*Page 761 - 772* **DOI:** *http://doi.one/10.1732/IJLMH.25242*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 3 | Issue 6**

**2020**

# COVID 19 Surveillance: Is Personal Privacy Overlooked?

MARIYA SHAHAB[1] AND NISHANT BHARDWAJ[2]

## ABSTRACT

*Coronavirus surfaced in China in December 2019. Fast forward a few months, it had become a pandemic and WHO named it 'COVID-19'. In an attempt to control this virus, the act of quarantine and the global lockdown has strictly been recommended and ardently followed worldwide. It was also accompanied by digital surveillance to gain accurate ground-level information. WHO also provided guidelines for health-related surveillance. Comprehensive surveillance, Sentinel syndromic surveillance, Hospital-based SARI surveillance, Mortality surveillance, Virological sentinel surveillance, are some of the methods, to name a few. With the advancement of time, voices were heard citing the dangers associated with rising surveillance. The Right to privacy is a fundamental human right under International Law. The Right to Privacy for an individual is the right to keep secrets or obscures elements of their life from the public at large. It is a part of domestic law in many countries. The companies must also provide a way in which customers can review the data collected about them and control their usage. The right to privacy was held to be a fundamental right in India by nine judges of the Supreme Court in the celebrated judgment of K.S. Puttuswamy v. Union of India. However, these rights have been blatantly violated in many jurisdictions by governmental and private bodies. This paper analyses such violations and tests them through the lens of privacy laws. The conclusion is reached that surveillance measures must be least intrusive and should not be at the cost of basic human rights and must be time-bound. States must also ensure that data collected through apps should not leak to the outside agencies and peoples should have a say in their data that how and where it should be used or what they want to do with their data collected.*

***Keywords:*** *Covid-19, Privacy & Surveillance.*

## I. COVID-19: ONSET AND REPERCUSSION

December 2019, a perplexing news story heralded the global media coverage. The city of Wuhan in China was plagued with a novel virus that was gnawing lives in no time. The

[1] Author is a student at Jamia Millia Islamia, New Delhi, India.
[2] Author is a student at Jamia Millia Islamia, New Delhi, India.

 [ISSN 2581-5369]

whole world was alarmed by this fast-spreading unidentifiable virus that started to hit other countries as well. In January 2020, WHO named it COVID-19, and declared it as a pandemic that might result in serious consequences.

As of April 2020, over 210 countries were infected by COVID-19, among which Europe, the USA, and Iran suffered heavily followed by China. In a short period, other countries reported a serious increase in the number of cases as well. 23.4 Million Cases have been recorded to date globally, with the death rate increasing every hour. Due to the lack of precise information about this virus, no treatment or vaccine has gained consent as yet.

In an attempt to control this virus, the act of quarantine and the global lockdown has strictly been recommended and ardently followed worldwide. All the nations took swift actions in this regard and called for a national lockdown for several months. Many countries across the globe ordered complete lockdowns in an attempt to "flatten the curve" of the pandemic.

Such a lockdown meant restricting 2.6 billion people into their homes, putting down trade and businesses, halting every economic activity, and ceasing all the public activities. Moreover, due to the lockdown, hundreds of flights were canceled globally, affecting both trade and tourism. A loss of over 2.44 billion dollars has been reported by Japan and Indonesia.[3]

Factories and industry shutdown massively affected the low earning masses, as around 90% of the global citizen's fall under the low to lower-middle-income scale. "The UN has estimated that over 300 million children who rely on school meals for most of their nutritional and dietary needs might now be susceptible to acute hunger, which could reverse the development made in the past 2–3 years in decreasing infant mortality within a year."[4]

## II. SURVEILLANCE PRACTICES AROUND THE GLOBE

Keeping in view such a grim situation, experts from the global community are undertaking intensive research, and drafting new effective strategies to stabilize the situation. Pandemic surveillance is one such practice to trace and counteract widespread diseases. It is a crucial element to ensure public health. It helps in obtaining precise ground-level information, assists in designing need-based strategies, and helps in forecasting possible outcomes. "The type of surveillance for a particular disease relies upon the attributes of that disease and the

