THE COVID-19 LAW AND POLICY CHALLENGE:

PUBLIC HEALTH VS. INDIVIDUAL PRIVACY IN THE AGE OF CYBER SURVEILLANCE

JAMAL AZIZ | AYESHA MALIK | NOOR FATIMA IFTIKHAR

RESEARCH SOCIETY OF INTERNATIONAL LAW

ABSTRACT

Cyber-surveillance is increasingly being used by desperate governments seeking to curb the rising figures of those infected with coronavirus. States are investing in and rolling out smartphone apps to track citizens' movements, trace locations and map outbreaks in a bid to tackle COVID-19. While not without its benefits, the proliferation of cyber surveillance raises important concerns regarding health rights and privacy of ordinary citizens. This paper explores these concerns and the legality of these measures as well as the issues with their particular application in the Pakistani context.

INTRODUCTION

As States around the world struggle with rising figures of those infected with coronavirus, they are increasingly turning to cyber-surveillance. The use of surveillance to collect data is gaining traction as a useful way to combat the virus in some countries, through information sharing, tracing movements of infected patients or to enforce quarantine. The proliferation of cyber surveillance through smartphone apps to monitor and map the outbreak brings with it a range of challenges and opportunities. This paper will explore the ways in which these measures use personal location data to ensure contact tracing via dissemination of health alerts, the use of surveillance in selected countries including via big data and artificial intelligence (AI), the legality of these endeavours, and issues with their particular applicability in Pakistan.

1. What is Contact Tracing?

When dealing with infectious diseases, public health officials often turn to contact tracing as a strategy for tracking down potential patients, who may or may not be carriers of the disease. The strategy was used extensively in the Ebola crisis in West Africa, and is conducted in tandem with case finding (surveillance) and case investigation processes.[1] In COVID-19, this is critical as the virus has evolved to spread rapidly.[2] It takes on average between six to fourteen days for an infected patient to develop symptoms. In an alarming number of cases, statistics show that those infected can even remain asymptomatic, and thus be carriers despite showing no symptoms.[3] Contact tracing upon case detection and speedy implementation of isolation measures is thus crucial to stemming the spread of COVID-19.[4]

2. Process of Contact Tracing[5]

[1] World Health Organization, Emergency Guideline – Implementation and Management of Contact Tracing for the Ebola Virus Disease (September 2015) https://apps.who.int/iris/bitstream/handle/10665/185258/WHO_EVD_Guidance_Contact_15.1_eng.pdf;jsessionid=0F836B3C1FE835FA6EE2603225884742?sequence=1

[2] World Health Organization, Questions regarding COVID-19. Accessed 8 April, 2020 https://www.who.int/news-room/q-a-detail/q-a-coronaviruses

[3] Center for Evidence-Based Medicine (CEBM), COVID-19: What proportion are asymptomatic?, April 6, 2020. https://www.cebm.net/covid-19/covid-19-what-proportion-are-asymptomatic/

[4] Junaid Nabi, COVID-19: What the evidence so far means for containment, World Economic Forum, April 1, 2020 https://www.weforum.org/agenda/2020/04/covid-19-containment-suppression-strategy/

[5] Understanding Contact Tracing, World Health Organization. Accessed 8 April, 2020 https://www.who.int/features/qa/contact-tracing/en/

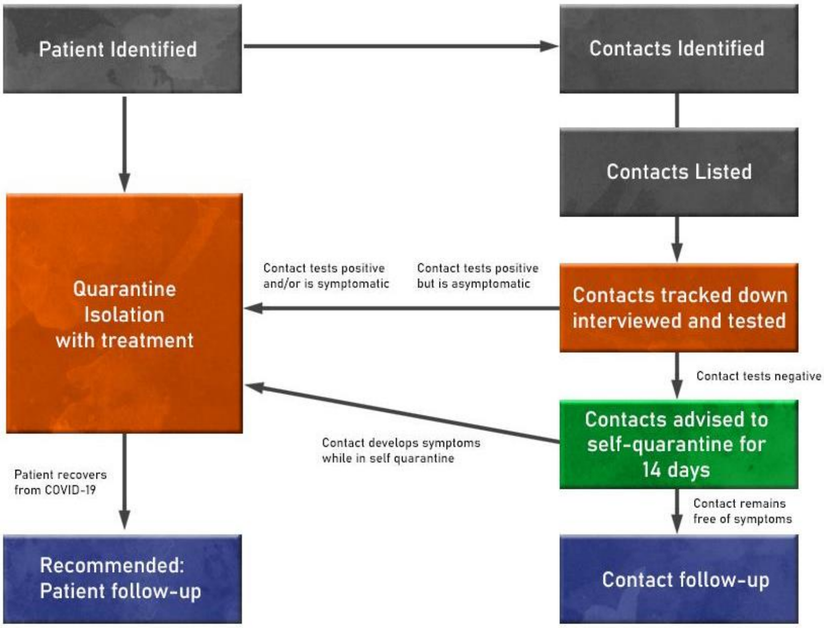
The detection of an infected patient activates the case investigation process, immediately after this, contact tracing commences. Once a patient has been detected, the WHO lays out three stages to undertake contact tracing:

Stage 1: Contact identification: The patient's contacts are identified by asking about the former's activities and roles of the people around them since the onset of illness. Contacts can be anyone who has been in contact with an infected person: family members, work colleagues, friends, or health care providers.

