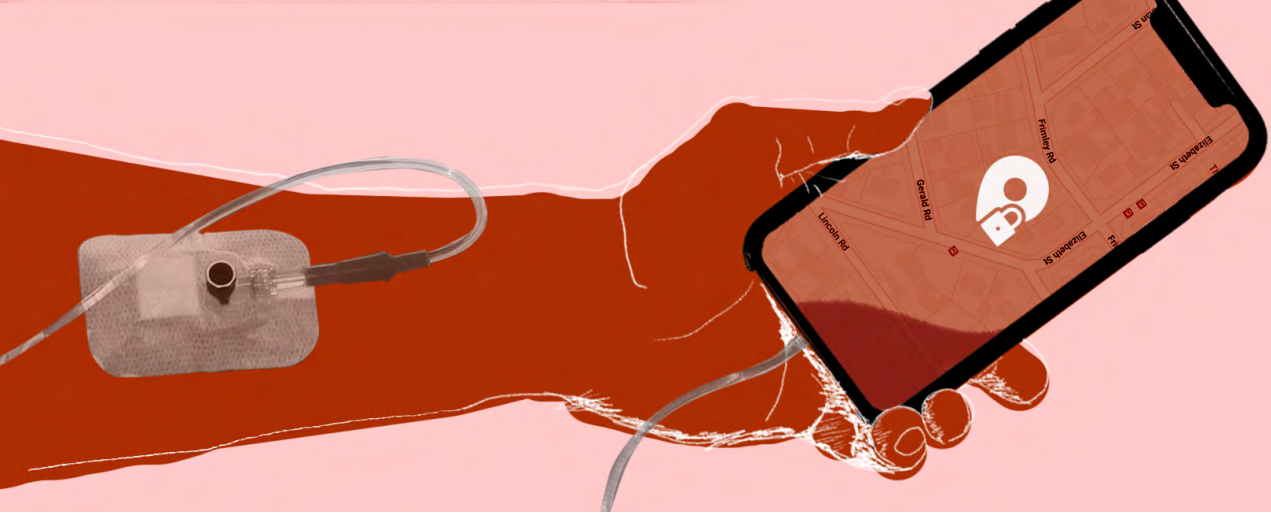

Data protection in the age of technology-based disease surveillance

AUTHOR: Amanda Manyame | COUNTRY: South Africa

INTRODUCTION

Principle 8 of the African Declaration on Internet Rights and Freedoms[1] provides for the right to online privacy, including the protection of every person's personal data. Such a right and such protection have become necessary because of the uses of personal data and data in general. It used to be that a person's personal space was limited. However, emerging technologies have allowed for entities to make use of data and personal data in a manner that provides strategic advantages. This has been particularly true in the health sector and during the COVID-19 pandemic, during which technology-based surveillance has been used to curb the spread of the virus.

The most popular measure being adopted by countries to curb the spread of COVID-19 has been the use of personal and health data to trace and predict the spread of the disease. This is being done by making use of technology-based disease surveillance which has resulted in the over-disclosure of personal and health data about persons infected with COVID-19 and those they have come in contact with. This approach has resulted in the mass collection of personal data and the limitation of the right to privacy of individuals. It is, however, generally accepted that human rights may be limited, if such limitation is reasonable and proportional to the reason for the limitation.[2] This was reiterated in the United Nations Policy Brief titled "COVID-19 and Human Rights: We are all in this together".[3] It has also been generally accepted that the use of technology

1 https://africaninternetrights.org

2 Article 29 of the United Nations Declaration on Human Rights, 1948; Article 4 of the International Covenant on Civil and Political Rights, 1966; Section 36 of the Constitution of South Africa, 1996.

3 United Nations. (2020). *COVID-19 and Human Rights: We are all in this together.* https://www.un.org/sites/un2.un.org/files/un_policy_brief_on_human_rights_and_covid_23_april_2020.pdf

in response to COVID-19 must adhere to the principles of processing personal data, which include transparency, accountability, confidentiality and security.

