International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Right to Privacy Vs. Right to Public Health: A Debatable Question of Supremacy

Dr. Rakesh Chandra

Academician

Abstract

Every human being is born free and deserves privacy in the realm of daily life. In India, this right has also been accorded the status of fundamental right. Normally, the right to privacy is the general norm but at the same time this right is not absolute. There are exceptions too to this right, including the right to maintain secrecy about one's own health card. There is no doubt that any person's personal health card is protected by the right to privacy. However, if any of the diseases with which any person is inflicted with, and that disease is contagious or otherwise harmful to society, it whole is of contagious nature that may affect the health of other persons, either of his family or of the surrounding locality, must be brought into public notice as it can affect the people in general. Here, it would be pertinent to note that individual rights can never supersede the public rights. Public health issues encompass the betterment of the public and therefore, the right to privacy of any individual is secondary to any other right. Mr. X vs. Hospital Z is the case in point where the apex court has clearly defined the contours of both the rights. The controversy around the Aarogya Setu during the times of Covid-19 pandemic was also laid to rest on the basis of public health which needs to be protected at all costs. This paper explores the various dimensions of both rights and suggests the way out.

Keywords: Individual Rights, Public Health, Right to Privacy, Contagious Diseases, Balancing of Rights.

INTRODUCTION

Right to public health comes under the purview of fundamental right to life and personal liberty under part four of the Indian Constitution. Though this right is not a fundamental right itself, it is a very significant right in itself. Its importance as a valuable right has drawn the attention of the lawmakers, activists and the legal scholars alike during the COVID-19 pandemic. Whereas the respective governments endeavoured their best to do the needful to provide relief to Corona victims, the superior courts intervened in the favour of the common man if they failed in their duties. Since then, the governments have started paying more attention to strengthening the skeletal healthcare services by providing more funds and devising better schemes for the betterment of health services. One significant aspect of these efforts was shown in the form of digitization of health records of the patients. Not only this but also, the official input of the health centres of the government began to be stored in computerized databases. Prior to that 'large private hospitals have bespoke digital systems and government hospitals have been dragged willy-nilly into maintaining some rudimentary digital capabilities by the good offices of the National Health Mission, a large fraction of Indian citizens' healthcare consultation occur in small private clinics with no real incentive to digitise, thereby

preventing patients and downstream physicians from acquiring an interoperable digital trail of medical records.'[1] This situation changed drastically during and post-COVID period when the computerization of all medical records became an accepted practice. Further, virtual apps like Aarogya Setu also added a lot more data to the existing one already available on the databases of various computer systems in different hospitals, private and government owned. With this enormously available healthcare data came the responsibility to safeguard it from all kinds of misuse and manipulation. Since such data belongs to the patients in general, any leak of data can adversely affect their precious right to privacy.

The second situation arises where the data of a particular patient appears in public domain without getting his consent, either deliberately or inadvertently. That may result in his loss of social prestige or other disadvantages including financial and occupational. Sometimes, the doctors do it purposely in the interest of other people. In both situations, the focus is on whether the right to public health is more important than the people's right to privacy. At this juncture, it would be worthwhile exploring the situation in both cases as such:

1. Aarogya Setu

This is a prominent example of a public healthcare system which involves a tussle between two rights, namely right to privacy and right to public health. The app was launched as the main contact tracing technology endorsed by the Central Government on April 2, 2020, for pan-India use and available in 11 languages. It was developed by the National Informatics Centre under the Ministry of Electronics and Information Technology. The app was used most during the nationwide lockdown imposed by the central government during the COVID-19 pandemic in 2020. By April 2020, it became the most downloaded app globally and crossed 75 million marks. The app was further equipped with additional functionalities such as Prime Minister's Citizen Assistance and Relief in Emergency Situations Fund or PM CARES fund, and hosting e-passes for essential service providers.[2] The app is designed to keep track of other Aarogya Setu users that a person came in contact with, and alert him or her if any of the contacts test positive for COVID-19. The app uses the mobile phone's Bluetooth and GPS capabilities to achieve its purpose. The app is designed to keep a record of all other Aarogya Setu users that it detected nearby using Bluetooth, and a GPS log of all the places that the device had been at 15-minutes intervals. These records are stored on the phone till the time any user tests positive or declares symptoms of COVID-19 in a self-assessment survey in the app. In such cases, the records are uploaded to the servers.[3]

