DGN Policy Brief 08

December 2020

internet
democracy
project

Data
Governance
Network

Anchored by IDFC Institute

Protecting Bodies and Rights in Disease Surveillance during COVID-19 in India

Radhika Radhakrishnan

Surveillance is increasing control over bodies of individuals, and the framework of data as a resource is facilitating this control, as illustrated here through the case of COVID-19 in India. Data governance frameworks view data as a disembodied resource, erasing its connections with people's bodies and making surveillance seem innocuous. A feminist bodies-as-data approach enables embodied harms of surveillance to be pinpointed, and recommendations to be made to alleviate them. Drawing upon research of lived experiences of marginalised communities whose voices are often left out in data protection discourse, this policy brief proposes recommendations preserving not just data privacy, but bodily integrity, autonomy, and dignity of individuals.

Context

On the one hand, data has played a key role in providing statistical insights into the COVID-19 pandemic in India, such as reporting the number of cases to mobilise public health resources and enabling communications. On the other hand, data has enabled surveillance when in the hands of powerful family members, communities, and the state. Various surveillance measures have been put into place to contain disease spread such as contact tracing, geofencing and door-to-door surveillance apps, drone patrolling, tracking mobile data of people, and requiring mandatory digital forms of identification to access essential services and rights. While surveillance is commonly carried out during health epidemics, its nature determines how it is experienced by people. The data-as-resource framework that is dominantly used within data governance policies conceptualises data as a disembodied asset, the worth of which depends on human ability to extract it, opening it up to possibilities of human exploitation. When surveillance is carried out within such a framework, this research shows that it is experienced as control over not just the data, but also the bodies of individuals. Instead, we propose a feminist approach that accounts for the interconnections between people's bodies and their data and helps us pinpoint specific embodied harms that arise from violations of data.

Main arguments

- As discussed above, departing from the dominant data-as-resource approach, a feminist embodied approach highlights power relations and social contexts that surveillance occurs within. This brings to light specific harms of surveillance during COVID-19. While the understanding of these harms may be different in each case, what is common is that putting bodies back into the picture makes embodied harms visible.

- First, surveillance reproduces inequalities within homes, communities, and through the state.
  - Within homes, access to data (mobile phones, Internet) is controlled by powerful family members through surveillance. This results in an inability to report domestic violence for women and impacts sex workers' ability to earn livelihoods from home.
  - For some marginalised communities, inequalities lead to stigmatisation during COVID-19, promoting surveillance of their bodies through data. This happens through information collected about them by state apps and digital disinformation campaigns targeting them. Since data is viewed as a truth-teller, surveillance legitimises prejudices about them, preventing them from accessing physical spaces, sometimes extending to violence.
  - State surveillance exacerbates inequalities within homes and communities. The state's geofencing and home quarantine apps extend its surveillant gaze into the home.[1] Some apps encourage communities to report each other for violating state orders, legitimising surveillance of marginalised communities by dominant communities who are more likely to have access to such apps, and furthering inequalities

between them.

- Second, surveillance during COVID-19 results in mobility restrictions in public spaces. While this may curb disease spread, it is being implemented through criminalisation without understanding social contexts. Drones and mobile location tracking are used to discipline physical bodies to stay at home without an official being present. However, people do sometimes need to step out of their homes, for example for emergencies, especially during a health pandemic. In such cases, people have reported hiding to avoid being caught by drones, and leaving their phones behind to physically sever the connection between bodies and their data and to, thus, avoid being tracked through their data.

- Third, measures to facilitate access to essential services and rights which may not be intended as surveillance, have the effect of surveillance by imposing social control through data. Aadhaar and Aarogya Setu are mandatory digital requirements and identity proofs which collect data about individuals and profile them into categories that often don't reflect their physical realities. Yet, these digital identities are given precedence over corporeal identities, and these inflexible categories hamper people's autonomy to make decisions about their lives, becoming a form of control. This results in their exclusion from accessing state services and rights such as healthcare, employment, pension, ration, and travel.

- If epidemiological surveillance is required to control the pandemic, it should ensure that the bodies and rights of people are protected. While data is helpful in providing insights on safety, it cannot itself keep people safe. Individuals and communities are resisting surveillance during COVID-19, but on a structural level, there are limitations to resistance when surveillance takes unprecedented datafied forms. We must incorporate feminist ethics of care and build mutual trust between the state and communities to prevent structural harms pointed out here.

