COVID-19

Data Governance in Kenya:

Lessons for the Future

April **2022**

CIPESA

Table of Contents

Acknowledgement:

CIPESA acknowledges the contribution of Kictanet in the writing of this report.
The report was produced with support from the Hewlett Foundation in the context of promoting data openness among public and private actors and advancing respect for data rights towards citizens’ participation and informed policy decisions in rights-respecting data-for-development initiatives. Similar reports have been produced for Ghana, Kenya, and Uganda.

Introduction

The outbreak of coronavirus (COVID-19) pandemic and the subsequent measures adopted by governments to fight against its spread reignited the debate around privacy and personal data as well as data governance. Governments, in collaboration with various stakeholders such as technology companies and international agencies, implemented a raft of extraordinary technological measures to enhance disease surveillance, coordinate response mechanisms, and promote public awareness.[1] These measures included the use of digital tracking and location data collection to identify hotspots where several people gathered, to enforce quarantines for people that were ill or exposed, and to track those who may have come into contact with infected people.

Even before the first case of COVID-19 was confirmed, in March 2020, the Kenyan government put in place measures to mitigate the spread and impact of the pandemic, including strengthening the healthcare system and introducing health and hygiene guidelines. The government also introduced policies on tax relief, dusk-to-dawn curfews, closure of schools, a ban on public gatherings including reduction of the number of attendees at weddings and funerals, and lockdowns that restricted movement in and out of the most affected areas. Other measures included massive collection of personal data including names, ID/passport numbers, telephone, and email contacts to enable contact tracing, and monitoring of suspected COVID-19 patients and their contacts.[2]

According to the government, contact tracing and monitoring was aimed at ensuring that those exposed to the virus had limited interactions in public spaces and where such persons were publicly exposed, then all contacts could be traced for quarantine purposes. Several applications were developed and rolled out in communities to support the contact tracing of COVID-19 suspects as well as mapping vaccination patterns.[3] However, some of these were not secure enough to host sensitive information, as they were created by entities lacking proper data governance frameworks and practices.[4] The use of such applications had the potential to cause data breaches and in the process lead to stigmatisation of some individuals affected by COVID-19 whose personal information would fall in the wrong hands.

The purpose of this research therefore was to review relevant data governance frameworks that were in place in Kenya during the pandemic and to document citizens' experiences in relation to COVID-19 data collection and contact tracing. The findings of the research and subsequent recommendations may help governments and data collectors to improve data governance practices including of public health data during emergencies.

The research entailed a review of COVID-19 related legislation and literature (policies, guidelines, and statements), media and other research reports.

[1] *COVID-19 in Africa: When is Surveillance Necessary and Proportionate?https://cipesa.org/2020/03/COVID-19-in-africa-when-is-surveillance-necessary-and-proportionate/*

[2] *Ministry of Health, Targeted testing strategy for COVID-19 in Kenya, https://www.health.go.ke/wp-content/uploads/2020/07/Targeted-Testing-Strategy-for-COVID-19-in-Kenya.pdf*

[3] *Nature, Digital technologies in the public-health response to COVID-19, https://www.nature.com/articles/s41591-020-1011-4*

[4] *Ibid*

Privacy, Data Protection and Governance in Kenya

The right to privacy and data protection is guaranteed under Article 31 of the Constitution of Kenya, 2010. The article grants the right to individuals not to have (a) their person, home or property searched; their possessions seized; information relating to their family or private affairs unnecessarily required or revealed; or the privacy of their communications infringed.

This right is further buttressed by the Data Protection Act[5] which was passed in 2019. The Act seeks to protect the privacy of data subjects by providing for their rights and regulating the processing of personal data and ensuring that the processing of personal data is guided by the data principles which are set out in section 25. The law also prescribes the different remedies available to the data subject whose data has been unlawfully processed under the Act.[6]

Section 25 of the Act provides that, "Every data controller or data processor shall ensure that personal data is — (a) processed in accordance with the right to privacy of the data subject; (b) processed lawfully, fairly and in a transparent manner in relation to any data subject; (c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes; (e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required; (g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and (h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

Section 39 outlines instances and exemptions on the retention of personal data by a data controller or processor. It states that (1) a data controller or data processor shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is — (a) required or authorised by law; (b) reasonably necessary for a lawful purpose; (c) authorised or consented to by the data subject; or (d) for historical, statistical, journalistic literature and art or research purposes. Under section 39(2), data controllers or data processors are required to delete, erase, anonymise or pseudonymise personal data not necessary to be retained under sub-section 39(1) in a manner as may be specified at the expiry of the retention period.