[3] Raghuvir keni, Anila Alexender, Pawan Ganesh Nayak, Jayesh Mudgal, and Krishnadas Nandakumar, *COVID- 19: Emergence, Spread, Possible Treatments, and Global Burden*, *Frontiers*, Frontier in Public Health, (Aug 25, 2020, 4:40 PM), https://www.frontiersin.org/articles/10.3389/fpubh.2020.00216/full

[4] Richard Cash and Vikram Patel, *Has COVID- 19 subverted global health*, The Lancet, (Aug 25, 2020, 8:24AM), https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(20)31089-8/fulltext

objectives of the immunization program."[5]

The World Health Organization provided an updated guideline on 7th August 2020 for carrying out Public health surveillance for COVID-19. It provides strict recommendations to its member states with regards to the regulations to be followed. The WHO Report also enumerates essential actions to be undertaken for effective COVID-19 surveillance, "use, adapt and strengthen existing surveillance systems; strengthen laboratory and testing capacities; use, adaptation and, enhancement of public health workforce to carry out case finding, contact tracing and, testing; include COVID-19 as a mandatory notifiable disease; implement immediate reporting, and establish systems to monitor contact tracing activity."[6]

Further, WHO demands a daily, as well as weekly data collection, through extensive testing and case reporting by the member countries and to trace the pattern of the spread. It also updates and assists in providing revised methods of data collection and scrutiny for facilitating and ensuring regular surveillance. COVID-19 surveillance at every level is carried out largely by keeping travel records of every citizen, tracing the movement of people, as well as scrutinizing all the medical records. Besides this, other countries are also coming together in practicing continuous surveillance. The European Union and the European Economic Area have drafted techniques to trace widespread transmission and executed robust public health and safety measures to control and prevent any further COVID-19 cases.

The technical report '*Strategies for the surveillance of COVID-19*' issued on 9th April 2020 aims to "reconcile data needs for effective pandemic response"[7] EU/EEA calls for a routine surveillance system under which several surveillance setups are required. Comprehensive surveillance, Sentinel syndromic surveillance, Hospital-based SARI surveillance, Mortality surveillance, Virological sentinel surveillance, are some of the methods, to name a few. The procedure of collecting samples for the reporting of the cases has been practiced throughout the countries following this guideline.

Moreover, a qualitative indicator checklist is provided to gauge the impact of COVID-19 on the healthcare system, to ensure the effective functioning of hospitals and medical institutions. These are "the number of confirmed cases and deaths among healthcare workers and their proportion among healthcare workers overall and those working in dedicated

[5] *Types of Surveillance*, World Health Organization, (Aug 25, 2020), https://www.who.int/immunization/monitoring_surveillance/burden/vpd/surveillance_type/en/.
[6] *Public Health Surveillance for COVID-19: Interim guidance*, World Health Organization, (Aug 25, 2020, 9:15 AM), file:///C:/Users/lapi/Downloads/WHO-2019-nCoV-SurveillanceGuidance-2020.7-eng.pdf.
[7] *Strategies for the surveillance of COVID- 19*, European Centre for Disease Prevention and Control, (Aug 25, 2020, 9:32 AM), https://www.ecdc.europa.eu/sites/default/files/documents/COVID-19-surveillance-strategy-9-Apr-2020.pdf.

 [ISSN 2581-5369]

COVID-19 hospitals/treatment centers; sick-leave numbers among healthcare workers overall and in dedicated centers; the COVID-19-related bed occupancy in hospitals overall, dedicated centers, ICUs and HDUs, beds with ventilators; the mean number of days' worth of private protective equipment left before depletion of stock; and the proportion of long-term care facilities, with a minimum of one case of COVID-19 among staff or residents or with increased mortality."[8]

The Government of India has ordered the adoption of resilient surveillance strategies to counter COVID -19 spread. The Government of Kerala took timely initiatives through "active surveillance, setting up of district control rooms for monitoring, capacity-building of frontline health workers, risk communication and strong community engagement, and addressing the psychosocial needs of the vulnerable population are some of the key strategic interventions implemented by the state government that kept the disease in control."[9]

Moreover, countries with higher economic status are quickly adapting these strategies with the assistance of advanced technologies, that are not only assisting in swift functioning but also reduced human labor investment. Face recognition technology, thermal imaging equipment, proximity tracing, and the ubiquitous CCTV installation to trace movements are a few examples of efficient technology.