Stage 2: Contact listing: All persons considered to have contact with the infected person should be listed as contacts. Efforts should be made to identify every listed contact and to inform them of their contact status, what it means, the actions that will follow, and the importance of receiving early care if they develop symptoms. Contacts should also be provided with information about prevention of the disease. In some cases, quarantine or isolation is required for high risk contacts, either at home, or in hospital.

Stage 3: Contact follow-up: Regular follow-up should be conducted with all contacts to monitor for symptoms and test for signs of infection.

Contact Tracing for COVID-19[6]


Patient Identified
Contacts Identified
Contacts Listed
Quarantine Isolation with treatment
Contact tests positive and/or is symptomatic
Contact tests positive but is asymptomatic
Contacts tracked down interviewed and tested
Contact tests negative
Contacts advised to self-quarantine for 14 days
Contact develops symptoms while in self quarantine
Patient recovers from COVID-19
Contact remains free of symptoms
Recommended: Patient follow-up
Contact follow-up

[6] In practice, once contacts are identified and listed, they should be interviewed by medical professionals or other relevant authorities and tested for COVID-19. In cases where contacts are symptomatic, they should be treated as a patient and transported to the designated quarantine/isolation centers. In cases where a contact tests positive, but is not symptomatic, there remains a chance that the contact will continue to transmit disease and may even develop symptoms later, requiring treatment – thus, they will also be labelled as a patient, and taken to quarantine/isolation.

In cases where contacts are tracked down but test negative for COVID-19 initially, they will still be asked to remain home and self-isolate for 14 days. During this time, the contact may develop symptoms later, in which case they must be tested and if positive, quarantined or isolated with treatment options. If the contact continues to remain symptom-free after self-quarantine, then it is clear that they did not contract COVID-19. Authorities should conduct tests and ensure through follow-ups the status of these contacts, and react to any deterioration of the situation accordingly.

Chart Modified to fit COVID-19 Context
World Health Organization, Emergency Guideline – Implementation and Management of Contact Tracing for the Ebola Virus Disease (September 2015) https://apps.who.int/iris/bitstream/handle/10665/185258/WHO_EVD_Guidance_Contact_15.1_eng.pdf;jsessionid=0F836B3C1FE835FA6EE2603225884742?sequence=1

3. From Digitizing Contact Tracing to Cyber Surveillance

In a bid to contribute to contact tracing, a range of options have been devised that can be used to keep track of patients' and contacts' movements to control the spread of COVID-19. Digitizing this response has led to the creation of specific smartphone apps, or gathering of information via mobile data, telecom networks, Bluetooth or big data/AI.[7] The purpose of these tools can range from managing and enforcing quarantines, to conducting follow-ups with contacts digitally.

Privacy International, in its continued study and analysis of COVID-19 measures around the world, has identified the following needs regarding data collection with respect to the pandemic outbreak:[8]

- In early stages of dealing with the pandemic, quick and effective contact tracing is required to curb the spread. This requires the use of data that illustrates interaction, proximity and precise locations of individuals when tracking their field of movements. This will give information regarding who interacted with who else, where and when precisely – all of whom will be contacted later as part of contact tracing.

- In the containment phase, tracing is not the highest priority and instead, physical distancing is more valued. In this phase, data can be used to

[7] Derek Thompson, The Technology that could free America from Quarantine, The Atlantic, April 7, 2020 https://www.theatlantic.com/ideas/archive/2020/04/contact-tracing-could-free-america-from-its-quarantine-nightmare/609577/

[8] COVID-19 Response Overview of Data and Technology, Privacy International. Accessed 8 April, 2020 https://privacyinternational.org/key-resources/3547/covid-19-response-overview-data-and-technology

monitor, develop policy, and for authorities to enforce lockdowns and quarantines, including tracking movement of people who violate rules and/or gather with others when specific gatherings are outlawed. In this scenario, location data to track fields of movement becomes priority.