Part II of the Data Protection Act provides for the establishment of the office of the Data Protection Commissioner (section 5) charged with overseeing the implementation of this law; establishing and maintaining a register of data controllers and data processors; and exercise oversight on data processing operations, either of own motion or at the request of a data subject.

[5] *The Data Protection Act, 2019; http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf*

[6] *Section 3 of the Act*

Data Collection Programmes in Kenya

Data collection in Kenya dates back to more than a century ago. The government has been documenting births since 1904.[7] Other personal data collection and processing practices that have been introduced over the years have been for purposes of voter registration, SIM card registration, marriage, driving permit and issuance of passports and national IDs.

In 2015, using rule 4 of the Kenya Information and Communications Act (Registration of SIM cards) Regulations, 2015,[8] Kenya introduced the mandatory SIM card registration exercise. The exercise required all mobile network providers to register all SIM card subscribers. Failure to provide the information as detailed in the SIM card regulations is an offence and is punishable by a fine of KES 300,000 (USD 3,000) or imprisonment for a term not exceeding six months, or both.

In addition, section 5(1) of the 2015 Kenya's Registration of Persons Act Cap (107)[9] provides for a national register of all persons who are citizens of Kenya and have attained the age of 18 years. Personal details to be captured in the register include the registration number; name in full; sex; declared tribe or race; date of birth or apparent age, and place of birth; occupation, profession, trade, or employment; place of residence and postal address, if any; finger and thumb impressions (or toe and palm impressions in case of missing fingers and thumbs); and date of registration.

In January 2019, President Uhuru Kenyatta announced the development of a central master population database, known as the National Integrated Identity Management Systems (NIIMS), which would be the authentic "Single source of truth" on personal identity in Kenya.[10] The database would replace the integrated Population Registration System (IPRS), and contain information on all Kenyan citizens as well as foreign nationals residing in Kenya. For each registration, the system would generate a unique identification number known as Huduma Namba.[11] As of May 2019, the mass registration process hnd captured the details of 37.7 million people but an estimated 11 million people had not been registered.[12]

[7] The State of Identification Systems in Africa, https://documents1.worldbank.org/curated/en/298651503551191964/pdf/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf

[8] The SIM card Regulations, https://ca.go.ke/wp-content/uploads/2018/02/Registration-of-SIM-%E2%80%93Cards-Regulations-2015-1.pdf

[9] Kenya Registration of Persons Act, 2015

[10] Speech by Uhuru Kenyatta, http://www.president.go.ke/2019/01/22/speech-by-his-excellency-hon-uhuru-kenyatta-c-g-h-president-and-commander-in-chief-of-the-defence-forces-of-the-republic-of-kenya-during-a-meeting-with-senior-security-officials-at-state-house-mo/

[11] Huduma Namba, http://www.hudumanamba.go.ke/

[12] Another Huduma Namba listing planned for those who missed out, or-another-huduma-namba-listing/

Surveillance, Contact Tracing and Management of COVID-19 Data

As one of the response measures to combat the spread of COVID-19, the government passed several legal instruments that provided for surveillance, contact-tracing, registration, testing, isolation, and quarantine of suspected COVID-19 patients. In April 2020, the government issued the Public Health (Prevention, Control and Suppression of COVID-19) Rules, 2020.[13] The rules empowered medical officers or public health workers to enter any premises to search for any case of COVID-19 cases, or to inquire whether there was or had been on the premises, any case of COVID-19 (section 5).

In addition, the regulations require employers to maintain a register of all employees who work from the office for purposes of contact tracing. Further, religious institutions and individuals planning weddings, funerals and other social gatherings are also required to keep a list of attendees - names, contacts and residence areas and body temperature for contact tracing purposes.

