Contact tracing during the COVID-19 pandemic: Protection of personal information in South Africa

Contact tracing during the COVID-19 pandemic: Protection of personal information in South Africa

I M Viljoen,[1] BPharm; **C de Villebois Castelyn,**[1,2] MDiv; **A Pope,**[3] BA, LLB, PG Dip Int Res Ethics; **M Botes,**[4] BProc, LLB, LLM, LLD; **M S Pepper,**[1] MB ChB, PhD, MD, PD

[1] *Institute for Cellular and Molecular Medicine, Department of Immunology, and SAMRC Extramural Unit for Stem Cell Research and Therapy, Faculty of Health Sciences, University of Pretoria, South Africa*

[2] *Centre for Ethics and Philosophy of Health Sciences, Faculty of Health Sciences Research, University of Pretoria, South Africa*

[3] *Department of Private Law, Faculty of Law, University of Cape Town, South Africa*

[4] *Howard College School of Law, College of Law and Management Studies, University of KwaZulu-Natal, Durban, South Africa*

Corresponding author: *M S Pepper (michael.pepper@up.ac.za)*

Containing the COVID-19 pandemic necessitates the use of personal information without the consent of the person. The protection of personal information is fundamental to the rights that ensure an open and democratic society. When regulations that limit the right to privacy are issued outside of the democratic process, every effort must be made to protect personal information and privacy. The limitation of human rights must be treated as an exception to the norm, and any regulations should be drafted to ensure minimum limitation of rights, rather than to the minimum acceptable standard. The contact tracing regulations included in the COVID-19 disaster regulations include some basic principles to ensure privacy; however, other important principles are not addressed. These include principles of transparency and data security. The envisaged future use of human data for research purposes, albeit de-identified, needs to be addressed by the COVID-19 designated judge appointed under the regulations.

S Afr J Bioethics Law 2020;13(1):X. https://doi.org/10.7196/SAJBL.2020.v13i1.718

A novel coronavirus claimed its first victims in December 2019 in Wuhan, China. The virus was named SARS-CoV-2, and the disease, coronavirus disease 2019 (COVID-19). The virus spread rapidly around the globe. By 2 May 2020, more than 3.3 million cases were confirmed, with more than 230 000 deaths. South Africa (SA) at that date had 5 950 confirmed cases, with 116 deaths.[1] On 11 March 2020 the World Health Organization (WHO) declared COVID-19 a pandemic, and on 15 March 2020 the SA government declared a national state of disaster in terms of the Disaster Management Act No. 57 of 2002.[2] Regulations to help combat the disease were published on 18 March 2020.[3]

On 2 April 2020, the SA government published contact tracing regulations to establish a new electronic COVID-19 tracing database (the tracing database).[4] The database will aggregate the personal information of people who are known or suspected to have come into contact with persons known or suspected to have contracted COVID-19. Personal data will be collected from a variety of sources, including obtaining location and mobility data from electronic communication service providers (ECSPs). The contact tracing regulations direct that the information in the database must be de-identified within 6 weeks of the lapse of the national state of disaster. Further, de-identified data shall be retained and used only for research, study and teaching purposes.

The protection of personal information is fundamental to non-discrimination, human dignity and the freedom of speech, of association, movement and trade, and government must ensure that personal information is protected. The Protection of Personal Information Act No. 4 of 2002 (POPIA)[5] has been 17 years in the making. Although it was due to take effect on 1 April 2020, this event was postponed due to the COVID-19 pandemic, which means that the POPIA is not legally binding yet.

The right to privacy and other fundamental human rights are protected in chapter 2 of the SA Constitution (the Bill of Rights).[6] In terms of section 36 of the Constitution, these rights may be limited only in terms of law of general application, i.e. within a 'reasonable and justifiable open and democratic society, based on human dignity, equality and freedom'. Factors to be considered when limitation is an issue include the nature and the purpose of the right, the nature and extent of the limitation, how the limitation relates to its purpose and whether there are less restrictive means to achieve the purpose. However, during disasters such as the COVID-19 pandemic, legal and ethical regulations often allow the usual procedures for transparent democratic law to be limited or amended to meet the urgent need brought about by the response to the disaster. Subsequently, even fundamental constitutional rights, such as the right to privacy, may be limited by regulations imposed by the minister responsible for a particular portfolio, outside of the usual democratic process.