- In the later phases, contact tracing may again be required once more to re-establish connections with former patients and/or contacts in a bid to follow up, as well as to ensure the enforcement of home quarantines and other mechanisms. Like the first stage, all manner of interactions, proximity to other people and location data will be collected and utilized for these purposes.

Once this data is collected, it is analyzed in the second phase through various data management tools, including big data and artificial intelligence (AI).

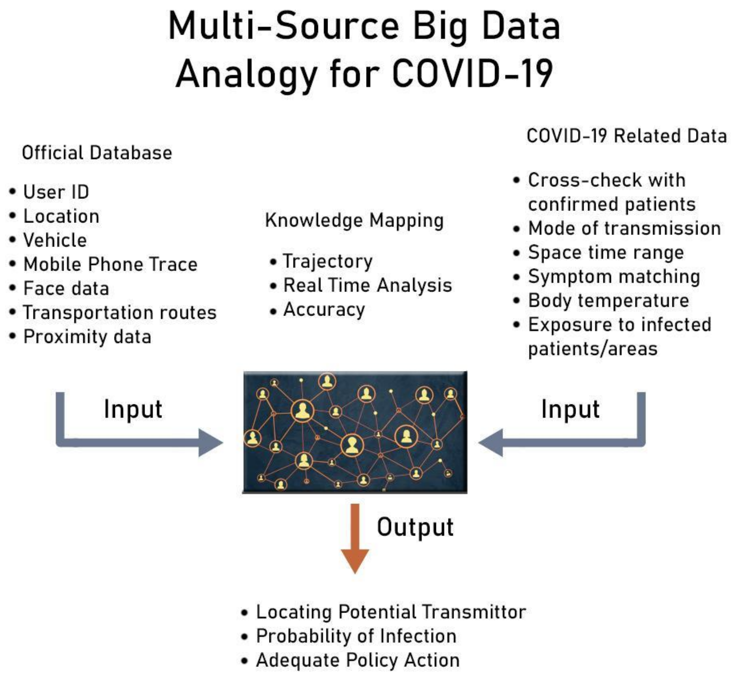
4. CYBER SURVEILLANCE AND BIG DATA/AI

These tools are used to organize, collate, interpret, and use the mass of data gathered through apps, telecom networks, or Bluetooth, and used for effective outcomes.

Big data is defined as the range of tools that analyze, systematically extract information from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing application software.[9]

[9] Big Data and Global Development – SAS Analytics https://www.sas.com/en_us/insights/articles/big-data/big-data-global-development.html

The mass of information gathered using such tools, including structured and unstructured data, are analyzed to determine correlations, generate trends and organize information that normal processing tools cannot handle.[10] With pandemics like the novel coronavirus, these tools have been tailored to serve as excellent sources of information, aiding both policy-making and enforcement, as illustrated below.[11]



However, employing big data and AI to counter the pandemic means understanding the scope of these complex technologies and the feasibility of using such methods in developing and lesser developed country contexts.

[10] What is Big Data? Oracle Pakistan https://www.oracle.com/pk/big-data/guide/what-is-big-data.html
[11] Sridhar Gandhi, How Digital Infrastructure can help us through the COVID-19 Crisis, World Economic Forum, 1 April 2020. https://www.weforum.org/agenda/2020/04/digital-infrastructure-public-health-crisis-covid-19/

5. KEY COUNTRIES USING CYBER SURVEILLANCE FOR CORONAVIRUS

5.1. Contact Tracing

Health authorities and district offices in South Korea have been sending out 'safety guidance texts' to the public, detailing the movements of those recently diagnosed with the virus.[12] They do not specify the names of those diagnosed but do give out some personal information such as gender and age. The country has also created a publicly available map of location data from individuals who have tested positive.[13] Some of this information sharing has negatively impacted some businesses visited by infected people before they were diagnosed.[14]

In Israel, Prime Minister Netanyahu has recently passed an 'emergency decree' to allow the Israel Security Agency to deploy surveillance technology normally reserved for terrorists to track coronavirus patients.[15] An app called 'The Shield' shares a user's location data with the health ministry, whilst the ministry promises the information shared is secure, there are worries that the terms of use are far-reaching and allow too much information sharing.[16]

[12] Barrie Sander and Luca Belli, Opinio Juris, April 1, 2020, COVID-19 Symposium: COVID-19, Cyber Surveillance Normalisation and Human Rights Law, http://opiniojuris.org/2020/04/01/covid-19-symposium-covid-19-cyber-surveillance-normalisation-and-human-rights-law/

[13] Future of Privacy Forum, A Closer Look at Location Data: Privacy and Pandemics, March 25, 2020, https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/

[14] Barrie Sanders (supra n.13)

[15] Financial Times, *Yuval Noah Harari: the world after coronavirus*, March 20, 2020 https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75?segmentid=acee4131-99c2-09d3-a635-873e61754ec6

[16] BBC News, Live Update available at: https://www.bbc.com/news/live/world-52026908

India has launched an app called Aarogya Setu (translates to bridge to health) which uses Bluetooth and location data to tell users if they have been within 6 feet of someone infected and are at risk.[17] The app also shares the data with the government. The data shared with the public is anonymised so the name or number of the individual will not be made public. However, the app does collect this information as well as the individual's gender, travel history and whether they are a smoker.