The government also maintained heightened surveillance at all points of entry into Kenya, at health facilities, and in communities across the country. In a press statement on June 25, 2020, the Cabinet Secretary for Health noted that the surveillance and response systems that had been in use for contact tracing since the first case of COVID-19 was recorded had been overwhelmed hence the need to upgrade to a more robust system.[14] The country then adopted an interoperable system which functioned as a web-based COVID-19 tracking system and a COVID-19 tracking application based on the open source community health toolkit (CHT).[15] According to the health secretary, the two systems supported:

- workflows for case registration;
- contact listing, tracing, investigations (laboratory orders);
- COVID-19 laboratory orders;
- managing quarantine sites; and
- data exchange with laboratories.

According to the Ministry of Health's directives of13th July 2020,[16] once a person was confirmed to have COVID-19, contacts were then traced through information from the patient as well as relevant registers where available. All contacts were taken for quarantine and COVID-19 tests were administered. In the event that the results came back positive, affected persons were transferred to the hospital from the quarantine facility by an ambulance and admission was arranged based on bed availability.

[13] *Ministry of Health, Public Health (Prevention, Control and Suppression of COVID-19) Rules, 2020, https://www.kenyachamber.or.ke/wp-content/uploads/2020/04/COVID-19RULES.pdf*

[14] *National Response Committee, 'Update on COVID-19 in the Country' (June 2020), COVID-19 Press Statement, June 25, 2020*

[15] *According to the health ministry, prior to the coronavirus pandemic the CHT was being widely used in the health sector to support "Universal Health Coverage and advance global health equity".*

[16] *Ministry of Health, Daily situation Report (July 2020), COVID-19 OUTBREAK IN KENYA*

On the other hand, if a person tested negative, they had to complete 14 days of quarantine to safeguard others in case they developed symptoms and turned positive for COVID-19 after the initial test. After the 14-day period, Ministry of Health staff would provide a self-quarantine declaration form[17] for signing before clearance, with the individual required to complete seven additional days of self-isolation.[18]

The self-quarantine declaration form requires information such as name, age, sex, passport number, COVID-19 test results date, reasons for desire to self-quarantine, travel history, exact physical address, description of the house being used for self-quarantine, name and contact details of health care worker offering care to self-quarantining person as well as car registration number, name and contact details of driver who transports person to self-quarantine.

The government is also reported to have developed a database of COVID-19 related information that collected and stored information relating to COVID-19 patient infection, contacts, treatment as well as COVID-19 vaccination related information.[19] In addition, at some point Kenya was reported to be monitoring the mobile phones of individuals who were under self-isolation and arresting those who violated the restrictions imposed on their movements.[20] The government had enlisted the National Intelligence Service (NIS) to facilitate access to patients' phone location data to trace their last movements, a procedure which was not feasible at large scale, and was expensive.

There were also independent initiatives to develop contact tracing applications in Kenya. In May 2020, the Jomo Kenyatta University of Agriculture and Technology (JKUAT) developed a contact tracing and case management web and mobile application to help identify who, where and when someone got into contact with a COVID-19 patient.[21] Another contact tracing application tracing system dubbed 'KoviTrace' was developed by Mount Kenya University.[22] The application provided access to all the persons that an individual came into close contact with in the previous 14 days. The identified contacts were then immediately contacted via push message.

Additionally, the ministry of ICT set up an advisory committee for the purposes of receiving proposals on technology for management of COVID-19 from local innovators in an effort to adopt the use of mobile and web-based applications for data collection, reporting, monitoring and response to the pandemic.[23] Part of the outcomes of the work of the committee included development of guidelines by the Data Protection Commissioner's office to guide application of privacy principles to the technologies adopted.[24]

Management of COVID-19 Vaccination Data

On March 25, 2021, the government rolled out mass vaccination with an initial target of 1.02 million doses of AstraZeneca's Covishield vaccine, with priority being given to frontline health workers and teachers for the voluntary shots. Recipients were required to register at an online e-portal, ChanjoKenya, on the ministry of health website with personal information.[25] The e-portal developed by the Kenyan ministry of health is used to register for vaccination, view vaccination status, update one's COVID-19 registration and obtain a vaccination certificate. In addition, by keying personal details into the portal, an individual is contacted through a text message about their vaccination. Unfortunately, the portal does not contain information on what the data collected would be used for, how long it would be kept, and the rights of data subjects.

