9 Tracking COVID-19: What are the implications for data privacy in Africa?

Alex Boniface Makulilo, Rindstone Bilabamu Ezekiel, Doreen Mwamlangala and Mbiki Msumi

Abstract

The outbreak of COVID-19 and its spread into a pandemic have compelled governments worldwide to take stern measures to protect their populations. As elsewhere, different African governments are tracking, tracing, collecting and using personal data to slow down the spread of COVID-19. Many African countries use physical contact tracing in which individuals that tested positive are interviewed to identify locations where they had been and identify people whom they had met. Some few countries have started using tracking applications so as to complement physical tracking methods and, hence, provide additional data sources. Notwithstanding the necessity of protecting the health of residents from the pandemic, the fact that this protection hinges on sensitive personal data of individuals raises concerns for data privacy in Africa. This chapter offers a detailed discussion of the implications for the privacy of tracking applications in the context of COVID-19 in Africa. Examples will be taken from different African jurisdictions. Specifically, the chapter answers the question of whether data privacy laws in Africa are capable of protecting personal data in the context of COVID-19.

1 Introduction

The outbreak of the corona virus pandemic was reported for the first time in late 2019 in Wuhan, Hubei province, China. It rapidly became a worldwide threat as it raised health concerns and has continued to pose a threat to people's lives.[1] The virus threat in China drew the attention of the Chinese Centre for Disease Control,[2] leading to the isolation of a new corona virus, COVID-19. This novel virus has persistently caused thousands of deaths globally. Only in January 2020, the outbreak rapidly engulfed the countries of China, Thailand, Japan, South Korea, Singapore, Vietnam, Taiwan, Nepal and the United States. At different stages, the world witnessed the spread of COVID-19 between late-January and mid-

1 Coronaviruses have been described as single, plus-stranded RNA viruses belonging to the family *Coronaviridae* including MERS (MERS-CoV) and SARS (SARS-CoV).

2 H Lu and others 'Outbreak of pneumonia of unknown etiology in Wuhan, China: The mystery and the miracle' (2020) 92 *Journal of Medical Virology* 401-402

February 2020 from Hubei province, China to Northern Italy; from China to Washington state; and, later, from Europe to New York City and from China to California.[3] Although many details of the emergence of this virus have remained controversial, the COVID-19 pandemic continued to surge and, in Africa, with severe health, social, and economic impacts on an unprecedented scale.

In Africa, the first confirmed cases of COVID-19 were reported in Egypt,[4] South Africa,[5] Senegal,[6] the Democratic Republic of the Congo (DRC),[7] Nigeria, Algeria and several other African countries. Available data reveals that apparently all early cases were imported in Africa among travellers from Europe. Subsequently, the majority of COVID-19 cases that were identified and reported in many African countries were the result of local transmission.

The pandemic has significantly affected people's lives and livelihoods due to upheavals of the pandemic that has claimed and continues to claim thousands of lives in many countries. Almost every country that was hit hard by COVID-19 had its health systems overwhelmed. Without any alternatives for livelihood, many countries shut down markets, airports, hotels, sports and public transport.

In an attempt to contain the rapid spread of the pandemic, many countries around the world introduced a range of measures underpinning

3 D Stole 'How Coronavirus took hold in North America and Europe, Igniting Major COVID-19 Outbreaks' https://scitechdaily.com/how-coronavirus-took-hold-in-north-america-and-europe-igniting-major-COVID-19-outbreaks/ (accessed 12 September 2020).

4 On 14 February 2020.

5 On 29 February 2020. A group of nine adult travellers returned from a skiing holiday in Italy, where the COVID-19 epidemic was rampant. After developing a flu-like illness, one traveller tested positive for COVID-19, which was confirmed by RT-PCR on 5 March 2020; his wife was asymptomatic but tested positive on 8 March 2020. Overall, seven of the nine travellers tested positive for COVID-19, five of whom were asymptomatic.

6 World Health Organization, African Region 'Senegal reports first COVID-19 case' https://www.afro.who.int/news/senegal-reports-first-COVID-19-case (accessed 12 April 2020).In Senegal, the first COVID-19 case was reported on 7 March 2020 whereby a traveller returning from Italy led to contact tracing that identified a cluster of transmission of 20 cases within his immediate household.

7 World Health Organization 'First Case of COVID-19 confirmed in Democratic Republic of the Congo' https://www.afro.who.int/news/first-case-COVID-19-confirmed-democratic-republic-congo (accessed 20 January 2021. DRC Congo confirmed its first case of COVID-19 on 10 March 2020 which involved an adult male who tested positive in the capital city of Kinshasa after developing a cough and fever, two days after returning from France.

key guiding responses to the spread of the pandemic. These included measures recommended by the World Health Organisation (WHO) and additional measures preferred by individual countries. These include quarantine whereby a person or group of people who have been exposed to a contagious disease were separated even if they had not become sick. This trend has been variably implemented by countries and continues to be imposed in some countries around the world. This has been believed to be capable of preventing the possible spread of COVID-19. Lockdown restrictions were introduced by many countries in response to the spread of COVID-19 across the European region, Asia, North and South America as well as, to a certain extent, in Africa. Other measures include regular hand washing with soap and water; coughing into a tissue or a bent elbow, ensuring to afterwards safely dispose of the tissue; maintaining a social distance of at least one to two metres, particularly if a person is coughing; avoiding touching the eyes, nose and mouth; and seeking early medical attention if a person develops a fever or cough.