Germany may track the spread of coronavirus by asking users to voluntarily download an app.[18] If a person becomes infected, the app will automatically send a push notification to anyone they have crossed paths with in the past two weeks, to warn them of the risk of infection. This approach focuses on attempting to inform persons that they have interacted with an infected person and encourage them to act appropriately, for instance, by self-quarantining. Germany's Federal Commissioner for data protection has, however, assured citizens that the data would be stored for a limited and clearly defined period in order to fight the pandemic after which it will be deleted.[19]

5.2. Big Data/AI

In East Asia, a range of cyber surveillance methods involving big data and artificial intelligence (AI) were employed to counter COVID-19. China was

[17] See BBC Live Updates at https://www.bbc.com/news/live/world-52130552

[18] The Local, Privacy-mad Germany turns to app to track coronavirus spread, April 2, 2020, https://www.thelocal.de/20200402/privacy-mad-germany-turns-to-app-to-track-virus-spread

[19] Ibid

"closely monitoring people's smartphones, making use of hundreds of millions of face-recognising cameras, and obliging people to check and report their body temperature and medical condition", which allowed them to quickly identify coronavirus carriers and track their movements and everyone they came into contact with.[20] Mobile apps even warned citizens about their proximity to infected patients. A new system called Health Code assigns users colour codes (green, yellow, red) based on travel history, time spent in infection hotspots and potential exposure to virus carriers, and then shares this information with the police.[21] A 'bad' red score means you cannot use public transport to go to work or school.[22]

Thermal scanners installed at various subway transit points in China and Taiwan[23] not only actively monitored passengers' temperatures, but also employed facial recognition software to aid in identifying them, and automatically notifying their contacts if they exhibited symptoms.[24] CCTV footage was used in tandem to track fields of movements of individuals under quarantine. Telecom companies have been providing "travel verification reports" to employers, based on an employee's location data and local travel

[20] Financial Times, *Yuval Noah Harari: the world after coronavirus*, March 20, 2020 https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75?segmentid=acee4131-99c2-09d3-a635-873e61754ec6

[21] Opinio Juris, COVID-19 Symposium: COVID-19, Cyber Surveillance Normalisation and Human Rights Law, Barrie Sander, April 1, 2020, https://opiniojuris.org/2020/04/01/covid-19-symposium-covid-19-cyber-surveillance-normalisation-and-human-rights-law/

[22] NBC, COVID-19 tracking data and surveillance risks are more dangerous than their rewards, March 20, 2020, https://www.nbcnews.com/think/opinion/covid-19-tracking-data-surveillance-risks-are-more-dangerous-their-ncna1164281

[23] Big Data helps Taiwan Fight Coronavirus, Spectrum, March 2020 https://spectrum.ieee.org/the-human-os/biomedical/devices/big-data-helps-taiwan-fight-coronavirus

[24] How China is using AI and Big Data to Combat the Coronavirus, Al Jazeera, March 2020 https://www.aljazeera.com/news/2020/03/china-ai-big-data-combat-coronavirus-outbreak-200301063901951.html

history charted over 14 days leading up to the Chinese Lunar Year to track intra-state spread of the disease.[25] These are separate from the data gathered through voluntarily-installed smartphone apps, or unknowingly monitored through data usage by telecom companies around the world.

Google and Apple have also announced a rare collaboration, where they would integrate contact-tracing programming into smartphones' operating systems so that no third-party apps need to be installed for the purpose.[26] Implementing this would allow these companies to effectively trace and follow-up with more than one third of the global population to tackle COVID-19.[27]

6. PUBLIC HEALTH V. INDIVIDUAL PRIVACY

The use of bio-surveillance to track people's movements and communications in order to contain the spread of the coronavirus has given rise to concerns that this may lead to unnecessary incursions into the right to privacy. Whilst technology has an important role to play in a global effort to save lives through the dissemination of health messages, awareness campaigns and also increased access to healthcare, heightened surveillance may also threaten privacy in ways which could degrade trust in governments.[28]

[25] Ibid.

[26] Apple, Google team up to 'Contact-Trace' the Coronavirus, New York Times, April, 2020 https://www.nytimes.com/2020/04/10/technology/apple-google-coronavirus-contact-tracing.html

[27] Ibid.