Policy recommendations

1. **Policies responding to COVID-19 that aim to protect personal data and data privacy must be broadened to respond to the embodied harms pointed out here, to ensure that individuals retain control over not just their data, but also their datafied bodies.**

2. Access to mobile phones and the Internet is often restricted for women within the home. Thus state helplines and WhatsApp numbers[2] for domestic violence survivors during COVID-19 aren't accessible to many women. **Accessible non-technological alternatives should be made available to women to report domestic violence.**

3. Digital disinformation relies on taking data out of its original context to target marginalised communities. Even if this data may not be collected to exercise control, the bodies of those targeted are harmed in material ways.[3] This is because data exists within social contexts that are already prejudiced against them, and disinformation fuels these prejudices. **Social media platforms should incorporate fact-checking of posts and flag posts that may contain disputed claims or may be misleading.**

4. The state has introduced various measures to encourage community vigilantism, from state apps[4,5] that help communities report each other for violating state orders to community policing[6,7] with untrained community members from dominant communities. **Community policing cannot be carried out within an already discriminatory criminal justice system, and while these constraints remain, dominant communities should not be given access to data and tools that can surveil and harm marginalised communities.**

5. The state has released public surveillance lists containing personal data (names, addresses, phone numbers) of people suspected to be in the vicinity of COVID-19 hotspots which they tracked through their mobile location data.[8] Some people on these lists denied being in these locations, and expressed high levels of trauma and anxiety due to social consequences of being publicly (and in some cases, wrongly) identified. **If collected for tracking the spread of disease, personal data of people should not be made publicly available.**

6. Karnataka's Quarantine Watch app requires selfies to be shared to verify that people are following quarantine orders. This extends the state's surveillance gaze within the home,[9] and is especially concerning for women and other minorities for whom sharing private images with the

state could lead to slut-shaming, voyeurism, and predatory actions. **Data which may put some groups at risk, and that is not strictly necessary to contain the spread of the pandemic (such as selfies) should not be collected. Data collection should also be limited when there are other means of inferring the same information (such as whether a person is following home quarantine orders) that do not require the collection of intrusive images.**

7. Punjab's Ghar Ghar Nigrani app was made mandatory for ASHA workers for door-to-door surveillance.[10] This research found that smartphones and digital training were not provided to ASHA workers, and they were not financially compensated for the extra time invested in learning to use the app. Some workers also faced violence by people who did not want them to collect their data.[11] **Apps should not be mandated for use by ASHA workers, and if they are used, workers should be provided with smartphones and digital training, and should be monetarily compensated for the time spent on it.**

8. The Jharkhand Corona Sahayata App requires that inter-state migrants register with their selfie, bank account details, and Aadhaar number.[12] This research finds that migrants failed to receive financial support through the app due to technical errors causing failed registrations. **Apps should not be made mandatory for people to receive money from social protection schemes, and accessible non-technological alternatives should be made available to transfer benefits.**

9. The requirement of Aadhaar at hospitals for COVID-19 tests and for accessing rations and pensions[13],[14] caused many people to lose out on their entitlements during the health pandemic; some lost their lives.[15] Similarly, the government of India's app Aarogya Setu was made mandatory for accessing the Indian railways, private airlines, and metro travel, as well as for central government and industry employees.[16] Due to concerns around privacy and accessibility, worker unions opposed the linking of their livelihoods to an app, as this research showed. **Digital requirements such as Aadhaar and Aarogya Setu should not be mandatory for accessing essential services and rights during COVID-19.**

10. People interviewed for this research expressed fear of drones and a lack of knowledge about why drones were deployed in their localities. **"State should ensure that the people that are affected or may be impacted should be informed about the nature, purpose and implications of the use of this technology."**[17]

11. **If surveillance is to benefit people and keep them safe, then safety measures, and not data collection, should be at the heart of surveillance practices.** Safety measures should include providing safety gear to all workers and not criminalising violations.

This policy brief is based on research carried out for the paper: Radhakrishnan, Radhika. (2020). *"I took Allah's name and stepped out"*: Bodies, Data and Embodied Experiences of Surveillance and Control during COVID-19 in India. Mumbai, Data Governance Network. https://datagovernance.org/report/i-took-allahs-name-and-stepped-out-bodies-data-and-embodied-experiences-of-surveillance-and-control-during-covid-19-in-india

Endnotes

1) Datta, Ayona. (2020). Self (ie)-governance: Technologies of intimate surveillance in India under COVID19. *Dialogues in Human Geography*, 2043820620929797.

2) NCW launches WhatsApp number to report domestic violence during COVID-19 lockdown (2020, April 10). *The Economic Times*. https://economictimes.indiatimes.com/news/politics-and-nation/ncw-launches-whatsapp-number-to-report-domestic-violence-during-covid-19-lockdown/articleshow/75082848.cms?from=mdr

3) Ghosal, Aniruddha, Saaliq, Sheikh &, Schmall, Emily. (2020, April 25). Indian Muslims face stigma, blame for surge in infections. *AP News*. https://apnews.com/article/ad2e96f4caa55b817c3d8656bdb2fcbd.

4) Government of Rajasthan. (2020). *RajCovidInfo Mobile App* [PDF] (p. 9). https://jhunjhunu.rajasthan.gov.in/content/dam/doitassets/Jhunjhunu/Corona/RajCovaInfo%20Mobile%20App_10Apr20.pdf.