Some countries have continued to invest in low-cost preventive measures to improve physical distancing, namely, stopping international travel, reducing the number of people at religious and social gatherings, and universal masking using non-medical cloth masks for the community. Other measures could focus on protecting older people, allowing individuals restricted working hours for income generation, information campaigns for personal hygiene, physical distancing, and hand washing. As lockdowns and physical distancing measures are eased, proactive surveillance, case detection, and contact tracing with isolation will be required to prevent a dramatic resurgence of COVID-19 cases. African health ministries of are working closely with African Ministries of Health, Africa CDC alongside the WHO in preventive measures to curb the spread of COVID-19. Individual countries have gone further to develop mechanisms for use of technologies in contact tracing.

2 COVID-19 contact tracing and modern technology

Contact tracing is an essential public health measure and a critical component of comprehensive strategies to control the spread of COVID-19. Contact tracing breaks the chains of human-to-human transmission by identifying people exposed to confirmed cases, quarantining them, following up with them to ensure rapid isolation, and testing and treatment in case they develop symptoms[8]. When systematically and effectively implemented,

8 World Health Organization 'Contact tracing and quarantine in the context of COVID-19: Interim Guidance' 6 July 2022 https://www.who.int/publications/i/

these actions can ensure that the number of new cases generated by each confirmed case is maintained below one. In the context of COVID-19, contact tracing requires identifying persons who may have been exposed to a person with COVID-19 and following them up daily for 14 days from the last point of exposure. Since COVID-19 transmission can occur before symptoms develop, contacts should remain in self-quarantine during the 14-day monitoring period to limit the possibility of exposing other people to infection should they become ill.[9]

In response to the COVID-19 pandemic, many digital tools have been developed to assist with contact tracing and case identification. These tools include outbreak response, proximity tracing, and symptom tracking tools, which can be combined into one instrument or used as stand-alone tools.[10]

Africa has been less affected than Europe by the corona virus crisis, but the number of cases is increasing as the pandemic progresses across the continent. Many African countries have been severely hurt by the corona virus pandemic. In Africa, COVID-19 is disrupting millions of lives. Poor people and small and informal businesses are having particular difficulties getting by. Even with containment measures such as lockdowns and quarantines, the pace of this disruption is likely to accelerate in the months ahead.

South Africa is still in its infancy stages in developing mobile application technologies to be used as part of the contact tracing process. The South African government together with the University of Cape Town recently developed a mobile application called Covi-ID. The use of the application is by voluntary consent and as yet there are no state-mandated mobile application that people are expected to download and use. Similarly, the government operates a WhatsApp platform that provides people with information on the corona virus as well as information on symptoms of COVID-19. The WhatsApp platform has been criticised for a lack of transparency on the terms and conditions available regarding the processing of personal information collected via the platform.[11]

item/WHO-2019-nCoV-Contact_tracing_and_quarantine-2022 (accessed 6 July 2022).

9 As above

10 K Servick 'COVID-19 contact tracing apps are coming to a pone near you. How will we know whether they work?' https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how (accessed 2 January 2021).

11 Y Jacobs 'SA launches free Covid-19 contact tracing app: This is how it works' https://www.iol.co.za/technology/mobile/sa-launches-free-COVID-19-contact-tracing-app-

On the other hand, Ghana launched a new application called the COVID-19 Tracker Application that is designed to help in tracing people who have come into contact with COVID-19-positive individuals. The application is meant to augment the government's effort in the fight against the virus.[12] The application is able to trace contacts of persons infected by the virus and show where they have been in recent times through various telephone-related data, and link such people to health professionals for urgent action to be taken.[13] The application, through the same telephone-related data, is also able to report contacts that are, or recently have been to COVID-19-hit countries, as well as track whether individuals required to self-quarantine indeed are doing so.

However, the implementation of this application has also raised public concerns over the security of personal information required by the application to help in identifying and tracing persons who have come into contact with infected persons.[14]

In similar vein, on 23 March 2020 Kenya launched an application for contact tracing. Public service vehicle operators and passengers are required to provide information that helps trace the movements of people who have contracted the corona virus. All public drivers or operators are required to enrol using their vehicle registration numbers and collect details of every passenger. The application is expected to trace all the contacts made by an infected person inside public vehicles. An estimated 50 per cent of the Kenyan population daily uses public transport.[15]

On the other hand, technology developers in Kenya have introduced a contact tracing application by the name of KoviTrace[16] to help authorities trace the movement of patients who have tested positive for COVID-19, as well as those who have come into contact with these patients. The application can be installed on Android and IOS[17] phones or accessed

this-is-how-it-works--24b27e8b-d30f-43e4-82a5-4d508255c5cb (accessed 2 January 2021).

12 ITUNews 'Ghana launches COVID-19 Tracker App' https://news.itu.int/ghana-launches-COVID-19-tracker-app/ (accessed 2 January 2021).

13 As above.

14 'Ghana launches GHcovid19 symptom tracker to contain the spread of COVID-19' https://furtherafrica.com/2020/05/14/ghana-launches-ghCOVID19-symptom-tracker-to-contain-the-spread-of-COVID-19/ (accessed 2 January 2021).

15 European Investment Bank (EIB) 'Africa's digital solutions to tackle COVID-19' https://www.eib.org/attachments/country/africa_s_digital_solutions_to_tackle_COVID_19_en.pdf (accessed 12 September 2020).

16 This is a diagnostic test for the detection of Sars-cov-2 virus in nasal swab and saliva.

17 iPhone Operating System. This functions only on Apple iPhone, iPod, iPad, iWatch, Apple TV and iMac.

through unstructured supplementary service data (USSD) for users without smart phones.[18] It uses geo-sensing technology to track a patient's location at any given time over a 14-day period from the precise moment they tested positive.[19] The user will need to key in the patient's phone number and command it to trace all the persons with whom the patient came into contact within the stipulated time period. Currently authorities and health officials are relying on patients themselves to remember who they have been in contact with for the past 14 days.