[28] Joint Civil Society Statement: States use of digital surveillance technologies to fight pandemic must respect human rights, April 2, 2020, https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight

Citizen's personal data is being used to guide policy, contact trace, and enforce lockdowns. The increasingly intrusive means by which this is being done, including through phone records, CCTV, and temperature checkpoints, lends credence to worries of a panopticon which may never be rolled back.[29] In order to ensure that there is not an unnecessary and disproportionate erosion of our right to privacy, there must be oversight and regulation of the measures employed to curb the rate of infection.[30]

This is even more important given that many laws are currently being passed by decree as elected legislatures are unable to sit and hold votes, even emergency ones. These laws are far-reaching and new rules may not be time limited. The expansion of powers which curtail our digital rights is also alarming given the extent to which individuals are online at the moment. With a quarter of the world's population in some form of a lockdown, we are working, socialising, and engaging almost solely online.

This is the first pandemic of this scale that the world has seen, and therefore while exceptional measures are justified, they cannot unnecessarily and disproportionately violate rights to privacy. The UN High Commissioner for Human Rights has emphasized that 'human dignity and rights need to be front and [center]' in the effort to combat the spread of coronavirus.[31] The issue is the appropriate level of interference in the right to privacy that can balance the benefits to public health with continued respect for human rights.

[29] Nani Jansen Reventlow, *Why COVID-19 is a Crisis for Digital Rights*, April 16, 2020, https://ilg2.org/2020/04/16/covid-19-and-the-digital-rights-crisis/

[30] Ibid

[31] OHCHR, *COVID-19: States should not abuse emergency measures to suppress human rights – UN experts*, March 16, 2020, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E

7. Is it Legal?

International human rights law allows for States to make limitations so long as it is provided by law, undertaken in pursuit of a legitimate aim (such as public health), and are necessary and proportionate to the achievement of that aim. The International Covenant on Civil and Political Rights (ICCPR) identifies legitimate aims which include national security, public safety and public health as grounds for limiting – by law and when necessary and proportionate to such aims – a number of rights. These rights include the right to privacy (Article 17), the freedom to manifest one's religion or belief (Article 18), freedom of expression (Article 19), freedom of assembly and association (Articles 21-22) and freedom of movement (Article 12). Therefore, any measures taken by states which limit rights under the Covenant must be adopted by law, with the legitimate aim to protect public health and are necessary and proportionate.

The Siracusa Principles of 1985[32] also detail criteria by which limitations and restrictions on human rights can be lawful requiring that they be:[33]

- provided for and carried out in accordance with the law;
- based on scientific evidence;
- directed toward a legitimate objective;
- strictly necessary in a democratic society;

[32] UN Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28 September 1984, E/CN.4/1985/4

[33] Opinio Juris, *COVID-19 Symposium: Human Rights in the Time of COVID-19–Front and Centre*, Sam Zarifi and Kate Powers, April 6, 2020, https://opiniojuris.org/2020/04/06/covid-19-human-rights-in-the-time-of-covid-19-front-and-centre/

- the least intrusive and restrictive means available;
- neither arbitrary nor discriminatory in application;
- of limited duration; and
- subject to review.

The last criterion is crucial and will be increasingly difficult as courts shut in the face of the pandemic. The need for legislation to be subject to review may be enabled by the use of remote courts which can handle litigation and cases through video conferencing.

For cyber-surveillance to be a legal limitation to the right to privacy, a law must be passed in order to allow for it, and the aim it pursues must be legitimate. Further, it has been demonstrated by the scientific community and public health experts that measures to limit social contact are required to limit the spread of the coronavirus. Therefore, laws that deprive individuals of their liberty or privacy in order to enforce these limits may be considered adequate in this situation, and are not arbitrary under Article 9 as well as, not prohibited under Article 17.

This is supported by case law for instance in *Big Brother Watch and Others v. the UK*, the European Court of Human Rights (ECtHR) held that 'the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation'.[34] According to the Court, this interception regime constituted 'a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime.'

[34] *Big Brother Watch And Others v. The United Kingdom*, 58170/13, [2014] ECHR 178

States can also derogate from treaties. Article 4 of the ICCPR allows for derogations in times of public emergency threatening the life of a nation. However, several provisions cannot be derogated from including the right to life, the probation on torture, slavery, and the freedom of religion. The right to privacy and freedom of expression, however, are derogable rights. Nevertheless, derogations must only be to the extent that they are strictly required.[35] However, a state's ability to conduct cyber-surveillance is provided for under the limitations regime without having to resort to derogations.