Contact tracing is an important tool in combatting pandemics. 21st century tracing mechanisms include access to electronic location and communication data, which were not widely available in previous pandemics. Such access, inevitably, requires the limitation of certain human rights, sometimes without warning to, or consultation with, the persons concerned.

This article seeks to analyse the legal and ethical aspects of the regulatory provisions introduced to trace potentially infected

persons who have had contact with a COVID-19 carrier, including the justification for limiting certain human rights, more specifically the right to privacy. Furthermore, it seeks to briefly address these explored aspects to suggest safeguards for the current and future use of collected data in the tracing database.

COVID-19

COVID-19 is in many cases an asymptomatic or mild to moderate disease that can be treated at home, although some people may need hospitalisation and possible intensive care. The percentage of confirmed cases that require hospitalisation can vary greatly between countries and age groups. Even though only a small percentage need hospitalisation and intensive care, the infectious nature of COVID-19, coupled with the absence of a vaccine and an effective cure, cause a higher number of sudden hospitalisations than most healthcare systems can effectively accommodate. This necessitates that the rate at which newly infected persons (cases) are added to the system is slowed to a level that does not exceed health system capacity. This 'flattening of the curve' can be achieved by voluntary or compulsory quarantine or isolation measures, which include nationally declared lockdowns. The time bought by the slowing mechanism allows governments to scale up their treatment capacity. As more capacity becomes available, an increased case rate can be better managed. Compulsory lockdowns are drastic measures that severely restrict freedom of movement, freedom to trade and freedom of assembly, among other rights. An alternative to lockdowns is the rapid detection and isolation of infected persons.

Transmission

SARS-CoV-2 is primarily transmitted by droplets expelled by coughing, sneezing or even speaking. Social distancing aims to avoid these forms of transmission. While most droplets are relatively large and precipitate fast, others are fine aerosol particles (<5 µm) that can remain suspended in the air and be dispersed by airflow. Where droplets and aerosols land on surfaces, the virus particles can survive for up to 72 hours, and can lead to contact transmission.[7] This is the reason for recommending frequent hand washing and surface sanitising. SARS-CoV-2-positive individuals become contagious several days before the onset of symptoms, and are most contagious about 1 day before symptoms are evident.[8] The relatively short incubation and infectious period makes contact tracing, screening and quarantine extremely time sensitive.

Tracing

Identification of infected persons and their contacts can be achieved in two ways: mass testing and contact tracing. As testing results are only valid for the point in time when the test is conducted, the same people will have to be tested repeatedly. An alternative to extensive testing is intensive testing in areas where a high prevalence of infection has been identified. Contact tracing entails locating and screening persons who were potentially in contact with people infected with the virus, and then proactively quarantining and monitoring them. As asymptomatic COVID-19 patients are also contagious, tracing and screening can be extended to include contacts of still unconfirmed cases. This is referred to as 'one step ahead' contact tracing. Finding and reaching out to contacts of someone who has tested positive for an infectious pathogen is a labour-intensive and time-consuming process. The WHO reports that, in Wuhan alone, more than 1 800 epidemiology teams, with at least 5 people per team, traced, quarantined, monitored and tested contacts when necessary.[9] In SA, approximately 20 000 people have been trained to assist with contact tracing. In addition, and specific to the COVID-19 pandemic, countries are increasingly employing digital technologies in efforts to contain the spread and impact of COVID-19. This includes digital surveillance and collection of people's personal data, the use of big data and artificial intelligence.

Surveillance technologies

Covert surveillance technologies used by governments (especially since the 9/11 incident of 2001) include mass surveillance using facial recognition, biometric data, tracking of financial transactions and communication monitoring. Such surveillance also includes gathering mobility and location data using cell tower data.

In SA, cellular phone data can be accessed under section 7(1) and (2) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002 (RICA),[10] and under s 205 of the Criminal Procedure Act No. 51 of 1977.[11] The COVID-19 pandemic has led to the overt use of some of these technologies. Overt use means that use is published and authorised in the regulations in terms of the Disaster Management Act, even though the process of imposing the regulations may not follow the usual procedures for new legislation.