However, the advent of comprehensive tracking of individuals through technology is accompanied by the dangers of violation of privacy. The famous dialogue from *Spiderman,* namely, "with great power comes great responsibility" explains the way this situation needs to be dealt with. Let us not examine some of the dangers associated with excessive surveillance so that we can study its necessity and possible improvements.

## III. THREATS APROPOS SURVEILLANCE

Unlike the 90s Spanish Flu epidemic, COVID-19 has been tackled with unparalleled medical, scientific, and technological apparatus. This means that world Governments have vested more focus and power to these institutions to practice surveillance to fight COVID-19. The technological domain has gained the utmost leverage in this regard. The impact of such easy access is that data about everyone could have more serious consequences in the near future.

The Human Rights Watch highlighted the different ways in which Governments are tracing geolocation and proximity data from mobile phones and other digital devices that are causing

[8] *Id.*
[9] *Responding to COVID- 19 Learning's from Kerala,* World Health Organization, (Aug 25, 2020, 10:15 AM), https://www.who.int/india/news/feature-stories/detail/responding-to-covid-19---learnings-from-kerala.

 [ISSN 2581-5369]

high risk to privacy rights globally. In certain countries, it has been reported that authorities suggested health advisory information along with personal data of COVID-19 patients. These activities have alarmed experts as it violates medical privacy. "It does not fulfill the conditions required for surveillance to be lawful and therefore is a violation of the right to privacy."[10]

Moreover, Deborah Brown of Human Rights Watch stated that "Some restrictions on people's rights could be justifiable during a public health emergency, but people are being asked to sacrifice their privacy and switch over personal data for use by untested technologies."[11] These surveillance measures raise concerns regarding the collection and sharing of personal information for purposes other than health care and medical safety.

Though surveillance practices are a prerequisite to counter, monitor, and control the pandemic situation, it is equally important for the Government to provide strict criteria for limiting surveillance strategies. They should be able to display that actions executed are legally sound and are vital, effective, and time-bound. Along with this, they must also ensure transparency and legal monitoring to build a sustainably secure society.

Having enumerated some of the dangers associated with excessive surveillance, it is now expedient to have a look at privacy regimen around the globe first, and then in India specifically, so that we can hold ground reality against the lens of the law.

The Right to privacy is a fundamental human right under International Law. The Right to Privacy for an individual is the right to keep secrets or obscures elements of their life from the public at large. Article 12 of the UDHR, Article 17 of ICCPR, and Article 11 of the American Convention of Human Rights discuss the Right to Privacy. Article 12 of UDHR and Article 17 of ICCPR states an almost similar definition of the Right to Privacy that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attack upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks". On the other hand, the right to privacy as stated in Article 11 of the American Convention of Human Rights is similar to the definition given in UDHR and ICCPR with the addition of a sentence "Everyone has the right to have his honor respected and his dignity recognized."

In the U.S., questions related to protecting privacy against threats of government surveillance

[10] *COVID- 19, surveillance and the threat to your rights,* Amnesty International, (Aug 25, 2020, 1:12 PM), https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/.
[11] *COVID- 19 Apps Pose Serious Human Rights Risks,* Human Rights Watch, (Aug 25, 2020, 2:25 PM), https://www.hrw.org/news/2020/05/13/covid-19-apps-pose-serious-human-rights-risks.

 [ISSN 2581-5369]

is discussed in the Fourth Amendment, which guarantees that "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated . . . .".[12] Although the Fourth Amendment applies only to governments and their agents but under the established doctrine, a private person can also be subjected to Fourth Amendment regulation to the extent it is acting as an agent of the state.[13]

In the United Kingdom, the Regulation of Investigatory Powers Act, 2000 governs the provision for surveillance and investigation by government bodies. Regulation of Investigatory Powers Act gives guidelines to the public authority such as governmental departments or police in case they require getting any private information. Earlier, in Europe, there was no direct law as such to govern surveillance, and the members of the EU use guidelines of the UK's Regulation of Investigatory Powers Act.[14] But later, the draft European General Data Protection Regulation (GDPR) was introduced by the council in Europe which regulates the processing of personal data within the European Union which took effect on May 25, 2018, requiring that people know, understand, and consent to the data collected about them shifting the balance of powers towards consumers by giving them the upper hand on what to do with the personal data collected about them.