5) Malhotra, Vanshika. (2020, April 10). Swachhata-MoHUA app: Use this app to complain about Coronavirus lockdown violation, get food on Android, iOS. *India TV News*. https://www.indiatvnews.com/technology/apps-mohua-swachhata-app-report-coronavirus-lockdown-violation-how-to-download-android-ios-how-to-use-606340

6) Vigilantism mars community policing. (2020, May 27). *The Hindu*. https://www.thehindu.com/news/cities/Kochi/vigilantism-mars-community-policing/article31682455.ece

7) Poovanna, Sharan. (2020, July 15). Covid-19: Bengaluru police invite citizens to help in community engagement. *Livemint*. https://www.livemint.com/news/india/covid-19-bengaluru-police-invite-citizens-to-help-in-community-engagement-11594803235737.html

8) In New Delhi in March 2020, a religious congregation was organised by the Tablighi Jamaat, an Islamic missionary movement, in the Nizamuddin Markaz Mosque; it was attended by more than 9,000 missionaries. The Indian government claimed that this event caused the largest spike in COVID-19 cases in India, though this claim was disproved. See Ellis-Petersen, Hannah, & Rahman, Shaikh Azizur. (2020). Coronavirus conspiracy theories targeting Muslims spread in India. *The Guardian*. https://www.theguardian.com/world/2020/apr/13/coronavirus-conspiracy-theories-targeting-muslims-spread-in-india ; and Das, Gaurav. (2020, March 31). As Assam Gets First COVID-19 Patient, 'Nizamuddin List' Violates Privacy of Many. *The Wire*. https://thewire.in/rights/assam-coronavirus-nizamuddin-list.

9) Datta, Ayona. (2020). Self (ie)-governance: Technologies of intimate surveillance in India under COVID19. *Dialogues in Human Geography*, 2043820620929797.

10) Capt launches 'Ghar Ghar Nigrani' app for Covid surveillance (2020, June 13). *The Hindustan Times*. https://www.hindustantimes.com/chandigarh/capt-launches-ghar-ghar-nigrani-app-for-covid-surveillance/story-Z2iID0go6AmMTOO1Q175HJ.html

11) Coronavirus: ASHA workers endure abuse and assault on field. (2020, April 22). *Deccan Herald.* https://www.deccanherald.com/national/west/coronavirus-asha-workers-endure-abuse-and-assault-on-field-828525.html

12) Government of Jharkhand. (n.d.). *COVID-19 Help*. http://covid19help.jharkhand.gov.in/.

13) Dash, Sweta. (2020, August 29). Aadhaar-induced exclusion from the PDS is making poor go hungry in Odisha; universalise PDS, demand activists. *Gaon Connection*. https://en.gaonconnection.com/aadhaar-induced-exclusion-from-the-pds-is-making-poor-go-hungry-in-odisha-universalise-pds-demand-activists/

14) Dhara, Tushar. (2020, August 21). Cancelled ration cards deprived Telangana's poor of food rations amid lockdown. *Caravan*. https://caravanmagazine.in/government/cancelled-ration-cards-deprived-telanganas-poor-of-food-rations-amid-lockdown

15) Bengaluru hospitals demand Aadhaar details, patient dies. (2020, August 18). *The New Indian Express*. https://www.newindianexpress.com/cities/bengaluru/2020/aug/18/bengaluru-hospitals-demand-aadhaar-details-patient-dies-2184858.html.

16) Ranjit, Tanisha (2020b). *When and where is Aarogya Setu mandatory? We're keeping track*. The Internet Democracy Project. https://internetdemocracy.in/2020/05/aarogya-setu-tracker/

17) Jain, Tripti (2020). Submission in response to the Draft Unmanned Aircraft System Rules 2020. *Internet Democracy Project*. https://internetdemocracy.in/reports/submission-in-response-to-the-draft-unmanned-aircraft-drone-rules-2020/

Data Governance Network

The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy. At DGN, we work to cultivate and communicate research stemming from diverse viewpoints on market regulation, information privacy and digital rights. Our hope is to generate balanced and networked perspectives on data governance - thereby helping governments make smart policy choices which advance the empowerment and protection of individuals in today's data-rich environment.

About Us

The Internet Democracy Project works towards realising feminist visions of the digital in society, by exploring and addressing power imbalances in the areas of norms, governance and infrastructure in India and beyond.

Acknowledgments

I am grateful to Anja Kovacs for her guidance and support during this work.

About the Author

Radhika Radhakrishnan is a feminist researcher working at the Internet Democracy Project on the Bodies and Data Governance project. She has a Master's degree in Women's Studies from the Tata Institute of Social Sciences, Mumbai, and a Bachelor's degree in Computer Science Engineering from M.S. Ramaiah Institute of Technology, Bangalore. She previously worked with the Centre for Internet and Society (CIS) as a Programme Officer, with the Internet Governance Forum (IGF) of United Nations-DESA as a Consultant on Gender, and with the Women's Rights Programme of the Association for Progressive Communications (APC). She writes, speaks, and hosts podcasts on gender, sexuality, technology, and politics, and tweets at @so_radhikal.

Disclaimer and Terms of Use

The views and opinions expressed in this paper are those of the author and do not necessarily represent those of the Internet Democracy Project.