Smartphone applications

The use of smartphone apps as virtual health passports and to obtain anonymised aggregated mobility data and proximity monitoring is being explored worldwide, including in the European Union (EU) and China, albeit with varying degrees of privacy protection. China received praise from the WHO for its use of 'Health Code', a smartphone app that shares with the police the personal information and accurate global positioning system (GPS)- and Bluetooth-derived location, movement and proximity data of its 700 million users. Through the app, access to transport, stores or even housing complexes can be restricted according to the user's COVID-19 status. The police can also access people's status and link it to facial recognition technology to identify and locate them.[12-14] This system may be compared with that in the EU, where one of the key regulatory requirements is protection of personal data and privacy. In SA, smartphone app use is currently not a viable option because many people do not have smartphones.

Cell tower metadata

Cell tower metadata, supplied by ECSPs, relies on signal strength and delay times to triangulate the position of a cellular phone. This method is highly inaccurate, and even under ideal conditions and with a high density of cell towers, it can only locate a phone to approximately 100 m. Buildings scatter signals, and in rural areas with few towers, triangulation is not possible. Using this technology, it is also impossible to identify close contacts within 2 - 3 m of infected persons (such as waiting at a bus stop), or to do retrospective traces. Considering these limitations, it is highly unlikely that cellular telephone tracing using cell tower metadata can make a contribution to identifying or locating COVID-19 cases or contacts. This makes the choice of this technically inappropriate method questionable.

COVID-19 tracing database

Data privacy principles

Personal data protection is fundamental to privacy, non-discrimination, human dignity and the freedom of speech, association, movement and trade, all of which are central to an open and democratic society based on human dignity, equality and freedom. Protection of personal data is also an essential enabler of trust in governments.[15] The government must ensure that personal data are collected, stored, processed, distributed and disposed of in a manner that respects human rights and balances the limitations imposed thereon during the COVID-19 pandemic fairly and justifiably.

During the past decade, aspirational professional guidelines for ethical data management have been developed. Governments have also developed some of these guidelines into legislation for the protection of personal data/information (the terms personal data and personal information are used interchangeably in this article). Generally, the principles contained in these guidelines are based on the basic ethical principles of beneficence, non-maleficence, distributive justice (equality) and respect for persons (dignity and autonomy). From a legislation perspective, the EU General Data Protection Regulation (GDPR)[16] is arguably the most developed regulatory instrument, and has been further improved and strengthened as a result of legal challenges by civil society. The European Data Protection Board (EDPB) is the independent authority that ensures consistent compliance with the GDPR by following guidelines issued by the EDPB. Most recently, on 21 April 2020, the EDPB issued two important guidelines on the processing of health data for research purposes in the context of the COVID-19 outbreak. The guidelines aim to shed light on the most urgent legal questions concerning the use of health data, such as the legal basis of processing and further processing of health data for the purpose of scientific research, the implementation of adequate safeguards and the exercise of data subject rights in the EU.[17,18]

International industry watchdogs and human rights organisations have also issued general guidelines for ethical data management, and more specific guidelines to protect people's privacy during the COVID-19 pandemic.[19,20]

The POPIA, which was set to take effect on 1 April 2020, has been postponed as a result of the COVID-19 pandemic. Subsequently, this Act and its regulations are not yet legally binding.

Considering the abovementioned instruments, the most essential data privacy principles include transparency, accountability, information quality, security, data subject participation and the requirements that data processing, which consists of its collection, storage and use, must be lawful and for a clearly defined purpose that will determine the limits of use.

Lawful use

For the purposes of compiling the COVID-19 tracing database, according to the amended regulations issued in terms of s 27(2) of the Disaster Management Act (the contact tracing regulations) published in the Government Gazette on 2 April 2020, the first name and surname, identity or passport numbers, residential address, cellular phone numbers, a copy of a form of photo identification and COVID-19 test results must be obtained and stored for use.

Any personal data that include information about a person's health, such as his or her COVID-19 test results, constitute special personal information. In terms of s 26 of the POPIA, there is a general prohibition on the processing of special personal information, unless processing is carried out with the consent of the data subject, or if processing is necessary for the exercising of a right or obligation in law. The contact tracing regulations require this information to be treated confidentially, and prohibit its disclosure, unless it is necessary for the purposes of addressing, preventing or combatting the spread of COVID-19. Usually a person will consent to COVID-19 testing, but if not, regulation 11H(6) of the contact tracing regulations obliges the person who is taking the sample for purposes of COVID-19 testing to obtain as much of the abovementioned information as is available at that time. Regulations 11H(7) and (8) also oblige any laboratory that has tested a sample for COVID-19 and the National Institute for Communicable Diseases to transmit the personal information of tested individuals, including their test results, to the Director General of Health (DG Health) for inclusion in the COVID-19 tracing database. ECSPs must also provide the cell tower metadata on written request by the DG Health, as discussed above.