Rwanda has deployed digital tools in contact tracing for coronavirus infections, following in the steps of several countries that are using smart phone data and other digital surveillance tools to curb the virus from spreading further.[20] Aware that it is difficult to fully rely on the information provided by those who tested positive, Rwanda opted for a digitised contact tracing method.[21]

The team then tracks other phones that came in close contact with the infected person's phone using movement analytics. Deeper data analysis is then carried out and information obtained helps the COVID-19 command centre to trace these people and contact them for testing. The method has so far proved effective: Reports show this, as most of those who tested positive and those they with whom they got in contact had smart phones. Besides contact tracing, information technology (IT) solutions are also used to monitor and geo-fence people in localised isolation centres to keep them in areas of confinement while data obtained help to inform law enforcement agencies of people violating social distancing rules in areas of concentration.[22]

In Nigeria mobile applications and web platforms have emerged as some of the prevailing tools to educate, test and track people to curb the virus from becoming more disastrous than it already is. As of 9 June 2020 the total number of confirmed COVID-19 cases in Nigeria had risen to over 12 000 with 361 deaths.[23] As of 23 February 2021 Morocco accounted for around 8,4 per cent of the casualties on the African continent. Egypt was the second most affected on the continent, as the virus affected 10 443

18 EIB (n 15).

19 As above.

20 'Rwandan develops app for easy tracing of COVID-19 candidates' https://furtherafrica.com/2020/05/26/rwandan-develops-app-for-easy-tracing-of-COVID-19-candidates/ (accessed 12 July 2020).

21 As above.

22 As above.

23 www.africanews.com › 2020/07/01 › nigeria-coronavir (accessed 27 August 2020).

victims in the nation, which is nearly 10,2 per cent of the overall deaths in Africa. Notably, South Africa had faced the highest number of casualties on the African continent with 49 413 deaths. As of 23 February 2021 the overall deaths due to COVID-19 in Africa had reached 102 286. On the same date Africa recorded more than 3,87 million cases of COVID-19.[24] Even with these mounting numbers of cases, the ongoing argument around a defective COVID-19 tracking system has not stopped, raising many controversial questions as to the accuracy of the reported numbers and the likelihood of under-reporting.[25]

In Nigeria tracing and isolation of infected people are some of the vital ways of curbing the COVID-19 spread, but still other different methods are currently being explored to ensure an efficient tracking system in the country. However, this is still a very challenging task in a country of over 200 million people with an incapacitated healthcare system and limited experience with the handling of novel diseases.[26] Reasonably, technology companies are focusing their creative resources to solve this challenging task by creating applications and platforms that could aid the tracking process and help to report cases across the country.[27]

In Sierra Leone, for example, an existing unstructured supplementary service data government platform was extended to enable citizens to conduct a self-assessment of their symptoms and get updates on Sierra Leone's COVID-19 situation.[28] An additional SMS mobile application that offers users the same functionalities was also developed for smart phone users, and the ability of people to obtain an initial diagnosis not only reassures the population but also helps predict the spread of the virus.[29]

24 Statista 'Number of coronavirus (COVID-19) deaths in the African continent as of November 18, 2022, by country' https://www.statista.com/statistics/1170530/coronavirus-deaths-in-africa/ (accessed 24 February 2021)

25 As above.

26 T Obiezu 'Fear & Stigma Keep Nigerians from Helping Contact Tracers' VOA Africa https://www.voanews.com/africa/fear-stigma-keep-nigerians-helping-contact-tracers (accessed 27 August 2020).

27 As above.

28 K Ighobor 'Sierra Leonean technologist's app helps to fight COVID-19' https://www.un.org/africarenewal/magazine/august-2020/sierra-leonean-technologist%E2%80%99s-app-helps-fight-COVID-19 (accessed 12 December 2020)

29 As above.

3 Privacy concerns and debates around COVID-19

Since the dawn of COVID-19, many governments have taken unprecedented measures to track, trace and contain the spread of the pandemic. Tracking the spread of COVID-19 has been done by deploying some digital technologies and advanced analytics to access, collect, process and share data for effective front-line responses. The digital technologies use geo-spatial data, collected through the mobile devices' inbuilt global positioning systems and have helped officials to locate hundreds of thousands of people who might have contracted COVID-19 by interacting with the carriers or attending the virus hotspot locations. These technologies are considered effective for timely, secure and reliable data access and sharing. They form acritical means for understanding the virus and its spread, improving the effectiveness of government policies, and fostering global co-operation in the race to develop and distribute therapies and vaccines.

Some COVID-19 tracking approaches involve digital technologies by using applications that provide a tool for governments to monitor and contain the virus. Through the use of these technologies, governments have been harnessing the power of data to drive digital solutions for effective front-line response concerning the spread of the virus. Tracking the location of newly confirmed cases, rates of recoveries and deaths, and the source of new cases, such as international arrivals or community transmission, have been massively conducted at varying scales. The collection of health data has been crucial in assessing and improving the capacity of national healthcare systems, and in evaluating the effectiveness of containment and mitigation policies that restrict the movement of individuals. It is, thus, proven that digital technologies and advanced analytics are increasingly being developed in order to collect, analyse and share data for front-line responses through the use of geo-location data that is user-derived from mobile call data records or collected from mobile applications; and biometrics for facial recognition data, finger prints, and the like.