Without data protection regulations or COVID-19 regulations that provide for these principles and enforcement thereof, the personal and health databases that are being created may be susceptible to abuse – and more so in instances where there is not adequate regulation of the destiny of these databases after the COVID-19 pandemic. This is the predicament that South Africa faces, with the recent announcement that the provisions in the 2013 Protection of Personal Information Act (POPIA) for the processing of personal data are only effective from 1 July 2020, with a 12-month grace period for compliance.[4]

Accordingly, this paper explores the adequacy of the COVID-19 regulations enacted in South Africa as they pertain to protection of the personal and health data being collected in an attempt to curb the spread of COVID-19.

THE IMPORTANCE OF YOUR DATA

In South Africa the right to privacy is protected in section 14 of the country's constitution.[5] Even before the codification of the right, it was recognised as forming part of a person's right to dignity. This is so because a person's privacy is closely associated to their right to dignity. However, over the years, the way in which the right to privacy is protected has evolved to not just provide for protection within a person's private space, but to include general protection of information about a person. This is so because of emerging technologies that make use of personal data in nearly every transaction[6] and in decision making to obtain a competitive edge.[7] Data has, thus, been termed the new oil.

It therefore comes as no surprise that personal and health data has been successfully used to predict the spread of contagious diseases such as severe acute respiratory syndrome (SARS), Middle East respiratory syndrome (MERS) and now COVID-19. Personal and health data is collected and combined into what is referred to as data sets. Quantitative analysis software, making use of artificial intelligence, machine learning and algorithmic computation, is used to, among other things, make predictions and conclusions from the data sets. This is known as big data analytics. Predictions drawn from making use of big data analysis are accurate, resulting in its use during pandemics to stop the spread of viruses like the one that causes COVID-19.

However, because of the potential of these personal data sets, they are vulnerable and susceptible to cyberattacks, abuse and misuse, sometimes

4 Presidency of the Republic of South Africa. (2020, 22 June). Commencement of certain sections of the Protection of Personal Information Act, 2013. http://www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act,-2013

5 https://www.justice.gov.za/legislation/constitution/index.html

6 Tene, O. (2011). Privacy: The new generations. *International Data Privacy Law, 1*(1), 15-27. https://doi.org/10.1093/idpl/ipq003

7 Brynjolfsson, E., Hitt, L., & Kim, H. (2011). Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance? *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486

by the very entities that are responsible for these data sets. Consequently, to ensure that the personal data is used for its intended purpose, protected from abuse and with the data subject's privacy protected, meaningful accountability and consistent enforcement mechanisms have been developed in the form of data protection laws.

In South Africa, the POPIA data protection legislation was enacted for such a purpose. In terms of POPIA, public and private organisations that process personal data are required to do so in a lawful, accountable and transparent manner. Unfortunately, the relevant provisions of POPIA only came into effect on 1 July 2020, as announced by the Presidency on 21 June 2020.[8] This was after a national state of disaster had been declared and technology-based disease surveillance measures had been implemented. Furthermore, organisations processing personal data have 12 months from 1 July 2020 to comply with the collection, processing and storage provisions in POPIA. Consequently, a question arises of how personal data collected for the purposes of curbing COVID-19 will be protected for the duration of and after the national state of disaster.

CONTACT TRACING: THE MASS COLLECTION OF PERSONAL DATA DURING COVID-19

In South Africa, the commonly used measures to curb the spread of COVID-19 have been by way of collecting personal and health data and tracking and tracing the spread of the virus. The methods of collection that have been used to date include testing of individuals, identifying those that have contracted the virus, and gathering information about places these individuals have been to and people they have come in contact with.