The contact tracing regulations direct ECSPs licensed under the Electronic Communications Act No. 36 of 2005 to provide the DG Health with the location or movements of any person known or reasonably suspected to have contracted COVID-19, or to have come into contact with a person having contracted COVID-19, on written request. The period is limited between 5 March 2020 and the date on which the national state of disaster lapses or is terminated. It is important to note that any information obtained in this manner may only be obtained, used and disclosed when necessary for the purposes of addressing, preventing or combatting the spread of COVID-19 through the contact tracing process.

In view of the fact that POPIA is not yet binding law, it is legally allowable to collect, store and use the abovementioned information, even without the data subject's consent, based on compliance with the contact tracing regulations issued in terms of the Disaster Management Act, which is binding law. In addition, regulation (15)(2) of the Regulations Relating to the Surveillance and the Control of Notifiable Medical Conditions, issued in terms of the National Health Act No. 61 of 2003,[21] entitles the head of a provincial health department to obtain a court order[22] to subject a person who refuses to be tested to a medical examination, which may include the taking of any biological specimens. This way, the information prescribed in the contact tracing regulations and required by the tracing database can be lawfully obtained without the consent (or sometimes co-operation) of the infected, or suspected to be infected, individual.

Purpose and limits

The purpose of the collection of information for the tracing database is for the necessary address, prevention or combat of the spread of COVID-19. Regulation 11H(5) of the contact tracing regulations explicitly prohibits the disclosure of any information contained in the tracing database or any information obtained through this regulation, unless by a party authorised to do so, and unless the disclosure is necessary for the specified purpose. This therefore limits the amount and type of information collected, stored, processed, analysed, distributed and disposed of, as well as the period for which this will be done. Data must not be kept for longer than needed, and regulation 11H(17) of the contact tracing regulations specifically

determines that information kept in the tracing database must be de-identified (and if this is not possible, it must be destroyed) and retained and used only for research, study and teaching purposes, within 6 weeks of the national state of disaster lapsing or being terminated. Data subjects must not only be informed of the measures taken, but also have the right to verify this. In further protection of their privacy rights, the COVID-19 designated judge appointed under the regulations is also entitled to give any further directions regarding confirmation of the steps to be taken to protect the right to privacy of these data subjects, which directions given must also be tabled in Parliament in terms of regulation 11H(19) of the contact tracing regulations, to inform policies and legislation.

Transparency

Information transparency creates trust and public co-operation. For this reason, regulation 11H(16) of the contact tracing regulations directs that the DG Health must notify every person whose information has been obtained for the tracing database that such information regarding their location or movements was strictly obtained in terms of subregulation 11H(10), in other words, lawfully and for a specified purpose and time, as discussed above. In a similar vein, s 18(1)(h) of the POPIA provides data subjects the right to access and rectify any information collected, whether the supply of data is voluntary or mandatory, and if mandatory, data subjects must be informed under which law the collection was mandated and what the consequences would be of failure to comply. These measures ensure the quality of information contained in data bases such as the tracing database, and enhance transparency, trust and co-operation, which are much needed during times of pandemic.

Security safeguards

Not only people's data but also any devices, applications, networks or services involved in the collection, transmission, processing and storage of the data must be secured to protect against unauthorised or unlawful processing, loss, damage or destruction. Sections 19 - 22 of the POPIA make provision for various security measures on integrity and confidentiality of personal information, the processing of information, security measures to be taken and the notification requirements in case of any security compromises. Appropriate firewalls must be in place to ensure that data are not transferred or diverted between data capturing processes for unlawful use. Safeguards must be verified and continually updated. When operators are used, the responsible party must ensure that the operator complies with the regulations. In the case of security compromises, the regulator and data subjects must be informed.

