Legitimising Mass Surveillance through a Pandemic: The use of Aarogya Setu app in India

The Indian government developed the *Aarogya Setu* (meaning health bridge) app a year ago as a contact tracing technology to deal with the spread of the coronavirus pandemic and it was claimed to have crossed 50 million downloads in only 13 days. The app uses Bluetooth and GPS services of a phone to track a user, their medical and travel history, and map their contacts, noting that it evaluates their risk of infection through such mapping. While the app was released for voluntary use initially, there were soon directives making it a mandatory download across offices, some educational institutes and for travel purposes and the decisions around it have since swayed. However, a major question with regard to the app has been about data privacy, security and possibility of using it to surveil citizens. Had its mandatory provision continued, it would have been a roadblock for users demanding the erasure of their data from it. Internet Freedom Foundation, a digital rights organisation, referred to the app as a "privacy minefield," one that lacked transparency and accountability and could very well be a permanent fixture of the state's surveillance architecture. A year later, when the pandemic is causing unprecedented devastation in India with the country reporting the highest ever daily numbers, Aarogya Setu – that continues to exist in a legislative void – was back in the news again. This time, a court while granting bail to a political prisoner directed that he install the app, an implicit reference to the surveillance the app puts the person under.

The questions that an app like this raises relate especially to how the tropes of medicine, care, health can be put to use to allow people to 'consent' to such technology that challenges self-determination. When the app collects GPS data, it goes against data minimization practices, rather emerges as a tool of mass surveillance. Now it becomes important to think through such practices where the state induces fear of a pandemic, uses the language of care, love and concern for the citizenry to legitimize such interventions. This is especially crucial in contexts where people are already subjected to violence, for example Kashmir in the case of India's military occupation. Interestingly, when the pandemic set in, a bureaucrat in Kashmir proudly claimed how they had been using "remote heat maps, phone tracking, crowd sourcing apps, ATM usage" to track down "suspects" who had been hiding their travel histories. The language – suspects, tracking down, using of informants – reflects India's counter-insurgency manual. In addition, instead of questioning how this was done without legal backing and how it interfered with privacy, the media hailed the bureaucrat as Sherlock Holmes. Of late, it also came to the fore how data from the Aarogya Setu app had been shared with the police in Kashmir, which is known to be an oppressive force with documented human rights abuses against Kashmiris. As Saiba Varma (2020), a medical anthropologist, puts it, what India's occupation of Kashmir has brought forth over the decades is a close proximity of militarism and care, how "medicine was not just a remedy for violence but part of its repertoire… in a state of occupation, military and medical infrastructures were co- imbricated, physically and symbolically." These intersections are visibilised more strongly in a pandemic where public health becomes the alibi for extension of technology to surveillance, and one that has the potential to continue unabated post the pandemic. This also blurs the lines between crisis and non-crisis situations. In the Indian context largely, perhaps, the Personal Data Protection Bill 2019, yet to be enacted, could help minimize some privacy concerns around such apps. As Patnaik and Pratap (2020) argue, an important aspect is the *right to be forgotten,* for data erasure. However, for people whose relationship with the state is centred on violence, who continue to be at the margins, and for whom it is often lawlessness institutionalized through the law itself that renders them devoid of rights, one is left to wonder how to think through trustworthy data spaces or what such legislations can achieve, even as the collective is largely sceptic of powerful states finding loopholes in the policy to continue strengthening the surveillance architecture.