7.1. Pakistan's Legal Framework on Privacy and Cyber-Surveillance

The right to privacy is enshrined in Pakistan's Constitution under Article 14(1), which states that "the dignity of man and, subject to law, the privacy of home, shall be inviolable."[36] That said, there are provisions justifying conducting cyber surveillance by the Pakistan Telecommunications Authority (PTA) on the directives of the federal government, usually in the interest of national security (Section 54).[37] There are concerns that this wide exception to the right to privacy in the Constitution may be prone to abuse.[38]

8. Implementing Big Data in Pakistan

[35] See Human Rights Committee's General Comment No. 29 (at para. 5)

[36] The Constitution of the Islamic Republic of Pakistan – National Assembly http://www.na.gov.pk/uploads/documents/1333523681_951.pdf

[37] Section 54, Pakistan Telecommunication Authority (Re-organization) Act, 1996 (XVII of 1996)

[38] State of Privacy in Pakistan, Privacy International https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan

With a population of 220 million, 70% internet penetration, and cell-phone usage at 165 million,[39] there is tremendous potential for big data and AI analytics in terms of sheer data generation. Currently, private telecom companies, multinationals and local banks are amongst some of the biggest users of such software and analytics technologies in Pakistan primarily to serve business interests.[40]

At the government-level, certain departments have invested in and utilized such software in a bid to enhance public policy decision-making. National Database and Registration Authority (NADRA) for example, has been working with the US-based data analytics powerhouse, Teradata, to identify population demographics, support intelligence and formal investigations, amongst other uses.[41] Similar initiatives were also taken by the Federal Board of Revenue (FBR) to identify tax evaders through AI technology, increase efficiency, speed and accuracy in tax auditing as well as identify potential tax payers to widen the tax net.[42]

The recently launched Ehsaas Emergency Cash Program, is also an important example. Launched to ease the financial burden on 12 million families, the program blended eight databases to ensure that the poorest demographic, such as daily wage-earners who are acutely affected by COVID-19, would

[39] Telecom Indicators, Pakistan Telecommunication Authority (December 2019) https://www.pta.gov.pk/en/telecom-indicators

[40] Tech Expert Dives into Big Data Potential in Pakistan, Express Tribune, July 2016. https://tribune.com.pk/story/1151447/telecommunication-tech-expert-dives-big-data-potential-pakistan/

[41] Ibid.

[42] GOP to use Big Data and AI to Find Tax Evaders, Samaa TV, October 2018. https://www.samaa.tv/news/2018/10/pakistan-government-to-use-big-data-and-ai-to-find-tax-evaders/

receive cash handouts, amounting to nearly Rs 144 billion.[43] This illustrates political will to move towards such technologies, and a potential for implementing these for cyber surveillance purposes to counter the novel coronavirus.

9. Issues with Cyber-Surveillance

Despite the plethora of benefits brought about by cyber surveillance technologies – there are issues concerning its usage:

9.1. Potential Exclusion of Vulnerable Communities

Poor and vulnerable communities, who often do not have smartphones, may be deprived from receiving information or receiving services equitably. The lack of ubiquity in the use of smartphones also means that the results may be unreliable and therefore useless.[44] This is a significant issue when it comes to voluntary apps for data surveillance as they are more likely to capture data in affluent communities.[45] Surveillance may also deter vulnerable groups from seeking healthcare due to, for instance, fears of deportation. In Pakistan, this may potentially be very acute when it comes to Afghan refugees. It also may push infected people into the shadows which risks worsening the spread.[46]

[43] Payments under Ehsaas Program to Begin From Wednesday – Dr. Nishtar, Business Recorder, April 2020 https://www.brecorder.com/2020/04/05/586644/payment-process-under-ehsaas-emergency-cash-program-to-start-from-wednesday-dr-nishtar/

[44] Barrie Sanders (supra n.13)

[45] Future of Privacy Forum, A Closer Look at Location Data: Privacy and Pandemics, March 25, 2020, https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/

[46] NBC, COVID-19 tracking data and surveillance risks are more dangerous than their rewards, March 20, 2020, https://www.nbcnews.com/think/opinion/covid-19-tracking-data-surveillance-risks-are-more-dangerous-their-ncna1164281

9.2. Improper Application and Location Thresholds

Moreover, location data by mobile phone providers has been deemed so inaccurate as to be unsuitable in order to determine possible infections with coronavirus.[47] There is a danger that inaccurate raw data which is being used to inform policy will create an information overload which will overwhelm users who are given repeated and irrelevant warnings. Experts argue that location tracking based on mobile data is only accurate up to 50 metres, and therefore cannot tell us anything about the interaction between two people.[48]

9.3. Potential of Misuse

There is also an acute risk of misuse by governments who may normalize the use of surveillance to such an extent that it is expanded beyond the end of this pandemic.[49] This normalisation may mean it is used for other things after the outbreak is over such as tracking petty crime. Moreover, there is a threat that this data will be vulnerable to hacks or breaches.