Human rights

The protection of personal data goes much deeper than merely the protection of privacy. Personal data protection is fundamental to non-discrimination, human dignity and the freedoms of speech, association, movement and trade. These rights are central to an open and democratic society. The wellbeing of a society as a whole during any pandemic relies heavily on the codependent relationships between that society, its individuals and their government. During these times, the constitutional rights of the individual must be balanced with the need to protect the public against COVID-19, to prevent it from spreading and to save lives. Government therefore has a duty to ensure that there are adequate measures in place to protect personal data, thereby protecting the fundamental human rights of individuals and the health of the public as a whole.

Internationally, concern is growing that the measures taken in the exceptional circumstances of the COVID-19 pandemic could outlast the current crisis.[23,24] In March 2020, the United Nations special rapporteur on the right to privacy remarked: 'Dictatorships and authoritarian societies often start in the face of a threat, (and) that is why it is important to be vigilant today and not give away all our freedoms'.[25] Other international organisations point to human rights abuses during the COVID-19 pandemic, and raise the concern that the continued use of digital surveillance and data collection may adversely impact on basic human rights, including equality, privacy and human dignity, as well as freedom of speech, association and movement, and the security of the person.[26-28]

Information regulator guidance note

In the absence of an enforceable POPIA and mindful of the need for privacy protection, the information regulator urged parties to nonetheless proactively adhere to the basic principles of privacy protection, such as accountability, lawful processing, purpose of collection and processing, retention and restriction of records, quality of information and security measures, and issued a guidance note on the processing of personal information in the management and containment of the COVID-19 pandemic in terms of the POPIA.[29] The information regulator was appointed on 11 April 2014 and the powers, duties and functions of its chairperson and other members were established.[5] However, the undated guidance note was not gazetted, and is consequently not enforceable. It encourages 'proactive compliance' with POPIA; however, as the current text of POPIA is not implemented, proactive compliance is meaningless. The guidance note 'recognises the need to effectively manage the spread of COVID-19, which has necessitated the limitation of various constitutional rights of data subjects', in paragraph 2.3, followed by: 'The regulator, therefore, supports the need to process personal information of data subjects in order to curb the spread of COVID-19.' This acknowledges the need for legal effects of the provisions contained in the POPIA, but for the time being, legal reliance can only be based on the provisions of the Disaster Management Act and various regulations issued in terms thereof, or the National Health Act, which deals with communicable diseases (see above).

This statement by the regulator must be criticised for its failure to consider the context. The full rights of data subjects remain constitutionally protected during a state of disaster. Any regulations that envisage surveillance of, and data collection from, data subjects, as is currently the case in SA in terms of the regulations to the Disaster Management Act, cannot unjustly limit the constitutionally protected rights of individuals. All measures in this regard must be in line with constitutional, legal and ethical principles, including international best practices and guidelines.

Ethical considerations regarding the contact tracing regulations

Certain ethical considerations arise concerning the tracing and setting up of a database of personal identifiable data, as proposed in the contact tracing regulations. The ethical justification for limiting civil liberties, such as the right to privacy, freedom of movement,

freedom of association and freedom of trade (as stipulated in the Bill of Rights), i.e. autonomy-limiting strategies, is an important basis. These limitations can only be ethically justified if they are proportional to the seriousness of the public health threat, limited to achieve the necessary objective (i.e. clear measurable beneficial outcomes to public health, which outweigh possible individual harm), and are scientifically justified.[30] Individual harm may include negative effects on mental and physical health and stigmatisation of individuals and communities if there is a failure to keep personally identifiable data of a positive COVID-19 patient confidential, or if it is processed by a third party after contact tracing has ceased. Specific attention must be given to sensitive data and the extensive harm that could result if confidentiality were breached. Special information, as defined in POPIA, includes any information about a person's health, such as the person's COVID-19 status. Any breach in confidentiality may lead to discrimination, ostracisation, inability to access basic services and even threats of violence. In a country in which stigmatisation is prevalent, this is a serious harmful outcome that must be safeguarded against.

During the COVID-19 pandemic, the Bill of Rights and the Disaster Management Act clearly underpin the government's duty to ensure statutory protection of personal information. Proper planning for and implementation of the protection of personal information are important first steps towards ensuring protection. In the current situation, not enough attention has been given to exactly how confidentiality is protected, and what will happen if it is breached.