The emergence of contact tracing technologies in the fight against COVID-19 in many countries, particularly in Europe and America, has raised privacy and data protection concerns, particularly because privacy and security are important values worthy of attention. The public holds strong privacy concerns about how their personal health data is used. This is especially more so when personal health data is handled and used in a manner that is not directly relevant to providing care. In some cases, not even company employees can fully access the data and link it to a named individual. Privacy concerns arise from the fact that the regulation of fast-moving, rapidly-evolving technologies variably is inadequate and

where it tends to exist, its efficacy remains opaque. It is believed that emerging contact-tracing technologies pose a higher risk to privacy in COVID-19 tracking, thereby violating data privacy policies on preserving the confidentiality, integrity and availability of personal information. Questions on proportionality of the use of contact-tracing applications have been asked touching on fundamental data protection and privacy principles in which information should be accessible only to those authorised to have access.[30]

There are assumed possible breaches in data utilisation during the COVID-19 crisis. This is because there are fears that contact-tracing applications have been implemented without full transparency, accountability and a commitment to ensuring that data privacy rights of individuals are guaranteed and actually protected. A lack of clear, strong and enforceable data privacy laws across many countries worldwide during COVID-19 tracking creates a fertile environment for massive data privacy breaches by governments, organisations, and individuals involved with tracking, collecting, storing and sharing personal health information. Some COVID-19 tracing approaches have been considered controversial in terms of their potential risk of violating privacy and other fundamental rights of citizens. Particular concerns emerge when such deploying of digital contact-tracing technologies and other physical methods become devoid of transparency, public consultation, and consent of data subjects. Under the framework of information security law, there have been doubts about the integrity of personal health information collected during the contact tracing for COVID-19, particularly in countries that have not adopted enforceable laws on data protection. Data subjects and informed persons have suspected the lack of transparent mechanisms for safeguarding the accuracy and completeness of information and processing methods for protecting personal information against unauthorised modification. Privacy disclosures of personal information are considered as being able to provide governments with ways to monitor and contain the COVID-19 virus. The latter is done by identifying better potential COVID-19 infections and track the spread over time.

It is a given fact that, within a particular health protocol, health information of individuals will be collected, stored and shared by doctors, nurses and other healthcare providers during the treatment of patients. In order to preserve privacy, anonymisation has been used in order to allow

30 See AB Serwin 'Privacy 3.0: The principle of proportionality' (2009) 42 *University of Michigan Journal of Law Reform* 869-890, https://repository.law.umich.edu/mjlr/vol42/iss4/5 (accessed 12 December 2020); also see HD Gunnarsdóttir and others 'Applying the proportionality principle to COVID-19 antibody testing' (2020) 7 *Journal of Law and the Biosciences* 1-8.

doctors, nurses, hospitals, clinics and other organisations and companies to use and share data without endangering the individual's privacy.[31] This brings in the concept of using personal data anonymously for intended purposes without linking back to the identity of the data subject. Existing scholarship, however, shows that anonymisation works through de-identification which involves the removal of direct identifiers from the dataset. This technique that blurs and suppresses indirect identifies of a person that may include gender, date of birth, zip code, medical diagnosis, cccupation, extreme age, Approximate location ethnicity, uncommon race, and other details by enabling the resultant dataset to be released for consumption as open data is facing fierce criticism. Various technologies are used to ensure that sensitive data is stored on protected remote servers without sharing individual-level data with the data analysts.

Anonymisation requires data analysts to simply send queries to servers for analysing such queries. However, hi-tech engineers have argued that anonymisation that is primarily hinged on privacy is not good during this era of hi-tech as it kills innovation. This debate posits that data privacy regimes should not be used to deter the use of modern technological advances in innovation such as the use of artificial intelligence (AI) that is able to unlock the anonymous information so that hidden data may be used for numerous solutions of scientific problems for social good and economic development.[32] For example, nEmesis system in AI helps health departments to identify, for instance, certain restaurants that are the source of illnesses, mainly those that are food-borne.[33] It is further argued that AI is capable of being used to analyse social media data and discover and suggest behavioural and environmental impacts on health. In addition to the nEmesis system described above, examples include tracking of a disease declared a pandemic, such as SARS, influenza or COVID-19 and predicting the likelihood that particular social media users will become ill. The debate here argues that the world should not be entangled or locked in or stuck in the dichotomy of having either innovation or privacy. The contenders of this debate say that such a dichotomy is considered a false one.[34]

31 YA de Montjoye & A Gadotti 'Moving beyond de-identification will allow us to find a balance between using data and preserving people's privacy' https://linc.cnil.fr/fr/ya-de-montjoye-and-gadotti-moving-beyond-de-identification-will-allow-us-find-balance-between-using (accessed 15 September 2020).

32 GD Hager and others 'Artificial intelligence for social good' Computing Community Consortium (CCC), National Science Foundation, 2017 8-9. A Sadilek and others 'Deploying nEmesis: Preventing foodborne illness by data mining social media' Association for the Advancement of Artificial Intelligence 2016.

33 As above.

34 A Sadilek and others 'Deploying nEmesis: Preventing foodborne illness by data

Arguments have it that personal health information is the most sensitive information because it is well associated to an individual's private life. Many countries have numerous suitable and sometimes unsuitable policies, legislation, guidelines, and compliance requirements. All these are key to safeguard health information, privacy and security. However, in Africa, as in many other less-developed parts of the world, data privacy breaches remain key issues for electronic healthcare systems. The privacy of the patient is best protected by implementing a systematic mix of technologies and best practices such as technical de-identification of data and restrictive data access, as well as security measures in the specified technical platforms. Studies have indicated that the use of systematic mix of technologies and best practice have provided security models that make personal data security unauthorised access of protected patient health information extremely improbable, and they may not be compromised.[35]