This has been made possible by the declaration of a national state of disaster in terms of section 27 of the Disaster Management Act, 2002 (DMA).[9] The DMA provides for management policies that focus on reducing the risk of disasters like the COVID-19 pandemic. In terms of section 8(1) of the DMA, the National Disaster Management Centre was set up. The National Centre is empowered, in terms of section 18(1) of the DMA, to request information that is reasonably required by it for the purposes of providing it with adequate information on all aspects of COVID-19 so as to allow it to curb its spread. A requestee may not fail to comply with an information request from the National Centre. A failure to furnish the National Centre with the requested information may be reported to the Minister (a cabinet member designated by the president to administer the act), who must take the necessary steps to ensure compliance. Accordingly, the provision does not allow for failure to provide the information requested.

In addition, the DMA empowers the relevant authorities to issue regulations and directions to deal with a national disaster. Consequently, the Disaster

8 Presidency of the Republic of South Africa. (2020, 22 June). Op. cit.

9 http://www.cogta.gov.za/cgta_2016/wp-content/uploads/2016/06/DISASTER-MANAGEMENT-ACT.pdf

Management Regulations, 2020[10] were issued, in terms of which the Electronic Communications, Postal and Broadcasting Directions, 2020 (Electronic Communications Directions)[11] were issued. The latter provided for tracking and tracing of persons. In terms of Direction 8.1, electronic communication network service licensees and electronic communication service licensees, as well as the internet and digital sector in general, are required to provide location-based services in collaboration with the relevant authorities identified to support designated departments to assist and combat the spread of COVID-19. Moreover, Direction 8.2 requires the South African Post Office to avail its national address system to assist the relevant authorities to track and trace individuals that have been infected or come in direct contact with infected persons. The South African Post Office's database may be correlated with other sources from the government or the private sector.

Although the Electronic Communications Directions do not provide for penalties for failure to comply with them, section 60(1) of the DMA provides that it is an offence to fail to comply with a request made by the National Disaster Management Centre in terms of section 18(1). Section 60(2) further provides that if convicted, the accused will be liable for a fine or imprisonment not exceeding six months or both.

In addition, sections 7 and 8 of the Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002 (RICA)[12] provide that state agencies are permitted to surveil citizens without an interception direction where the aim is to prevent serious bodily harm or determine a location during an emergency. An emergency is not defined in RICA. Furthermore, section 8(3) provides that telecommunication service providers must determine the location of the sender of a communication and furnish the details to law enforcement. Failure to comply with requests in terms of RICA also constitute an offence for which the telecommunications service provider or their employees will be liable for a fine or imprisonment. Accordingly, in its efforts to collect information necessary to inform its strategies to curb COVID-19, the National Disaster Management Centre may make requests for information in terms of RICA.

As the infection rate in South Africa rose, the Department of Co-operative Governance and Traditional Affairs (Department of Co-operative Governance) issued amended regulations so as to provide for contact tracing. According to Regulation 11H(2) of the Department of Co-operative Governance Regulations,[13] the National Department of Health is required to develop and maintain a database to enable the tracing of "persons who are known or reasonably suspected to have come into contact with any person known or reasonably suspected to have contracted COVID-19." Regulation 11H(3) further provides for the information

10 https://www.gov.za/sites/default/files/gcis_document/202004/43258rg11098gon480s.pdf

11 https://www.gov.za/sites/default/files/gcis_document/202003/43164gon-417.pdf

12 https://www.justice.gov.za/legislation/acts/2002-070.pdf

13 https://www.gov.za/sites/default/files/gcis_document/202004/43199rg11078-gon446.pdf

that should be included in the tracing database, which includes the individual's name, identity numbers and residential and other addresses where the individual could be located, and cellular phone numbers of all persons who have been tested for COVID-19, the COVID-19 test results of all such persons, as well as the details of the known or suspected contacts of any person who tested positive for COVID-19.