[47] Noyb, Data protection in times of coronavirus: not a question of if, but of how, March 30, 2020, https://noyb.eu/en/data-protection-times-corona

[48] Noyb, Ad hoc Paper (V0.2) SARS-CoV-2 Tracking under GDPR, March 29, 2020, https://noyb.eu/sites/default/files/2020-03/ad_hoc_paper_corona_tracking_v0.2_5.pdf

[49] Barrie Sanders (supra n.13)

9.4. Ensuring Data Security

Questions have also been raised regarding the effectiveness of surveillance systems with organisations like Electronic Frontier Foundation and Privacy International stating that there is limited evidence to suggest that it has been useful in tackling Ebola or Middle Eastern Respiratory Syndrome (MERS).[50] This is in part because of the high number of false positives or false negatives in testing systems. The lack of reliable information will impede the effectiveness of surveillance as well as trust in the government. Moreover, if an AI incorrectly quarantines you, it is difficult to challenge or reverse this automated judgment and this has been a problem in China. Therefore, the lack of accurate and reliable data is a significant setback.

There are also concerns regarding the safety and storage of data systems, including data gathered from third-party apps. Such technologies often rely on cloud computing and storage, amongst other avenues.[51] Developing countries, like Pakistan, must develop core capacities in these fields to ensure local solutions are available in terms of storing and protecting data. Alternatively, third party-apps present another host of challenges pertaining to privacy, particularly in terms of tracking fields of movements and contacts of individuals.[52] There also remains a risk that collected data could be leaked to other parties, or be hacked/stolen directly. Recently, the Federal Investigation Agency (FIA) in Pakistan was ordered to probe a data breach,

[50] Ibid

[51] Advanced Analytics for Coronavirus Trends and Predictions, TeraData https://www.teradata.com/Blogs/Advanced-Analytics-for-Coronavirus-Trends-Patterns-Predictions

[52] Apps and COVID-19, Privacy International. https://privacyinternational.org/examples/apps-and-covid-19

whereby information from 115 million cell-phone users in Pakistan was stolen and was up for sale on the dark web.[53] Ensuring protection of such information during data collection and when in storage is thus crucial in successfully implementing such technologies.

9.5. State Capacity in Pakistan

The establishment and evolution of NADRA has been a monumental success story which has allowed the government to undertake several effective policy interventions over the years based on big data analytics. However, despite the success of initiatives like the Benazir Income Support Programme (BISP) and the recent Ehsaas Programme, there remain several key challenges in implementing big data analytics for cyber surveillance purposes. Firstly, the health sector needs to be empowered with qualified data scientists for the categorization, collation, analysis and summation of data from COVID-19 cases in real-time.

This is particularly important, as the outbreak of the coronavirus exposed severe deficiencies in the National Institute of Health (NIH)'s data measuring capabilities.[54] Key statistics were found conflicting with provincial tallies, data-set categories were unaligned with international standards, and new categories were created arbitrarily – creating doubts regarding the authenticity of the data. Daily situation reports commenced nearly two weeks after the first case and were discontinued almost a month later – other official sources

[53] FIA asked to probe 'data breach of 115m mobile users' – DAWN. 20 April 2020 https://www.dawn.com/news/1548536

[54] New COVID-19 Cases as Pakistan Tally Hits 194, Express Tribune, March 17, 2020. https://tribune.com.pk/story/2177847/1-10-new-covid-19-cases-confirmed-as-pakistans-tally-hits-194/

were grossly incongruent with the figures generated by the NIH.[55] Therefore, it is critical to ensure data science capabilities embedded within the public sector to avoid data discrepancies in all departments of federal and provincial governments.

10. Recommendations on Implementing Cyber-Surveillance

In the wake of the outbreak, Pakistan has implemented a mobile phone tracking system which uses geospatial data to identify where coronavirus patients have been during the last 14 days and those who have been in close proximity to them have been sent a text message directing them to self-isolate.[56] These messages have been sent through the Pakistan Telecommunication Authority which stated that it has directed cell phone operators to send 109 million SMS to subscribers regarding preventive measures they should take in light of the outbreak.[57] 170 thousand messages have also been sent to passengers arriving in the country from China and Iran advising them to obtain immediate assistance if they develop virus symptoms.