Another mixed debate revolves around the legal challenges related to digital contact tracing during COVID-19, including potential risks of harmful acts, lack of privacy, biased algorithms, misinformation, and hacking.[36] There is a debate as to the extent to which a right to explanation exists in data privacy. A growing concern is about the practical feasibility of implementing such right in the context of complex data processing such as big data, artificial intelligence and machine learning. In South Africa, big data and deployment of AI has been worked out in several areas, including the healthcare sector, which increases the potential for data mining by social media. It is already underscored that privacy by design as techniques that primarily focus exclusively on protecting confidentiality and the identification of individuals whose data has been accessed, collected, processed, stored and shared is still debated upon as well. Veale, Binns and Ausloos have argued that there is a problem that continues to be debated upon, mainly that the data would still be potentially re-identifiable by third parties with enough capabilities given the automation and artificial intelligence in innovation through technologies.[37] Thus, intrusion and the disclosure of personal health information would still be

mining social media' (2017) 38 *AI Magazine* 37-48, https://doi.org/10.1609/aimag.v38i1.2711 (accessed 20 September 2020).

35 M Puppala and others 'Data security and privacy management in healthcare applications and clinical data warehouse environment' Conference Paper February 2016, doi: 10.1109/BHI.2016.7455821 1-28.

36 https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/1-a-framework-for-understanding-artificial-intelligence (accessed 20 September 2020).

37 M Veale, R Binns & J Ausloos 'When data protection by design and data subject rights clash' (2018) 8 *International Data Privacy Law* 105-123, https://doi.org/10.1093/idpl/ipy002 (accessed 20 September 2020).

a problem because AI allows the processing of personal data in new and unanticipated ways. Other difficulties emanate in the process of identifying specific individuals for linking them with data. This creates challenges of making access, erasure and objection as among the basic rights of the data subject in the process of protecting the data privacy of a person.

Wachter and others[38] have doubted the legal basis for the right to an explanation in the *General Data Protection Regulation* (GDPR), particularly in the context of digital data protection where machines process data, consent, collection, and disclosure through automation. They have argued that the right to an explanation is not compatible with the way in which modern machine learning technologies are being developed for production of meaningful information about the logic of processing. They state that it does not help much in the preservation of personal health information. Machine learning systems are designed to discriminate, but some forms of discrimination are socially unacceptable and the systems need to be restrained. The general obligation of fairness in data protection provides the basis for the need to have some level of insight into the functioning of algorithms, particularly in profiling. In this context there are said to be problems in another data privacy issue, namely, transparency in the context of algorithmic accountability. For example, providing the source code of algorithms may not be sufficient and may create other problems in terms of privacy disclosures and the gaming of technical systems. Thus, Wachter and others argue that an auditing approach could be more successful instead by looking at the external inputs and outputs of a decision process, rather than at the inner workings: 'explaining black boxes without opening them'. Their main departure is their proposal to partially decouple transparency as a necessary key step towards accountability and redress. They argue that people attempting to tackle data protection issues have a desire for an action, not for an explanation. The actual value of an explanation will not be to relieve or redress the emotional or economic damage suffered, but to understand why something happened and to help ensure that a mistake does not reoccur.

Another privacy debate, particularly on the African continent, is that privacy protection hinders access of useful information for the public good. This is why data privacy and protection issues in Africa are not a priority for many governments. African governments put much interest in legislation that protects their right to access information from individual

38 S Wachter, B Mittelstadt & L Floridi 'Why a right to explanation of automated decision-making does not exist in the general data protection regulation' (2017) 10 *International Data Privacy Law* 1-25.

persons and organisations, under the guise of national security interests.[39] Contenders of privacy rights argue that the right to privacy in many cases has to be balanced against other compelling interests of the state.[40] Such public interests include the policy agenda of improving the quality of life and promotion of public safety. Thus, public health emergency may override privacy concerns in the interests of the safety of the public.

4 COVID-19 and privacy regulation

As mentioned earlier, tracking COVID-19 raises privacy concerns around the world. During the COVID-19 pandemic, it is witnessed that the interests of public health in many nations overshadows the protection of personal privacy.[41] This has been the practice even in those nations where privacy is protected as a fundamental right in different instruments as well as in constitutions as in European Union (EU).[42] Moreover, the EU has the stringent privacy protection regime worldwide since 2018 under the General Data Protection Regulation (GDPR) and also through the Directive on Privacy and Electronic Communications (ePrivacy Directive);[43] yet it requires its member states to exchange personal data collected through contact tracing. The pandemic exemplifies that the privacy right is not absolute, and it may be limited under some special circumstances, such as the COVID-19 pandemic.[44] These concerns necessitated the development of new trends of privacy regulation in the context of the COVID-19 pandemic in different regions, sub-regions and nations. These encompass the adoption of new laws, the amendment of the existing laws and the suspension of certain laws.

Globally, the first trend that developed during the COVID-19 pandemic is the adoption of new laws. This was due to the fact that the existing laws were inadequate in responding to the pandemic. This can be seen in some European member countries such as Italy, Switzerland, Australia, Belgium and many others that passed specific laws for protecting privacy

39 A Green 'Scarcity of data protection laws in Africa leaves NGOs exposed' June 2018.

40 BT Sharp 'Right to privacy: Constitutional rights and privacy laws' Live Science Reference Editor 12 June 2013, https://www.livescience.com/37398-right-to-privacy.html (accessed 14 September 2020).

41 H van Kolfschooten & A de Ruijter 'COVID-19 and privacy in the European Union: A legal perspective on contract tracing' (2020) 41 *Contemporary Security Policy* 479.

42 Art 8 European Convention on Human Rights; Charter of Fundamental Rights of the European Union arts 7 and 8.

43 Consolidated version of the directive on privacy and electronic communications (ePrivacy directive), 2002 OJ (L 201) 37, https://perma.cc/YHA5-EFXV (accessed 30 August 2020).