Moreover, Regulations 11H(6) and (7) require that when testing for COVID-19, the person testing is required to obtain as much information as is available at the time of testing and submit it to the Director General: Health, for inclusion into the tracing database. This information includes the above-mentioned information as well as a copy of the passport, driver's licence or identity book of the person tested. In addition, Regulation 11H(10) provides that the Director General: Health may in writing and without prior consent direct electronic communication service providers to provide it with the location or movements of any person known or reasonably suspected to have contracted COVID-19 and the location or movements of any person known or reasonably suspected to have come into contact with a person who has tested positive for COVID-19, during the period 5 March 2020 to the date on which the national state of disaster lapses or is terminated.

To feed the contact tracing database with the required information to combat COVID-19, personal and health data is being collected from security checkpoints between provinces where citizens are tested for COVID-19, and from workplaces where employers are required in terms of the Disaster Management Act: COVID-19 Occupational Health and Safety Measures in Workplaces, 2020[14] to provide a safe environment in workplaces, which has included reporting any cases of COVID-19 or suspected cases.

Hospitals and medical facilities that have any cases of COVID-19 are required to furnish this information to the Director General: Health. Also, the provincial Health Department in Gauteng added a COVID-19 feature to the Mpilo app,[15] allowing individuals to not only access information on COVID-19, but to self-check symptoms and provide location information to emergency medical services, if needed.

As can be seen from the regulatory measures stated above, there has been an unprecedented collection of personal and health data which will result in the South African government possessing large data sets, during and after the pandemic and the national state of disaster.

To provide for the protection of this personal data, the Department of Co-operative Governance Regulations provides that the data forming part of the COVID-19 database is confidential and may not be disclosed without authorisation, unless the disclosure is necessary for fighting the spread of COVID-19. Also, this personal data is to be collected for a specific duration and is

14 https://www.gov.za/sites/default/files/gcis_document/202004/43257gon479.pdf

15 Molelekwa, T. (2019, 21 October). Mpilo app: Will using technology improve Gauteng's healthcare? *Health-e News*. https://health-e.org.za/2019/10/21/mpilo-app-will-using-technology-improve-gautengs-healthcare

to be de-identified – only if it will be used for research, studying or teaching purposes – or deleted within six weeks of the termination or lapsing of the national state of disaster. In this way, the Department of Co-operative Governance Regulations ensures that the database is protected after the pandemic and national state of disaster.

However, the Regulations do not adequately address the illegal and biased exploitation of personal data. Such large data sets are susceptible to data breaches, as was the case with the Life Healthcare Group data breach that occurred on 9 June 2020.[16]

The Department of Co-operative Governance Regulations do not provide security measures that should be taken by the National Disaster Management Centre or the Health Department so as to ensure the protection of the tracing database. These security measures are provided for in POPIA, which organisations still have 12 months to comply with. Notwithstanding, the Information Regulator issued a guidance note[17] encouraging proactive compliance with POPIA.

Additionally, the Department of Co-operative Governance Regulations provide for oversight of the contact tracing, by requiring the appointment of a designated judge. However, the designated judge is merely required to receive weekly reports from the Director General: Health setting out the location information obtained from the electronic communications service providers. Although the designated judge is empowered to provide for further steps to ensure that the right to privacy is protected, she is yet to exercise this power. Consequently, there are no security measures to provide for security and protection against data breaches, maladministration, or misuse of the database.

The limitation on any human right is permissible only when it is necessary, reasonable and in pursuance of a legitimate aim. As this is this case in South Africa at the moment, it is arguable that the limitation placed on the right to privacy is reasonable and justifiable in terms of section 36 of the constitution, as well as in terms of international norms. It is, however, unsettling that the necessary safeguards and security measures that are provided for by data protection laws were not incorporated in the Department of Co-operative Governance Regulations or any other regulations.