As stipulated in the contact tracing regulations, after contact tracing has ceased, the data will be de-identified, and will 'only be used for research, study and teaching purposes'. All data unable to be de-identified must be destroyed. Over and above the oversight these data enjoy by the appointed designated judge, the contact tracing regulations do not clarify how and by whom the data will be de-identified, repurposed or destroyed.

Anonymised v. de-identified data

At face value, it appears that great care has been taken to ensure the privacy of personal data. However, privacy concerns remain. The contact tracing regulations provide that data will be de-identified within 6 weeks of the state of disaster formally ending. De-identified data can, however, be re-identified at a later stage. All retained data must instead be anonymised entirely of all personal data that would enable a knowledgeable person to re-engineer the identity of the data subject. The regulations should ideally specify upfront which data fields must be removed, and which may be retained.

Data retention for research purposes

The purpose of the tracing database is to address, prevent and combat the spread of COVID-19, and not to aid human health research in general. Even though the regulations provide that de-identified data should be retained for possible further research, not all such research can simply be seen as further processing. Further processing of personal information must be in accordance with or compatible with the specific purpose for which it was collected. Furthermore, if human health data are used in research, the SA National Department of Health's research ethics guidelines must be adhered to, which may require further consent from data subjects.[31] Consent may not be required if data are de-identified, but an ethics committee will have to determine if the level of de-identification is adequate.

Conclusions

The COVID-19 pandemic requires rapid health interventions to limit the spread of the disease. This in turn necessitates the use of personal data to address, prevent and combat the spread of the disease. In maintaining the delicate balance between the public interest and individual privacy during a time of crisis, appropriate safeguards must be established to protect personal interests. This requires that regulations made during the COVID-19 disaster should more clearly set out how protection of personal information and human rights will be ensured.

In the context of the Bill of Rights and the Disaster Management Act, and in the absence of an effective POPIA, the full rights of data subjects remain constitutionally and legally protected during a state of disaster. The limitation of human rights must be treated as an exception to the norm, and any regulations should therefore not merely be drafted to the minimum acceptable standard, but should be drafted to ensure the minimum limitation of rights.

The contact tracing regulations are drafted to address the basic rights and principles of ethical data management, but are lacking in other important aspects. Principles that are not adequately addressed in the regulations are those of transparency, data quality, time and processing limitation, data subject participation, security and the role of the designated judge. What cannot be ignored is the fact that health data are special data, which therefore should not simply be de-identified as suggested, but rather anonymised. This necessary anonymisation is closely linked to the further processing instruction in the regulations, in which de-identified data shall be retained and used for research, study and teaching purposes. Subregulation 11H(17)(b) cannot be allowed to remain in the regulations as an afterthought. The proposed use of human data for research requires additional guarantees regarding the processes that will be followed before such data can be used. This may include obtaining ethical approval as well as informed consent from data subjects.

Acknowledgements. None.

Author contributions. MSP initiated and oversaw the project, and reviewed drafts of the manuscript throughout the process. IMV participated in early discussions, prepared the first draft and integrated co-author comments throughout. CdeVC participated in early discussions and edited the manuscript throughout. AP was involved in the first discussions at initiation of the project, and edited the manuscript throughout. MB edited the manuscript throughout.

Funding. CdeVC holds the joint Department of Science and Technology and National Research Foundation Doctoral Innovation Scholarship (grant no. SFH191127494634). MSP is funded by the SA Medical Research Council (Flagship and Extramural Unit awards) and the University of Pretoria (through the Institute for Cellular and Molecular Medicine).

Conflicts of interest. None.

1. Johns Hopkins University. Coronavirus COVID-19 global cases by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU). ArcGIS. Johns Hopkins CSSE. https://coronavirus.jhu.edu/ (accessed 2 May 2020).
2. South Africa. Disaster Management Act No. 57 of 2002.