[17] *Self-Quarantine Declaration Form, https://medical.unon.org/sites/default/files/2020-07/Request%20for%20self%20quarantine%20%20individual%20template.pdf*

[18] *UNON, 'Information during Mandatory Period, https://medical.unon.org/sites/default/files/2020-05/Mandatory%20Quarantine%20Kenya%20Nairobi%20FAQs.pdf*

[19] *Ocha Services, Republic of Kenya COVID-19 Operations Dashboard, https://www.humanitarianresponse.info/en/operations/southern-eastern-africa/kenya-covid-19-operations-dashboard*

[20] *State taps phones of isolated cases, https://www.standardmedia.co.ke/nairobi/article/2001365401/state-taps-phones-of-isolated-cases*

[21] *Kenyan university launches contact tracing app, http://www.xinhuanet.com/english/2020-05/07/c_139035989.htm*

[22] *MKU Researchers develop COVID-19 contact tracing App, https://www.mku.ac.ke/index.php/mku-latest-news/1566-mku-researchers-develop-COVID-19-contact-tracing-app*

[23] *Ibid*

[24] *Office of the Data Protection Commissioner, Gudiance Note on Access to Personal Data During the COVID-19 Pandemic, https://ict.go.ke/wp-content/uploads/2021/01/Draft-Data-Request-Review-Framework-Jan-2021.pdf*

[25] *Chanjo of Kenya, https://portal.health.go.ke/*

Management of Passenger Travel Data

The Government of Kenya was the first country to adopt TrustedTravel, an application associated with the African Union (AU), which acts as a continental COVID-19 digital passport.[26] The innovation was developed by the AU through its lead health agency, the Africa Centres for Disease Control and Prevention (Africa CDC), and private sector technical partners. It has enabled travellers across Africa to enjoy faster clearances at points of entry. TrustedTravel is currently being used by Kenya to verify one's COVID-19 status when they come into and out of the country.

In March 2020, the government announced that it would launch a contact tracing app known as mSafari for public transport to provide contact data that would help trace the movements of confirmed or suspected cases.[27] All public service vehicle operators would be required to enrol on the platform using their vehicle registration numbers. Further, they would be required to collect contact details of every passenger, which would automatically be registered on the mSafari platform. The service would be free across all networks through user code *483*42#, and would track the GPS location of the vehicle. However, it appears that this application did not gain widespread usage as it has less than 100 downloads on Google's PlayStore.[28]

Another application, MyrideAfrica, was developed for use by both private and public service vehicles. The application allowed the collection of personal information of passengers, such as identity card and phone numbers, so that they could be traced if there was virus exposure reported in a vehicle they had boarded.[29]

Safety and Security of COVID-19 Data

In January 2021, the Office of the Data Protection Commissioner (ODPC) in Kenya published a Draft Guidance note on Access to Personal Data During the COVID-19 pandemic,[30] providing direction on how technological innovations built in response to the pandemic, including apps and other services, may request for access to personal data from government institutions or private entities to enable product development. The guidance note acknowledges that health data and geo-location may be necessary for contact tracing.

Specifically, the guidance note served to re-emphasise the key principles of data processing as provided for under the Data Protection Act, 2019, as explained below.

Data Processing: The note called upon data controllers to process personal data in an accountable manner by ensuring that the personal information of an individual is processed for a specific purpose, which in this context is to detect, contain and prevent the spread of COVID19. Secondly, personal data requested should only be that which is adequate, relevant, and limited to what is necessary in relation to the purpose for which the personal data is requested. Moreover, that the data should not be kept for longer periods than is necessary to achieve the purpose for which the data was collected and processed. The data must also be correct, complete, and up-to-date.

In addition, once the purpose for which the data is collected is achieved, the data should be destroyed or be rendered de-identifiable. The personal data must be processed securely to retain confidentiality and integrity in consistency, accuracy, and trustworthiness over its entire life cycle.