44 ECHR art 8(2) and CFREU art 52.

rights after contract-tracing applications were implemented.[45] For example, Australia made a temporary human bio-security emergency declaration regarding human corona virus with pandemic potential in March 2020.[46] It gives the minister responsible expansive powers to set requirements and give directions to combat the pandemic.[47] The government passed a law on COVID-safe application privacy protections. This is known as Privacy Amendment (Public health Contact Information) Act 2020 and was passed into law on 14 May 2020.[48] Moreover, Switzerland enacted the temporary Swiss regulation that regulated the organisation, use, operation and data processing by the COVID-19 tracking applications in the country.[49] In tandem to other countries, Poland also adopted an emergence Bill in March 2020 known as the COVID-19 Act as a response to the pandemic.[50] In the same vein, the Italian government issued Decree 28, to create a legal framework for processing personal health data by private companies that form part of the health system as well as by the health authorities during the state of emergency.[51] Similarly, the Norwegian government issued a regulation on tracing and epidemic contagion related to COVID-19.[52]

The second trend that has been adopted in order to protect privacy rights while tracking COVID-19 is an amendment of the existing law. Various states around the globe amended their existing laws so that they can be sufficient in responding to the pandemic. An example of this can be seen from the case of Australia. Despite the fact that Australia adopted some new laws for the pandemic, as explained above, it also amended its Privacy Act in mid-May 2020. The gist of the amendment is to provide stronger privacy protections for the users of the COVIDSafe application and data collected through the application, and also to criminalise the use of data

45 L Edwards 'Apps, politics and power: Protecting rights with legal and software code' in L Taylor and others (eds) *Data justice and COVID-19: Global perspectives* (2020) 43.

46 Privacy Amendment (Public Health Contact Information) Act 2020, http://www.legislation.gov.au/Details/C20202A00044 (accessed 30 August 2020).

47 H Maclean & K Elphick 'COVID-19 legislative response – Human biosecurity emergency declaration explainer' *Flagpost parliamentary library*, http://perma.cc/Y473-TWXT (accessed 18 September 2020).

48 Parliament of Australia Privacy Amendment (Public Health Contact Information) Bill 2020, https://perma.cc/UK7M-DY6Y (accessed 16 September 2020).

49 Switzerland 'Regulation on proximity tracing app pilot adopted' http://www.loc.gov/law/foreign-new/article/switzerland-regulation-on-proximity-tracing-app-pilot-adopted (accessed 18 September 2020).

50 http://prawo.sejm.gov.pl/sap.nsf/download.asp/WDU20200000374/O/D20200374.pdf (accessed 17 September 2020).

51 OECD 'Ensuring data privacy as we battle COVID-19' (2020), http://www.oecd.org/policy-responses (accessed 17 September 2020).

52 *Forskrift om digital smittesporing og epidemikontroll I anledning utbrudd av COVID-91* (FOR 2020 03 27-475), https://perma.cc/UKS8-5Y5W (accessed 14 September 2020).

collected by the tracking-up for uses other rather than contact tracing.[53] Another example of a country that amended its laws so as to facilitate tracking COVID-19 is Poland. It amended the Telecommunication Act[54] and, hence, allowed the Minister of digital to have access to the location data of quarantined and infected persons from the telecommunication service providers.[55]

In the same vein, in order to fight COVID-19 some other countries suspended some existing legislation that was regarded as an impediment to fighting the pandemic. Some of these laws provide for the right to privacy. Hungary is an example of the countries that suspended privacy right of individuals in fighting COVID-19. In so doing, the government in March 2020 issued a decree allowing the Minister for Innovation and Technology to access all data available, personal data inclusive, without limits.[56] Further, in April 2020 it also issued another decree allowing staffs of a body set up for the defence against coronavirus to be granted access to information from any entity upon request in order to implement their duties.[57] Among other things, such information included health, contact personal identification and register data.[58] Conversely, there was no provision in the decree providing for the limitation of the access for the protection of privacy of the individuals. In tandem with this, the same government issued a decree in May 2020 suspending the application of the General Data Protection Regulation and the domestic Privacy Act (especially provisions dealing with the rights of data subjects, such as the right to information, erasure, objection, and so forth) until the end of the state of perceived or experienced danger, which may not necessarily be coronavirus pandemic.

Privacy challenges arising from tracking COVID-19 in other parts of the world are also experienced in Africa. Besides, its impact is more prominent in Africa due to the fact that only 30 out of 55 countries in

53 Privacy Amendment (Public Health Contact Information) Bill 2020 https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1920a/20bd098 (accessed 14 September 2020)

54 http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20041711800 as amended (accessed 18 September 2020).

55 M Brewczynska 'Policing quarantine via app' in Taylor and others (n 4) 234.

56 https://magyarkozlony.hu/dokumentumok/c4210b08dd73832b3ca261193f85d58498c9718/megtekintes (accessed 17 September 2020).

57 https://magyarkozlony.hu/dokumentumok/13285bbde75a626ff044ec795e70a6ee5d700b29/megtekintes (accessed 17 September 2020).

58 I Borocz 'Suspending rights and freedoms in a pandemic induced state of danger' in Taylor and others (n 45) 146.

Africa variably adopted data privacy laws.[59] Most of these laws follow the spirit of the repealed EU Data Protection Directive, 1995. This implies that they are not in line with the current technological development. Similarly, most of the existing laws have not entered into force and some data protection authorities are yet to be appointed.

