arbitrary and unreasonable. In order to enforce quarantine and to keep a check on social distancing being practices, the government cannot share data of covid-19 patients in public domain. In India, this becomes highly problematic, given our past with untouchability and the fact that Indians are prone to mob mentality ignoring science and rather bullying the patients.

DATA PROTECTION AND RIGHT TO PRIVACY ACROSS THE WORLD : A GLANCE AT GERMANY'S CONTACT TRACING APP

Germany launched its contact tracing app called Corona-Warn-App in the midst of June, 2020 which is much later in comparison to the rest of the world. The developers of the app made sure that the app remains true to privacy, completely secure and non-discriminatory. A person is shown as infected on the app only if a person has a positive covid result from a lab. There shall be QR code on the lab result which shall be scanned by the person through the app, and in turn the app will send a warning to all the app users in proximity to the infected person for at least fifteen minutes within the last fourteen days.[32] The ones who get the warning on the app, become entitled to a free Covid-19 test and are recommended to self-isolate. The merits of the app are that all contacts are stored in the form of an anonymous, randomly generated ID which ensures the user's privacy.[33] This data is not accessible by anyone, neither the developers nor any

[32] Alina Behne; "*Learnings from the design and acceptance of the German COVID-19 tracing app for IS-driven crisis management: a design science research*"; (BMCMIDM) Article No. 238(2021), August, 2021; Available at https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-021-01579-7

[33] Alessandro Blassimme, Effy Vayena and Agata Ferretti; "*Digital Contact Tracing Against COVID-19 in Europe: Current Features and Ongoing Developments*"; (FDH), June, 2021; Available at https://www.frontiersin.org/articles/10.3389/fdgth.2021.660823/full

third party. There is no central server which collects information about the identities or people's locations. The entire data is encrypted and saved only on user's device. Even the source code of the app was made public by the developers.

With the onset of the pandemic, countries were quick to jump to the wagon to introduce apps to record contact between people in their bid to make the infection traceable and to break its chain. However, Germany took its time. In turn, this has proved to be a good thing to do, as the result of it has been the creation of an app which is very good at protecting and securing private data. Unlike India or China, where the contract tracing app create a complete, visible movement profile of its users and sends it to central government computers, the German app does not detect user location at all. The app does not even attempt to find the location of its user, which means that it cannot become a tool to spy on people. Its only recognise the app users in vicinity to send the warning. This works with the aid of Bluetooth, a wireless mode of exchanging data between devices in proximity to each other. The devices send each other short-term identification numbers, while the actual data is only stored on the user's respective device and that too in an encrypted form. Therefore, even the phone owner cannot view it. This data is further automatically deleted after two weeks.

The data which is stored on the app servers is completely anonymised and is used only to send verification keys and transaction numbers to ensure the secure working of the app.[34] Furthermore, to build public trust in the app and guarantee transparency, the developers have published the source code of the app in advance only. Another excellent feature of the app is the scanning of QR code with the test result through the device. It is only when this is done that the app sends an alert to nearer phones. This helps in ensuring that only alerts of true cases are sent to people and no unnecessary panic and hysteria is created. Thus, no one can trigger a false alarm because only QR Code from the laboratory will lead to release of warning.

Therefore, it can be seen that Germany has served as an example that not all technology needs to be invasive and in conflict with privacy of a person. It is possible to cater to provide for contact tracing to prevent the virus from spreading further but without infringing privacy of anyone. This is certainly an example from which the world can learn for devising future technologies.

CONCLUSION AND SUGGESTIONS

With the advent of Coronavirus pandemic and its terrible toll on human life, the government had to resort to extraordinary measures. To protect the health of the public at large, the government considered it best to place restrictions on movement of people and introduce mechanism of health tracking and reporting. This included contact tracing apps with recording and transmitting of personal health information of people which has scratched the deep-rooted fear of threat to personal data and privacy. Thus, during the pandemic, the government had to balance the two conflicting rights of public health and protecting personal privacy. While it is true that the prime purpose for targeting such information and monitoring is to control the

[34] Supra Note 30

disease, a result of these has been invasion of privacy giving rise to the fear of its misuse.