One of the main provisions of GDPR requires companies to inform customers about the kinds of data that are collected from their devices, along with the ways in which it might be used. This includes names, addresses, locations, etc. The companies must also provide a way in which customers can review the data collected about them and control their usage. The law protects individuals of the 28 member countries of the European Union, whether or not the data is processed elsewhere.

## IV. COVID 19 AND PRIVACY REGIMEN IN INDIA.

Let us now shift our focus to the privacy regimen in India. The Indian constitution guarantees a fundamental right to privacy. The right to privacy was held to be a fundamental right by nine judges of the Supreme Court in the celebrated judgment of *K.S. Puttuswamy v. Union of India*[15] which states that the right to privacy is a fundamental right under Article 14, 19, and 21 of the Constitution of India and also the same should not be infringed unless the same is necessary for protecting the sovereignty and integrity of the state.

However, the same court, after a year, completely changed its character in the case of the

[12] U.S. Const. amend. IV.
[13] Natalie Ram & David Gray, *Mass surveillance in the age of COVID-19,* JLB, Jan- June. 2020.
[14] Ashok Kumar Kasaudhan, *Surveillance and right to privacy: Issue and challenges,* IJL, 2017.
[15] (2017) 1 SCC 10.

*Aadhaar* judgment[16]. It upheld Aadhaar-PAN linkage and allowed the unique number to be used for government schemes and subsidies making it compulsory for those who seek to receive any subsidy, benefit, or service under the welfare scheme of the government expenditure whereof are to be met from the Consolidated Fund of India but struck down the most mandatory private use of Aadhaar.

In India, there are mainly two legislations that regulate digital and telephonic surveillance, i.e., *Information Technology Act, 2000,* and the *Indian Telegraph Act, 1885*. Section 5 of The Indian Telegraph Act empowers the Central and State government to intercept messages during two instances. First, in the occurrence of any public emergency or the interest of public safety, and secondly, if it is considered necessary or expedient to do so. Other than the above two points, messages may also be intercepted, in the interest of the sovereignty and integrity of India, the security of the State, public order, friendly relations with foreign states, and for the prevention of incitement to the commission of an offense.[17]

Further, *Rule 419A* was incorporated in the *Indian Telegraph Rules (1951)* in 2007 and last amended in 2014 framed under the Indian Telegraph Act. These Rules provide that "*Directions for interception of any message or class of messages under sub-section (2) of Section 5 of the Indian Telegraph Act, 1885 (hereinafter referred to as the said (Act) shall not be issued except by an order made by the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India and by the Secretary to the State Government in-charge of the Home Department in the case of a State Government."* The Rule also provides that "*In unavoidable circumstances, such order may be made by an officer, not below the rank of a Joint Secretary to the Government of India, who has been duly authorized by the Union Home Secretary or the State Home Secretary, as the case may be".*

Similarly, the *IT Act, 2000* widely regulates the interception, monitoring, decryption, and collection of information on digital communications in India. More specifically, *section 69* of the *IT Act, 2000* authorized the Central Government and the State Governments to issue directives for the monitoring, interception, or decryption of any information transmitted, received, or stored through a computer resource.

However, in December 2019, Personal Data Protection Bill, 2019 was introduced in the parliament, which is the first cross-sectoral legal framework for data protection in India

[16] Justice Puttaswamy (Retd.) and Anr. v. Union of India and Ors., (2019) 1 SCC 1.

[17] Shashwat singh, *Surveillance in India Post the Right to Privacy Judgment,* Legal Service India, (Aug. 28, 2020, 3:31 PM), http://www.legalserviceindia.com/legal/article-2273-surveillance-in-india-post-the-right-to-privacy-judgment.html

 [ISSN 2581-5369]

making a drastic change in data collection and processing practices in India. The PDP Bill is meant to improve data handling and data privacy in a way that is similar to the European Union's GDPR allowing consumers the right to access, correct, and erases their data after the same is processed for the purpose for which it was meant.