Due to the privacy challenges brought about by contact tracking during COVID-19, some countries in Africa resorted to the adoption of new laws so as to protect privacy. Others resorted to the amendment the existing laws while others suspended some laws that were regarded as an impediment in tracking COVID-19. However, other countries decided to use digital tracking of COVID-19 without having any law for the protection of the privacy of individuals.

To date, particularly in Africa, the important parts of the private lives of victims of COVID-19 have been suspected to have been intruded contrary to the fundamental right to privacy.[60] A substantial amount of data was randomly and widely collected in an unlimited pattern through a combination of a variety of COVID-19 tracking approaches. These included physical contact tracing, oral questioning through face-to-face interviews, the application of digital technologies such as the use of mobile phones, applications, geolocation data, and so forth. It is in this context that we contend that tracking COVID-19 has both negative and positive implications for data privacy in Africa.

Largely, health information has been and continues to be collected, processed, stored and shared without clear and enforceable data privacy laws in Africa. Only a few countries in Africa have functioning data protection legislation. For example, South Africa has the Protection of Personal Information Act (POPIA).[61] Thus, POPIA is South Africa's law on data protection that seeks to give effect to the constitutional right to privacy by putting in place conditions that have to be complied with by authorised parties involved in the extraction and processing of personal information.

59 CIPESA 'Mapping and analysis of Privacy Laws and Policies in Africa-Summary Report' (July 2021) 5 https://cipesa.org/wp-content/files/reports/Mapping-and-Analysis-of-Privacy-Laws-and-Policies-in-Africa.pdf (accessed 11 October 2020).

60 M Muson 'Contact tracing and data protection during COVID-19 pandemic in South Africa', https://blogdroiteuropeen.com/2020/07/29/contact-tracing-and-data-protection-during-COVID-19-pandemic-in-south-africa-by-melody-muson/ (accessed 15 September 2020).

61 Act 4 of 2013.

In Mauritius, the Data Protection Act 2017 (DPA) governs some exceptional measures that involve the processing of various types of personal health data of the individual, including body temperature, other health data, geolocation data, and so forth. During the COVID-19 pandemic, Mauritius permitted hypermarkets, supermarkets, superettes and food retail shops or food outlets to take the body temperature of their customers. Regulations were passed on who can take the temperature and to whom the temperature can be communicated. Also, Mauritius has the Prevention and Mitigation of the Infectious Disease (Coronavirus) Regulations 2020, which itself is made under section 79 of the Public Health Act. Under the said regulations, the General Notice (GN) 547 of 2020 enacted under Regulation 13(2) of the Regulations contains conditions for reopening and operation of food outlets in Mauritius. The body temperature of each customer may be taken by staff of the relevant food outlet. Where any customer has a high temperature (38 degrees and above), the law provides that the customer will be transferred to the nearest hospital and he will be dealt with according to the protocol of the Ministry of Health and Wellness. The General Notice directs the taking of temperature to be done as from Thursday 2 April 2020 until 15 April 2020 and, upon expiry of that period, a new regulation would need to be enacted to extend this duration so that this practice may lawfully continue beyond the earlier date issued, that is to say 15 April 2020.

Mauritius went further by providing the duty to explain to the customer the reason and purpose for collecting the data. The person collecting information must state to which authority the information will be communicated. A categorical statement of the right of the data subject has to be stated and the period of retention of such data. An individual has the right to lodge a complaint with the Data Protection Commissioner in situations where they are not satisfied with the way in which their personal data is being processed. The easy accessibility of collected information should be stated in clear and plain language, and so forth.

Despite efforts made by a few African countries, it is highly doubtful whether there can be a reliable guarantee of the protection of personal health data in most African countries. In most African countries, data is shared without legislation to govern data privacy, information processing and sharing. Personal data is collected and used without securing specific and unambiguous consent of data subjects. There is massive unauthorised sharing of health information by organisations that collect and use such information.

Generally, in Africa, a few countries, such as South Africa and Mauritius, have frameworks in place to support extraordinary COVID-19

control measures in ways that are relatively fast, scalable and, to some extent, in compliance with existing privacy and data protection regulations within certain provided framework of protection of rights of data subjects. However, security and trustworthiness of legal mechanisms remain to be seen as citizens from these countries and literature have shown that there are still some dangers of a clash between data protection and data subjects' rights.[62]

Ghana is an example of a country with privacy protection regulation, but which went further and adopted a new legislation to combat the COVID-19 pandemic.[63] It passed an Executive Instrument (EI) 63 – the Establishment of Emergence Communication System Instrument in March 2020 – which provides, among other things, for the establishment of an emergency communication system to trace all contacts of persons suspected of or affected by a public health emergence, COVID-19 inclusive. However, the instrument is very wide as it does not define the public emergencies in which the law can be applicable. Also, the instrument does not restrict its applicability to the COVID-19 pandemic and, hence, instead of protecting privacy during the COVID-19 crisis, it legalises impending intrusive state surveillance in the long run. It is also interesting to note that while public emergencies fall under the state of exception, the instrument seems to be laying down a permanent registry without providing any safeguards. Consequently, it may amount to a permanent threat to individuals' data privacy rights.[64] It is worth noting that the EI instrument in Ghana was used to suspend the applicability of the existing laws that makes the monitoring of personal communications by state and security actors subject to a court warrant.

Another example is that of South Africa, a country with an incomplete data protection landscape. The Protection of Personal Information Act was adopted in 2013, but it has not yet fully entered into force. However, most of its provisions only came into force in July 2020 with a grace period of one year for data processors to comply.[65] In the response to the COVID-19 pandemic, the minister responsible issued a regulation geared to expand the state's powers for mining personal data from the citizen. This raises concerns over whether this mining adheres to privacy protection principles.