However, in order to enhance cyber surveillance frameworks, it is necessary to ensure congruence with provisions of privacy and other rights as outlined above. The following options may be considered by stakeholders:

[55] Covid-19 Response, National Institute of Health https://www.nih.org.pk/novel-coranavirus-2019-ncov/

[56] The Conversation, Coronavirus: how Pakistan is using technology to disperse cash to people in need, April 2, 2020, http://theconversation.com/coronavirus-how-pakistan-is-using-technology-to-disperse-cash-to-people-in-need-134873

[57] PTA Website, PTA Supporting National Efforts In Fight Against Corona Virus, March 19, 2020, https://www.pta.gov.pk/en/media-center/single-media/pta-supporting-national-efforts-in-fight-against-corona-virus--200320

i. Data security and protection policies need to be well-defined, and enshrined within local legislation and rules of business across the federal, provincial and district levels. With the degree of digitization of records and personal information, it is critical that data protection protocols be implemented with utmost priority. Public bodies in particular, such as NADRA, where computerized NICs are used to determine information ranging from tax records to registering mobile SIMs, need to devise data security protocols, including emergency measures in cases of breaches of sensitive information. Apart from national legislation, data security education and reform needs to occur within all public institutions, mandated by the authorities for assured protection.

ii. Data protection policies and laws that are designed to be enacted within public institutions must be formulated with consultations from private data experts, public stakeholders as well as members of the civil society. Transparency regarding the storage, usage, and protection of data must be maintained, and oversight bodies must be created to ensure that data protection is implemented across all spectrums of public institutions that utilizes or handles personal data.

iii. Given Pakistan's emerging data capabilities illustrated through the Ehsaas Programme, it will be useful to engage data scientists and engineers to create dashboards that monitor, map, track and record coronavirus cases on real-time dashboards for the NIH and other health agencies in Pakistan. This will create opportunities for public-private collaborations to reach innovative solutions for Pakistan's corona-case management and allow for no discrepancies between data collection.

iv. Engaging and empowering the private sector can also be useful as private laboratories and other hospitals are engaged in coronavirus testing, and/or provide intensive care treatments to COVID-19 patients. It is necessary to collate data from these sectors into a real-time dashboard to illustrate a complete picture of all on-ground actors involved in curbing the spread of the coronavirus. The government must also be transparent about any data-sharing agreements with other public or private sector entities

v. In terms of cyber surveillance and Pakistan's inherent capacities, specified smartphone apps can also be rolled out, targeting returnees from abroad most of whom have access to smartphones. This is particularly necessary once travel bans and other restrictions are lifted or eased, as Pakistan's initial wave of coronavirus cases was traced to returnees from abroad, who were neither instructed to quarantine initially, nor told to follow preventive measures.

vi. An 'infected unless proven healthy' approach could be adopted which allows individuals to voluntarily download an application which would become a de facto requirement for participation in public life.[58] For instance, businesses may require consumers to have this app for them to use their services. This approach may allow for a proportionate interference in people's lives while circumventing draconian

[58] Noyb, Ad hoc Paper (V0.2) SARS-CoV-2 Tracking under GDPR, March 29, 2020, https://noyb.eu/sites/default/files/2020-03/ad_hoc_paper_corona_tracking_v0.2_5.pdf

surveillance measures which would be difficult to implement in Pakistan.

vii. In order to avoid breaches of privacy, anonymized data can also be used. The European Commission has requested that mobile carriers provide anonymised and aggregate mobile data. This would ensure that no personal information is included in the data collected, instead unique identifiers are used instead of names in order to pseudonymise the data. However, this may still not be entirely effective in keeping data anonymous as people's behaviour can be traced back to their homes by, for instance, observing where the device stays at night.[59] Location datasets should be treated as private, sensitive information in order to protect people's privacy to the greatest extent possible.

viii. Data should also be encrypted to ensure recipients can share data without misusing it. The system should also be independently verified to ensure that false information is not provided which can trigger inaccurate notifications.[60] There should also be strict time limits so that the data cannot be retained after the pandemic and to ensure trust among users that they are voluntarily giving up their data only in order to contain the pandemic.

ix. A detailed review of Pakistan's domestic framework needs to be carried out to consider the legal and constitutional viability of large-scale cyber-

[59] Future of Privacy Forum, A Closer Look at Location Data: Privacy and Pandemics, March 25, 2020, https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/

[60] Noyb, Ad hoc Paper (V0.2) SARS-CoV-2 Tracking under GDPR, March 29, 2020, https://noyb.eu/sites/default/files/2020-03/ad_hoc_paper_corona_tracking_v0.2_5.pdf

surveillance for public health purposes. In our preliminary assessment, legislative changes may be required to ensure compatibility with Pakistan's human rights obligations and fundamental rights under the Constitution. Further, any laws which give the state surveillance powers should be publicly declared and reported to treaty bodies when fundamental rights are being limited. They should all include protections and safeguards against abusive surveillance and provide access to effective remedies. This could be through the setting up of remote complaints mechanisms to process any grievances against their operation.