These provisions adequately summarize the privacy regimens around the globe and specifically in India. In this light, we shall now examine the ways in which these laws are being allegedly violated by surveillance practices of various states. This shall be achieved by comparing laws and ground realities side by side.

Digital surveillance is being established for contact tracing, to administer quarantines, to assess general trends on how the virus might be spreading, or to determine the effectiveness of "social distancing," among other reasons. However, a rise in state digital surveillance powers, such as obtaining access to mobile phone location data, impose severe restrictions on people's freedoms, including to their privacy and other human rights in ways that could reduce trust in public authorities subverting the effectiveness of any public health response.

Different countries have adopted different ways to keep track of their citizens, which in one or another way infringed the rights of the people. Even some of the critics point that the current increase in surveillance by the different states post-COVID would give unlimited authority to the executives, permanently opening the doors to more invasive forms of snooping later.

Civil Libraries experts say that it is a lesson Americans learned after the terrorist attacks of Sept. 11, 2001. Even today, two decades later, law enforcement agencies have access to higher-powered surveillance systems, like fine-grained location tracking and automatic face recognition technologies which can be repurposed to further political agendas.[18] Surveillance measures must be the least interfering available to attain the desired result but they have to not do more harm than good. Though public-private collaborations can provide necessary creative solutions to cope with health crises, governments are taking the help of surveillance companies with deeply worrying human rights records.

For instance, controversial surveillance vendors Clearview AI and Palantir are reportedly in discussion with US authorities. The Israeli surveillance company NSO Group, which has a history of selling to abusive governments, is now selling an enormous data analysis tool

[18] Natasha Singer and Choe Sang-Hun, *As Coronavirus Surveillance Escalates, Personal Privacy Plummets,* N. Y. Times, March 23, 2020.

 [ISSN 2581-5369]

which claims to trace the spread of the disease by diagramming people's movements.[19]

In South Korea, government agencies are hitching up surveillance camera footage, smartphone location data, and credit card purchase record to assist to trace the recent movements of coronavirus patients and establish virus transmission chains. Similarly, In Lombardy, Italy, the authorities are examining location data transmitted by citizens' mobile phones and In Israel, the country's internal security agency is assured to start using a cache of mobile phone location data. In many of the cities of China, the government is making obligatory for citizens to use the software on their phones that automatically categorized each person with a color code red, yellow or green indicating contagion risk. While in Singapore, the Ministry of Health has posted information of each coronavirus patient online, even exceptional details, including relationships with other patients.[20]

Many countries have launched a smartphone app for citizens to assist the authorities to locate people who may have been exposed to the virus. Like in India, the government has introduced the Arogya *Setu* app and Singapore has introduced the TraceTogether app tracing the people's location. However, in most of the cases, not only are the government's technological solutions have no strong foundation in legislation, but there is also little to suggest that they exhibit the least restrictive measures available. However, especially in India, the government's technology solution which seeks to utilize people's health data to fight the COVID does not meet minimum legal requirements. While the measures deployed prima facie sound reasonable, the mediums employed in implementing the program fails to look at important concerns relating to the rights to human dignity and privacy.

Moreover, technology has been used at three levels. First, in creating an inventory of persons suspected to be infected with COVID-19 were State governments have channeled the Epidemic Diseases Act of 1897; secondly, in establishing geo-fencing and drone imagery to monitor compliance by quarantined individuals, which is unsanctioned; and third, through the use of contact-tracing smartphone applications, like AarogyaSetu.[21]

However, the drones deployed also do not appear to have any visible registration or licensing. Indeed, many numbers of the model are simply not permitted to be used in India. While cell-phone based surveillance might be credible under the Telegraph Act of 1885, but until now the orders authorizing surveillance have not been published.

---

[19] *COVID-19, surveillance and the threat to your rights*, Amnesty International, (Aug 28, 2020, 9:30 PM), https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/.
[20] Supra note 16.
[21] Surith Parthsarthy, Gautam Bhatia and Apar Gupta, *Privacy Concern during Pandemic*, The Hindu, April 29, 2020.