The Privacy policy of the app envisages that the users will be provided with a colour coding of green and yellow based on their self-assistance. Only the user data falling in the yellow category will be uploaded to the server. On the contrary, the green category users' data-purportedly the lower risk group-is retained in the app.[4]

At the time of registering, the app collects a set of personal information such as name, sex, phone number, current location and travel history. This information is further uploaded to government servers, which then generates a unique digital identity for that user. When the Bluetooth of two Aarogya Setu users sniff each other out, the unique digital identity is exchanged along with the time and location of the meeting. In case an app user tests positive, all unique digital identities in his or her records get an alert

[1] RS Sharma and Nisheeth Srivastava, Unlocking medical data's value, The Indian Express, Nov 11, 2025.
[2] P.J. George, What are the concerns around the Aarogya Setu app? The Hindu, April 26, 2020.
[3] Ibid.
[4] Ibid.

on the risk they face and instructions on self-isolation and next steps.[5] On May 11, 2020, the central government issued new protocol for Aarogya Setu data collection which contained following guidelines as such:

- Only data that is necessary and proportionate for health interventions should be collected.
- Contact and location data will remain on the user's data unless it is determined that it must be shared for health responses.
- Data should be stored securely.
- Demographic information remains on servers for 180 days unless user requests for deletion.
- Data can be shared with other government agencies and third parties as long as it is for critical health purposes.
- Universities and researchers can request an anonymized version of this data.

'The Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020' restricts the use of data -such as the information people provide during self-assessment of their health and a record of who they came in contact with- "strictly" to purposes necessary and proportionate for the government's "health responses".[6]

The Supreme Court of India in her historic judgment in K.S. Puttaswamy vs. Union of India (2017) has held that the right to privacy is a fundamental right, but this right is not absolute like other fundamental right which are subject to some reasonable restrictions. There exist circumstances in which this right can be legitimately curtailed. "However, any such restriction, as the Court held in Puttaswamy, must be tested against the requirements of legality, necessity and the doctrine of proportionality. This will require government to show us, first, that the restriction is sanctioned by legislation; second, that the restriction made is in pursuance of a legitimate state aim; third, that there exists a rational relationship between the purpose and the restriction made; and the fourth, that the State has chosen the "least restrictive" measure available to achieve its objective…….In this case, not only are the government's technological solutions unfounded in legislation, there is also little to suggest that they represent the least restrictive measures available. A pandemic cannot be a pretext to abnegate the Constitution."[7] In this context, it may be pointed out that during the pandemic period, there was no separate privacy or data protection law in the country. Even in case of violations of data security protocols by any entity will be punishable under Section 51 to 60 of the Disaster Management Act, 2005, which invites jail terms for up to two years.[8] Therefore, in absence of any legislation regulating the online privacy of Indians, Aarogya Setu users have no better option but to accept the privacy policy provided by the government. As per the policy, "persons carrying out medical and administrative interventions necessary in relation to COVID-19" will have access to the data. According to a working paper from the Internet Freedom Foundation, this "suggests interdepartmental exchanges of people's personal information" and is "more excessive than countries like Singapore and even Israel".[9]

The Aarogya Setu app has been criticized by digital rights activists for its tracing of location histories. In the first week of May 2020, a French computer programmer said that vulnerabilities in the tool's design could allow attackers to access data of millions of Indians.[10] In this connection, India's cyber security

[5] Ibid.
[6] Amrita Madhukalya, Govt issues new protocol for Aarogya Setu data collection, Hindustan Times, May 12, 2020.
[7] Suhrith Parthsarathy, Gautam Bhatia & Apar Gupta, Privacy concerns during a pandemic, The Hindu, Apr 29, 2020.
[8] Amrita Madhukalya, Govt issues new protocol for Aarogya Setu data collection, Hindustan Times, May 12, 2020.
[9] P.J. George, What are the concerns around the Aarogya Setu app?, The Hindu, Apr 26, 2020.
[10] Amrita Madhukalya, Govt issues new protocols for Aarogya Setu data collection, Hindustan Times, May 12, 2020.