[26] *Africa Union CDC, Trusted Travel, https://africacdc.org/trusted-travel/*

[27] *Government to launch contact tracing application, https://www.standardmedia.co.ke/health/article/2001365263/app-uses-passenger-data-to-trace-virus-path*

[28] *mSafari, https://play.google.com/store/apps/details?id=com.keypadsys.msafariapp&hl=en*

[29] *Kenyan youth develop a contact tracing app, https://www.capitalfm.co.ke/business/2020/05/kenyan-youths-develop-a-contact-tracing-app-in-psvs/*

[30] *OPDC, Guidance note on access to personal data during COVID-19 pandemic, https://tinyurl.com/2p86n96e*

Data Request and Sharing: The guidance note requires that where possible, personal data should be collected directly from individuals subject to their express consent. Further, personal data sharing between parties has to be guided by a valid agreement including nondisclosure, data confidentiality provisions, data protection safeguard provisions including the data destruction technique to be used, data protection impact statement, and a data responsibility matrix. The sharing should be approved by the Office of the Data Protection Commissioner.

In addition, access to personal data must be limited to those who need the information to conduct treatment, research or other responses that are addressing the crisis or any other relevant exemption, and to the largest extent possible, personal data should be in an anonymised format and in a manner that individuals cannot be re-identified. On the other hand, for the applications requesting access to personal data, the data controller shall publish policies on what information is being collected and with whom the information may be shared. And where personal data is kept for a longer duration, it shall be non-identifiable information.

The selling of processed data to third parties or transferring it out of the country is also prohibited without the concerned individual consenting to the transfer. In addition, the transfer of personal data to another country shall only take place where sufficient proof has been given on the appropriate safeguards with respect to the security and protection of the personal data.

Conclusions

Like many countries, the Kenya government issued a raft of measures aimed at containing the spread of the coronavirus, including legal instruments that provided for contact-tracing, testing, isolation, and quarantine of suspected COVID-19 patients. Unfortunately, these contact tracing measures, including the technology applications deployed, remained questionable and potentially violated privacy rights, as they lacked clear or any legal oversight, and there were no documented safeguards in case of any breaches.

While Kenya has a data protection law, proper guidance on the processing, storage and sharing of personal data was only provided in January 2021. This means that all the contact tracing and the attendant collection and processing of personal data for purposes of combating COVID-19 throughout 2020 lacked clear legal guidance and express safeguards in the event of breach. In addition, there was lack of clarity and limited public awareness of the data governance framework which the government and its partners employed in collecting, processing and managing COVID-19 data.

A core part of data governance is securing information and holding all stakeholders accountable for how they handle the information collected and processed. Kenya's Data Protection Act and guidance note require data controllers to take measures to ensure the safety and security of personal data. This obligation must be fulfilled in government health data policies and data standards, including those dealing with information collected in the course of COVID-19 surveillance, treatment and vaccination. The government must have full oversight over where COVID-19 data is stored, who is updating the data, who is accessing it and for what purposes.

There were notable gaps in the handling of COVID-19 data in Kenya. They included the long delay by the Data Protection Authority to issue guidelines to govern the data collection and handling, the regulator's lack of proactive monitoring of the data collectors' operations, and the haphazard development and deployment of apps, some of which did not have the backing of the government, which meant that data could be collected by entities whose practices could not be monitored or audited.

To-date the health ministry has never provided information on the extent of the data that was collected, the number of apps that collected such data, how the data was used, and whether the data has been destroyed since it is no longer necessary for the purpose for which it was collected. Similarly, the health ministry has not publicly stated whether there were any data breaches or what the utility of the apps that were deployed was. The lack of such transparency and audits means that opportunity is lost to identify the pitfalls to avoid and the good practices to build on in handling data in emergency situations such as that which was posed by COVID-19. Ultimately, it can be concluded that the lack of regulations to guide the data collection, the multiplicity of data-collection and contact tracing apps that were not adequately regulated, and the hardly-visible oversight role by the regulator, the ODPC, all went against international best practice and indeed the principles of the Data Protection Act of 2019. This scenario undermines citizens' trust in data-based initiatives by government bodies and other actors such as the private sector.