With this being said, a major takeaway from the Covid-19 pandemic is that the lack of India's privacy protection laws. While legislature sought to enact a new privacy law in 2019, it has not yet seen the light of the day and is confined to the status of a Bill. However, the reality today is that everyone, both the public and the private entities were equally unprepared for the pandemic and had to walk the thin divide between privacy and health. The pandemic has also exposed the shortcomings of the existing GDPR which is considered to be one of the strictest privacy laws ever made. However, believers in the stringent nature of GDPR are of the view that the law is not completely incompetent in dealing with privacy concerns during Covid-19, but is flexible to incorporate all the measures undertaken during this time as well. Under GDPR, the government is allowed to take measures in national interest, and the measures taken to curb the pandemic, are very much covered by the regulations. However, the need is to place limitation on the data which can be accessed. GDPR provides two main principles of data minimizations and purpose limitations and these two guidelines are sufficient to guide the government that as minimum as possible data is to be utilised and accessed and further, the access should be for the sole purpose of curbing the spread and containing the disease.

During the pandemic, many smartphone apps have been launched and introduced to use contact tracing as a tool to contain the spread of the virus, however, this has been done without any prior knowledge of their actual effectiveness. Two years have gone by and we are still not sure as to how far these methods employed by the government have been helpful. Have they worked as intended? Only a rigorous assessment of the effectiveness of digital contact tracing and disclosing the names and address of quarantined and infected people will allow public health benefits to be measured as against its disadvantages to any individual. Therefore, stringent evaluation is needed to discuss and develop contract tracing apps before they are introduced as an accepted and ethical tool to contain any future outbreak of other infectious and contagious disease. It is no secret that mere developing of any such app is not a final solution to the pandemic itself, but is it highly difficult to trace the effectiveness of the apps in actual response to Covid-19.

Given that the international community has started regarding right to privacy and data protection as a fundamental human right, India is also being brought under a moral as well as legal obligation to enact privacy and data protection regulations. Even though the privacy bill is currently pending its approval in the parliament, one mode which can be adopted by the government is that of self-regulation. India can consider encouraging initiative for self-regulating privacy concerns among companies and industries, especially those working in the field of e-commerce. This will offer flexible policy making catering to the specific needs and desires of their customers. It will also be cost efficient for the government, as no enforcement mechanism need to be established. This can be done till a specific legislation is introduced. Countries like USA have primarily taken this approach of self-

regulation in order to protect privacy especially on internet. However, this is in no case an alternative to appropriate legislation. A uniform and effective application of privacy standards is required, which can be introduced through legislation by the parliament.

While introduction of policies for protection of privacy and data is of utmost importance, what should be understood is that the policies must be easily understandable by the common man. Taking consent of individuals whose information is to be gathered is essential and for this purpose, a notice must be given. However, this notice must be in a clear language, which must specify the purpose of data collection, the identity of the data controller, the kinds of third parties with whom the data will be shared, manner in which the organisation collecting and processing the data can be contacted. The choices which are available to the individuals for limiting disclosure of information should be expressly specified and communicated to the subject. Thus, the choice of opting out of having their personal information used in any way which is found to be inconsistent with the purpose of collection and consent so given, must be clearly spelt out.

While data has once been collected, the law must ensure that this data can be transferred further by the data controller only to a party which guarantees compliance with the principles of notice and choice as mentioned above. Another method is that the data controller can enter into a contract with the third party to create obligations to guarantee at least the same level of data protection as the data controller himself. Last but not the least, enforcement mechanisms must be set up to provide adequate remedies and affordable recourse to investigation into complaints and disputes of individuals regarding breach of obligation by data controller to ensure privacy to subjects. There should be simple and easy method of verifying the truthfulness of the statements of the data controller regarding its privacy practices, failure of which should result into severe punishment.

One of the core principles of data protection is transparency. Transparency and fairness in collection of data means being clear, open and honest with the individuals regarding the processes involved in data processing. Thus, the need is to provide information in clear and concise language which can be easily understood by common man. In case information is shared with third party or there is change in the purpose for which the data was collected, all such relevant details must be brought within the knowledge of the individual whose data is involved. A successful privacy and data protection policy must take note of these measures and must live up to these principles.

It is true that the past two years have proved to be difficult and trying times for all of us. The entire world has been shocked and was completely unprepared to meet the pandemic. However, we must not lose sight of the fact that privacy is essential for the autonomy and protection of human dignity. It is the right which forms the foundation of many other human rights. Right to privacy is the freedom and choice with a person against unnecessary intrusion and a choice as to how to interact with the world. Technology has made out lives easier, but technical advancement has also expanded the scope of surveillance and

VOLUME 30 | JUNE, 2022 ISSN 2456-9704

hence, interference with our privacy. In the era marked with technological advancement, the possibility of state surveillance and misuse of personal data is rapidly increasing. Mass interception of communication, locational surveillance, compulsory biometric systems and indiscriminate data retention policies are just the beginning. Therefore, the need of the hour is to regard right to privacy as a highly valuable right and to make stringent laws to ensure data protection.

*****