agency CERT-In had issued an alert in the first fortnight of May, 2020, saying phishing attacks centred around the government's contact tracing application-Aarogya Setu-are spiking as cyber criminals try to take advantage of the pandemic. Phishing is a cybercrime in which a target is contacted by email, telephone or text message by someone posing as a legitimate institution and is lured into providing sensitive data such as banking and credit card details.[11] However, the government has stated that the app is secure. Seeking to address concerns over privacy and surveillance, the government stated that several measures have been taken to ensure data security. The app had a clear data destruction policy among other measures to make it a safe and secure tool to keep citizens safe. According to Ajay Sawhney, Secretary, Ministry of Electronics and Information Technology, "Location data is used in order to facilitate containment actions and to protect the community. Data for only 30 days is stored on the app and data of positive patients too is deleted from the server 60 days after the date of cure."[12]

Right to Privacy and Right to Health in Reference to Individuals

The Supreme Court of India has held in case of Mr. "X" v. Hospital "Z" (1998) (**1998) 8 SCC 296**), that it was open to the hospital or the doctor concerned to reveal such information to persons related to the girl whom he intended to marry and she had a right to know about the HIV-positive status of the applicant. In this case, the appellant was an Assistant Surgeon Grade I as junior specialist in Nagaland State. He was deputed to accompany his uncle who was a Minister of Transport and Communication to the respondent hospital at Chennai. As the patient was anaemic, the surgery was postponed. The appellant and his driver offered to donate blood and blood samples of the appellant were sent for testing. The appellant was engaged to be married which was scheduled to be held on 12.12.1995. The Minister of Transport and Communication called the appellant's brother-in-law and sister to his residence and informed him that the appellant's marriage was being called off; It was conveyed to him that his blood was tested at the hospital, and it was found to be HIV-positive. This information was furnished to the concerned Minister by a doctor, who was impleaded as a respondent in the case. Therefore, the marriage of the appellant was called off on account of his HIV-positive status by his brother-in-law. The appellant went to the hospital the next day and confirmed his status. He then tried to contact the Director of the hospital to enquire about the unauthorized disclosure by the hospital about his HIV status as he was unable to obtain any information from the management in this regard. Consequently, he was forced to leave Kohima, the capital of Nagaland, as several people including the appellant's own family members and certain other members of the community were now aware of the appellant's HIV-positive status, and he was socially ostracized. Aggrieved by the unauthorized disclosure, the appellant filed a petition before the Commission on the grounds that the hospital had a duty to maintain confidentiality of personal medical information of the appellant. He also sought compensation from the respondents for breach of their duty to maintain the confidentiality of personal medical information of the appellant. The Commission dismissed the petition summarily and directed him to initiate civil proceedings for an appropriate relief. Accordingly, a Special Leave Petition was filed before the Supreme Court. The Court made an order on 21.9.1998 dismissing the said petition. The Court held:

" …..This is apart from, and in addition to, the Fundamental Right available to her under Article 21,

[11] Neeraj Chauhan, Phishing attacks around Aarogya Setu app on the rise, says Cert-in, Hindustan Times, May 17, 2020.
[12] Surojit Gupta, Govt: Aarogya secure, not being used for surveillance, The Times of India, May 12, 2020.

which, as we have seen, guarantees "right to life" to every citizen of this country. This right would positively include the right to be told that a person, with whom she was proposed to be married, was the victim of a deadly disease, which was sexually communicable. Since "right to life" includes right to lead a healthy life so as to enjoy all the faculties of the human body in their prime condition, the respondents, by their disclosure that the appellant was HIV(+), cannot be said to have, in any way, either violated the rule of confidentiality or the right to privacy. Moreover, where there is a clash of two Fundamental Rights, as in the instant case, namely, the appellant's right to privacy as part of right to life and Ms. 'Y's right to lead a healthy life which is her Fundamental Right under Article 21, the right which would advance the public morality or public interest, would alone be enforced through the process of court, for the reason that moral considerations cannot be kept at bay and the Judges are not expected to sit as mute structures of clay in the hall known as the courtroom, but have to be sensitive, "in the sense that they must keep their fingers firmly upon the pulse of the accepted morality of the day". (See: Allen: Legal Duties)"