Recommendations

Government Agencies

- Develop a comprehensive data governance framework for handling data during pandemics and other health emergencies. The framework should define the goals and success metrics of the collection, processing and management of data, including the rules applicable to processing of the data, accountability framework and appropriate controls to be applieds.
- The Government and particularly the Office of the Data Protection Commissioner should publish final enforceable guidelines relating to the governance and management of COVID-19 data in Kenya. The guideline document published in January 2021 available online still has 'draft' as a watermark. It is not clear if there was any public participation or stakeholder sensitisation following publication of the draft. Final guidelines after public participation should be published and all stakeholders sensitised on their content.
- In the meantime, Government entities collecting data on COVID-19 patients should follow the Draft Guidance note set out by the ODPC as this was designed to ensure that the collection and processing of COVID-19 data is in line with the Data Protection Act.
- Government should be transparent about partnerships it enters with private entities regarding collection and data sharing. In this regard, the government should develop a standard data policy to guide development of COVID-19 centred applications developed for adoption by the Government.
- The ODPC should provide a whitelist of countries with adequate data protection for purposes of supporting cross-border data flows for COVID-19 information or an exemption for data related to global pandemic management.
- The government also needs to consider the cyber security implication of relying heavily on technology in tackling the COVID-19 pandemic. Further, the government must anticipate and adequately prepare for any cyber risks that may occur from relying on applications. For example, the Italian COVID-19 Vaccination booking systems suffered what the Italian government called their most serious cyberattack on a public system.

Private Sector

- Comply with the Data Protection Act and any Guidance Notes issued by the ODPC when it comes to the collection and processing of data related to COVID-19. The Act and practical guidance forms are part of the data governance framework for COVID-19 data. The framework only works where all stakeholders and data stewards discharge their responsibilities.
- Adhere to privacy by design when developing COVID-19 related applications. Private companies should also have data governance frameworks in place that highlight the steps to ensure that the data they collect and process is secure. Further, data protection impact assessments should be undertaken in line with the Guidance Note issued by the ODPC for such assessments and the results filed with the ODPC at least 60 days before launch of developed applications or implementation of new data governance processes.
- Have clear privacy policies written in plain language appropriately describing to the data subject the data that will be collected by the application, the purpose of the collection, key highlights of the data lifecycle management process and any cross-border data flows or sharing of data that will go on with third parties or processors. The policy should also communicate how consent (if given) can be withdrawn. The process to withdraw consent, where applicable, should be as simple as the process to give/collect consent in the first instance.
- Be transparent on the type of data sharing contracts that they enter with the government and the type of data they are sharing with the government.

Civil Society Organisations (CSOs)

- Conduct research and continue monitoring how government and private entities are collecting and processing data, document and raise concerns about any practices that negatively affect data subject rights. Part of this can include engagement with the ODPC and making specific requests to the ODPC to act where required in the interest of the public.
- Undertake activities to increase public awareness with regards to protections offered under the law to help the public understand the various roles and responsibilities of different stakeholders and data stewards of COVID-19 data. The increased public awareness will support an increase in documentation of instances where COVID-19 data was/is collected and misused by government or private entities, thereby increasing the accountability of stakeholders and data stewards.
- Partner with the ODPC in their planned public awareness campaign to sensitise stakeholders across the nation on the provisions of the Data Protection Act. The CSOs can provide support as well as input into the ODPC's communication and engagement strategy as well as help convene public stakeholders in their spheres of influence.
- Work with other stakeholders in the development of policies towards a sound data governance framework. This may include participation in calls for public participation with regard to relevant laws, regulations, guidelines, strategies to improve protection of personal data rights provided by the Constitution.

Platforms and internet businesses

- Platforms and internet businesses should resist the urge to share personal data in their possession with government agencies without following provisions of the law, including the notification of data subjects.

Academia and research organisations

- Academia and research organisations should research and explore the implications of COVID-19 measures and their effects on the rights of individuals, especially data protection and privacy, and how infringement could affect the enjoyment of other fundamental human rights.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
☎ +256 414 289 502
✉ programmes@cipesa.org
@cipesaug facebook.com/cipesaug Linkedin/cipesa
www.cipesa.org