Furthermore, data protection regulations establish that de-identified data is not personal data because it does not belong to an identifiable individual. It would therefore be prudent, in the fight against COVID-19, to regulate the processing of de-identified data after the national state of disaster has been terminated. It is important to regulate the processing of de-identified data because of the way that data in the information age can be used, going beyond the standard uses of aggregated data, presenting a higher possibility of the data being re-identified. This, therefore, calls for additional scrutiny of the

16 Eyewitness News. (2020, 9 June). Life Healthcare Group hacked amid COVID-19 fight. *Eyewitness News*. https://ewn.co.za/2020/06/09/life-healthcare-group-hacked-amid-covid-19-fight

17 https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf

requirement to de-identify the database. Moreover, there is a need to scrutinise the methods of aggregating data and third-party handling of aggregated data to minimise threats of de-identified data being misused.

Mass collection of personal data and surveillance of citizens interfere with and violate the right to privacy, unless if it for a justifiable reason. Nonetheless, organisations, including states, should frequently and regularly evaluate the context for the intended use of data and the purpose for which it is collected, created, stored, used, processed, disclosed or disseminated. The reason for the collection may be justified, reasonable and proportionate to the intended use, but measures have to be put in place to ensure that the right to privacy is protected, even when its enjoyment is limited. It should also be recognised that for the enjoyment of their right to privacy, individuals must be protected from unlawful surveillance by other individuals, private entities or institutions, including in their place of work or study and when using public internet access points.

That said, failing to make provision for the security of the contact tracing database, as well as addressing the potential of de-identified data being re-identified, is concerning.

CONCLUSION

Principle 8 of the African Declaration provides that the right to privacy includes the right to protection of personal data while online.

Furthermore, Principle 41 of the African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019[18] (ACHPR Declaration) states that laws providing for targeted surveillance of citizens' communications should also provide for adequate safeguards protecting the right to privacy. In addition, Principle 42 establishes provisions that should be included in legal frameworks that provide for the protection of personal data, including mechanisms that ensure transparency, accountability, confidentiality and security.

As a result of COVID-19, states, South Africa included, have been collecting large amounts of personal data by making use of various methods, from physical collection of the data to the use of technology-based disease surveillance measures. The provisions of the ACHPR Declaration should be kept in mind because Principle 43 requires states to adopt, among other things, legislative measures to give effect to the ACHPR Declaration. According to Principle 43(3), states should provide detailed records of the measures implemented to comply with the ACHPR Declaration.

While the benefits of such mass collection and processing of data cannot be ignored, it is clear that international, regional and national data protection frameworks require transparent, accountable, confidential and secure methods

18 https://www.achpr.org/public/Document/file/English/Declaration of Principles on Freedom of Expression_ENG_2019.pdf

of processing personal and health data to be used, so as to safeguard the right to privacy. With POPIA provisions coming into effect after the promulgation of the DMA Regulations, special provision should have been made for the transparent, accountable and secure processing of personal and health data during and after the national state of disaster.

To minimise the negative impact on data privacy, what is needed is data protection regulations that instil transparency, accountability, confidentiality and security into the ways in which the personal data is being used to curb the spread of COVID-19. Moreover, the principles of transparency, accountability, confidentiality and security should apply after the national state of disaster has been terminated. This is imperative because de-identified data can be re-identified, thereby leaving data subjects vulnerable to data privacy violations. There is also a need to provide for the protection of de-identified data to ensure that in its anonymised format, the right to privacy is still being protected.

Finally, there are benefits in disease surveillance for the government and its citizens of South Africa. The aggregation of the personal and health data is not only beneficial for curbing the spread of COVID-19, but it can lead to very deep insights that could prevent future health pandemics or improve health systems generally. As beneficial as it is, there is also potential of abuse of databases like South Africa's contact tracing database.

RESOURCE

For more information, see "Health and Medical Privacy", a presentation delivered during the 2012 Stanford Law Review Symposium co-sponsored by the Stanford Center for Internet and Society, at https://www.youtube.com/embed/ntL4WMGkiXo?feature=oembed