 [ISSN 2581-5369]

The most concerning amongst the measures invoked is the use of contact-tracing applications as its establishment is not backed by legislation. Like Aadhaar, it increasingly seems that the application will be used as an object of coercion. There have already been reports of employees of both private and public organizations being compelled to download the application. Also, much like Aadhaar, AarogyaSetu is framed as a necessary technological intrusion into personal privacy, in a bid to achieve a larger social purpose. But without a statutory framework, and in the absence of a data protection law, the application's reach is boundless.[22]

## V. SUGGESTIONS

The global community understands that in these troubled times, some drastic measures need to be taken to get the situation under control. However, such measures, including surveillance, should not come at the cost of violating basic human rights. Utmost diligence must be utilized while using technological innovations for tracking people.[23]

Instead of aggressive tracking of people which is sometimes not necessary, technology should be used to save lives by spreading information about good practices during the pandemic period, as ignorance about the disease, prevention methods, and cure is also widespread. This will also increase public confidence in the technology surveillance regimen. It must be remembered while implementing the policies that human rights never cease to exist, even during pandemics. States around the globe must not throw caution to the wind while implementing the policies of surveillance and other restrictions. Civil society must call upon the governments to take the following necessary steps before moving ahead.

First, governments must introduce only time-bound surveillance measures. That is, the public should be informed about its end date. This applies to the currently active plans as well. This will ensure that surveillance powers are not carried forward by the governments even when they are not necessary.

Secondly, the principle of proportionality must be remembered at all times. The measure taken to pacify a situation must not be more powerful than what is necessary for the situation. This directly means that the measure should also be lawful and should be such that is absolutely in the given circumstances. Also, world leaders should regularly interact with the public via the media to explain the measures taken.

[22] *Id.*
[23] Human Rights, Article 19, (Aug 25, 2020, 4:12 PM), https://www.article19.org/resources/covid-19-states-use-of-digital-surveillance-technologies-to-fight-pandemic-must-respect-human-rights/.

 [ISSN 2581-5369]

Thirdly, it must be ensured that while analyzing big data, all biases towards minorities and weaker sections in a country must be removed as it has been observed that sometimes, they have been ignored or misrepresented in large databases. And if such data is shared with other entities, the agreement must be based on the same principles that the government uses while analyzing the data. Data is a very powerful tool in the technological era. It can be used for either purposes, construction, or destruction. States must ensure that the data collected through applications like AarogyaSetu is not leaked to any outside agencies. Even within the government, the use of this data should only be to better respond to the COVID situation.

Elaborating on the previous point, it must be stated that the governments must take extra efforts while protecting people's data in these times. Since the people are already worried about the big data being created, they might panic at the occurrence of even a minor incident, which might result in their stopping to provide any data altogether. This situation will be far more dangerous as controlling COVID is next to impossible without data.

Lastly and most importantly, while framing any new measures for dealing with the pandemic, civil society should also be given a role in the drafting process to cater to the democratic values. All actions should be open to public scrutiny and surveillance should be removed or minimized when the public opinion is against it.

## VI. CONCLUSION

At present many countries are relaxing their lockdown even though the number of cases is increasing rapidly. But experts from around the globe are researching and drafting new strategies to stabilize the situation. WHO has also suggested public health surveillance to regulate the spread of COVID-19. Further, it also has demanded daily as well as weekly data collection to trace the pattern of the spread of the virus.

Different countries are adopting different methods of surveillance to counter the spread of COVID – 19. But there is a danger of violation of the Right to privacy because of the surveillance and contact tracing. Many countries are using cell-phone based surveillance and many others are using applications to trace the location of people and in most cases, government technologies have no strong foundation in legislation, which could lead to serious consequences in the future.

Some of the restriction on the people's privacy could be justifiable during the public health emergency but switching over the personal data for use to the untested agencies raise concerns, especially in the countries which do not have any data protection law. Like in India, it has Data Protection Bill, 2019 but does not have any data protection law to safeguard the

 [ISSN 2581-5369]

people's data.

There is a concern related to the current increase in surveillance as it would permanently open the door for more invasion of privacy as it happened after the 2011 attack in America that even today law enforcement agencies have access to the surveillance system, location tracking, and face recognition.

Thus, surveillance measures must be least intrusive; it should not be at the cost of basic human rights and must be time-bound. States must also ensure that data collected through apps should not leak to the outside agencies and peoples should have a say in their data that how and where it should be used or what they want to do with their data collected.

*****

 [ISSN 2581-5369]