62 M Veale, R Binns & J Ausloos 'When data protection by design and data subject rights clash' *International Data Privacy Law*, http://doi.org/10.1093/idpl/ipy002 (accessed 15 September 2020).

63 Ghana, http://www.news.itu.int/ghana-launches-COVID-19-tracker-app (accessed 17 September 2020).

64 S Oduro-Marfo 'Transient crisis, permanent registries' in Taylor and others (n 45) 141.

65 A Gillwald and others 'Protecting mobile user data in contact tracing' in Taylor and others (n 45) 250.

The government went further and amended the regulations of its Disaster Management Act to allow telecommunication service providers to provide geolocation data to health authorities for contact-tracing purposes only.[66] The new regulation is known as the disaster management contact-tracing regulation. Among other things, the regulation limits the scope of mobile data collection by a COVID-19-tracing data base to only those individuals that are suspected of or known to have come into contact with anyone who is suspected of or already is infected with the corona virus. The regulation encompasses some privacy protection principles in data collection. These include collecting data for specific purposes, accuracy of data, accountability of the collecting parties and limitation on the retention of data. However, the regulation is in conflict with other laws in the country that require a judge's order for communication interception as the regulation does not require such an order.[67]

Another example is Nigeria, a country with a complete data protection framework with a Data Protection Regulation since 2019 (NDPR).[68] In tracking COVID-19, Nigeria invoked the provisions of the NDPR to legitimise the collection and sharing of personal information.[69] The Act provides that a person's data may only be collected and disclosed under any of the following conditions: 'when the processing is required for the protection of the vital interest of a data subject or another natural person; or if the processing is necessary for the performance of a task carried out in the public interest'.[70]

Relying on the provision above, the Nigerian government authorised the use of the contact-tracking application for COVID-19 without enacting any new law or amending the existing. However, this practice proves to be detrimental to privacy right protection to Nigerians, taking into consideration how the applications are working. The same was the practice in countries such as Kenya. Moreover, there is another category of countries that used the COVID-19 tracking application without having a data protection regulation in force, for example, Botswana.[71]

66 As above.

67 Gillward and others (n 65) 251.

68 Nigerian Data Protection Regulation, 2019.

69 D Oturu 'Nigeria COVID-19 coping with data protection/privacy challenges within the context of the Nigerian data protection regulation' https://www.mondaq.com/nigeria/data-protection/910792/covid-19-coping-with-data-protectionprivacy-challenges-within-the-context-of-the-nigerian-data-protection-regulation- (accessed 18 September 2020).

70 Nigerian Data Protection Regulations sec 2.2.

71 Botswana 'Data protection overview' https://www.dataguidance.com/notes/botswana-data-protection-overview (accessed 18 September 2020).

5 Conclusion

The discussion above demonstrates the difficulty with which jurisdictions around the world have struggled to fight COVID-19 while variably trying to ensure the protection of the fundamental rights of individuals. Nonetheless, a variation of legal approaches to the regulation of privacy in Africa and beyond has left it open for possibilities by governments, private sectors and individuals to infringe the right to privacy of individuals. In Africa, where data protection regulation in general is still emerging, and with limited data privacy practices, it has become more challenging to guarantee individuals' right to privacy. A common approach by African states could have helped to mitigate the difficulty of cross-border enforcement of data privacy.

References

Edwards, L 'Apps, Politics and Power: Protecting Rights with Legal and Software Code in Taylor, L and others (eds) *Data justice and COVID-19: Global perspectives* (2020) 40

Gregory, DH and others 'Artificial Intelligence for Social Good Computing Community Consortium (CCC), National Science Foundation (2017)

Gunnarsdóttir, HD and others 'Applying the proportionality principle to COVID-19 antibody testing' (2020) 7 *Journal of Law and the Biosciences* 1

Hripcsak, G and Albers, DJ 'Correlating electronic health record concepts with healthcare process events'(2013) *Journal of the American Medical Informatics Association* 20(e2), pp.e311-e318, 2013 (accessed 27 September 2021)

Lu, H and others 'Outbreak of pneum\\onia of unknown etiology in Wuhan, China: The mystery and the miracle' (2020) 92 *Journal of Medical Virology* 401

Maclean, H & Elphick, K 'COVID-19 legislative response – human biosecurity emergency declaration explainer' Flagpost parliamentary libraryhttp://perma.cc/Y473-TWXT

Oduro-Marfo, S 'Transient crisis, permanent registries' in Taylor, L and others (eds) *Data justice and COVID-19: Global perspectives* (Meatspace Press, 2020)

Paxton , Cand others 'Developing predictive models using electronic medical records: challenges and pitfalls. In AMIA Annual Symposium proceedings (pp 1109-1115), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3900132 (accessed 21 October 2020)

Sadilek, A and others 'Deploying nEmesis: Preventing Foodborne Illness by Data Mining Social Media' (2016) 38 AI Magazine 37

Serwin, BA 'Privacy 3.0: The Principle of Proportionality' (2009) 42 *University of Michigan Journal of Law Reform* 869

van Kolfschooten, H & de Ruijter, A 'COVID-19 and privacy in the European Union: A legal perspective on contract tracing' (2020) 41 *Contemporary Security Policy* 479

Veale, M and others 'When data protection by design and data subject rights clash' (2018) 8 *International Data Privacy Law* 105

Wachter, S and others 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2016) 7 *International Data Privacy Law* 1

YA de Montjoye and Gadotti, A 'Moving beyond de-identification will allow us to find a balance between using data and preserving people's privacy' https://linc.cnil.fr/fr/ya-de-montjoye-and-gadotti-moving-beyond-de-identification-will-allow-us-find-balance-between-using (accessed 27 September 2021)