In another case, Sharda v. Dharampal (2003) (**2003) 4 SCC 493**), the question involved before the Supreme Court was whether a party to a divorce proceeding can be compelled to a medical examination. This question has arisen from a judgment dated 17.11.1999 passed by the Rajasthan High Court at Jodhpur in S.B. Civil Revision Petition No. 1414/99. The parties herein were married according to the Hindu rites. Later, the respondent filed an application for divorce against the appellant under Section 12(1)(b) and 13(1)(iii) of the Hindu Marriage Act, 1955. He filed an application seeking directions for a medical examination of the appellant on 5th May 1999. His application was allowed directing the appellant to submit herself to the medical examination. Aggrieved by the said order, she filed a Revision Petition before the High Court which was dismissed by the impugned judgment. The Supreme Court, in her judgment observed that in para 76 as such:

"Privacy" is defined as "the state of being free from intrusion or disturbance in one's private life or affairs". Mental health treatment involves disclosure of one's most private feelings. In sessions, therapists often encourage patients to identify "thoughts, fantasies, dreams, terrors, embarrassments, and wishes". To allow these private communications to be publicly disclosed abrogates the very fibre of an individual's right to privacy, the therapist-patient relationship and its rehabilitative goals. However, like any other privilege, the psychotherapist-patient privilege is not absolute and may only be recognized if the benefit to society outweighs the costs of keeping the information private. Thus, if a child's best interest is jeopardized by maintaining confidentiality, the privilege may be limited".

The Court finally concluded:

1. "A matrimonial court has the power to order a person to undergo medical test.
2. Passing of such an order by the court would not be in violation of the right to personal liberty under Article 21 of the Indian Constitution".

However, the Court should exercise such a power if the applicant has a strong prima facie case and there is sufficient material before the court. That makes the legal position very clear as to an individual's right to health v right to privacy.

In a recent case of Indrakunwar v. The State of Chhattisgarh, (2023), Criminal Appeal No. 1730 of 2012,[13] the Supreme Court deliberated on the question as to what extent does the right to privacy shield

[13] 2023 LiveLaw (SC) 932.

the matters concerning the personal life of a woman accused of committing a crime, particularly when the prosecution has failed to discharge its duty? Replying to this question, the Apex Court held that "…. Although there is a requirement by law to disclose the aspects required to adjudicate in a criminal matter, such duty cannot unreasonably and unwarrantedly step over the fundamental right of privacy". The Court observed in the judgment that "Privacy enables the individual to retain the autonomy of the body and mind. The autonomy of the individual is the ability to make decisions on vital matters of concern to life……. Privacy is the ultimate expression of the sanctity of the individual. It is a constitutional value which straddles across the spectrum of fundamental rights and protects for the individual a zone of choice and self-determination". The Court allowed the Appeal as such.

Conclusion

The right to privacy of an individual stands on the same footing as to his right to health, broadly coming in the periphery of the Fundamental Right to Life and Liberty under Article 21 of the Indian Constitution. Though the right to privacy is a sacred right, it is not an absolute right. Hence, in some cases the question of primacy of any of these rights arises. The Supreme Court of India has categorically stated in several cases that where some information related to an individual's health may be of concern to another individual's future or to the community at large, such information may be disclosed by doctors and the concerned hospital in public interest. But as a general rule, an individual's right to privacy must be maintained by them in regard to maintaining confidentiality of patients' medical records. At the same time, the concerned medical staff must be sure of the fact that it has become absolutely necessary to divulge the secret and confidential records of the patient to the public at large or to his or her near and dear ones. Undoubtedly, public good is more important than private good. As far as government apps like Aarogya Setu are concerned, it is the prime duty of the government to safeguard patients' data from misuse by anti-social elements in particular. Also, only that data should be secured which is of use for a long period. All unnecessary data should be deleted within the shortest possible time. Now, a specific data protection enactment is available, it can be hoped that the stored medical and health data of individuals will remain safe and secure, and the unscrupulous infiltrators will be severely punished as per the provisions of the law. Lastly, the civil society's active role has to be further stressed in overseeing the implementation of the Personal Data Protection Act, 2023. Active and aware citizenry is needed most in a vibrant democracy.