3. South Africa. Department of Cooperative Governance and Traditional Affairs. Declaration of a National State of Disaster. Government Notice 313 in Government Gazette 43096. 15 March 2020.
4. South Africa. Disaster Management Act No. 57 of 2002. R446 Amendment of Regulations issued in terms of section 27 (2), 2020.
5. South Africa. Protection of Personal Information Act No. 4 of 2013, as amended.
6. Constitution of the Republic of South Africa, 1996.
7. Van Doremalen N, Bushmaker T, Morris D, et al. Aerosol and surface stability of HCoV-19 (SARS-CoV-2) compared to SARS-CoV-1. N Engl J Med 2020;382:1564-1567. https://doi.org/10.1056/NEJMc2004973
8. He X, Lau EH, Wu P, et al. Temporal dynamics in viral shedding and transmissibility of COVID-19. Cold Spring Harbor Laboratory. Nat Med 2020;May(epub ahead of print) . https://doi.org/10.1038/s41591-020-0869-5
9. World Health Organization. Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19). Geneva: WHO, 28 February 2020. https://www.who.int/docs/default-source/coronaviruse/who-china-joint-mission-on-covid-19-final-report.pdf (accessed 30 April 2020).
10. South Africa. Regulation of Interception of Communications and Provision of Communication Information Act No. 70 of 2002.
11. South Africa. Criminal Procedure Act No. 51 of 1977.
12. Wang M. China: Fighting COVID-19 with automated tyranny. The Diplomat, 1 April 2020. https://thediplomat.com/2020/03/china-fighting-covid-19-with-automated-tyranny (accessed 20 April 2020).
13. Yineng C. On China's 'Color codes' and life After COVID-19. Sixth Tone, 9 April 2020. http://www.sixthtone.com/news/1005452/on-chinas-color-codes-and-life-after-covid-19 (accessed 10 April 2020).
14. Mozur P, Zhong R, Krolik A. In coronavirus fight, China gives citizens a color code, with red flags. New York: New York Times, 1 March 2020. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html (accessed 12 April 2020).
15. European Commission. Communication from the Commission to the European Parliament and Council on data protection rules as a trust-enabler in the EU and beyond – taking stock. Brussels: European Commission, 24 July 2019. https://ec.europa.eu/commission/sites/beta-political/files/communication_from_the_commission_to_the_european_parliament_and_the_council.pdf (accessed 12 April 2020).
16. Eur-Lex European Union Law. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). http://data.europa.eu/eli/reg/2016/679/oj (accessed 11 April 2020).
17. European Data Protection Board. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak. Adopted 21 April 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf (accessed 25 April 2020).
18. European Data Protection Board. Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. Adopted 21 April 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (accessed 25 April 2020).
19. Wiewiórowski W. EU digital solidarity: A call for a pan-European approach against the pandemic. European Data Protection Supervisor, 6 April 2020. https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf (accessed 10 April 2020).
20. Human Rights Watch: Joint civil society statement: State's use of digital surveillance technologies to fight pandemic must respect human rights. 2 April 2020. https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight (accessed 14 April 2020).
21. National Department of Health, South Africa. Regulations relating to the surveillance and the control of notifiable conditions. Government Gazette No. 40945:604. 30 June 2017.
22. Botes WM, Thaldar DW. COVID-19 and quarantine orders: A practical approach. S Afr Med J 2020;110(6):(epub ahead of print). http://doi.org/10.7196/samj.2020v110i6.14794
23. Harari YN. The world after coronavirus. Financial Times, 13 April 2020. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 (accessed 13 April 2020).
24. Snowden E. Interview with the Copenhagen International Documentary Film Festival: Privacy in the age of coronavirus. CPH:DOX, 23 March 2020. https://www.youtube.com/watch?time_continue=1762&v=9we6t2nObbw&feature=emb_logo (accessed 23 March 2020).
25. Bacchi U. Coronavirus surveillance poses long-term privacy threat, UN expert warns. Thomson Reuters Foundation, 31 March 2020. https://www.reuters.com/article/us-health-coronavirus-privacy/coronavirus-surveillance-poses-long-term-privacy-threat-un-expert-warns-idUSKBN21I1XG (accessed 20 April 2020).
26. United Nations Office of the High Commissioner on Human Rights. COVID-19: States should not abuse emergency measures to suppress human rights. Geneva: WHO, 2020. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722 (accessed 19 April 2020).
27. Human Rights Watch. Human rights dimensions of COVID-19 response. New York: HRW, 19 March 2020. https://www.hrw.org/news/2020/03/19/human-rights-dimensions-covid-19-response (accessed 15 April 2020).
28. Zarifi S, Powers K. Human rights in the time of COVID-19: Front and centre. International Commission of Jurists, 6 April 2020. https://www.icj.org/human-rights-in-the-time-of-covid-19-front-and-centre/ (accessed 17 April 2020).
29. Information regulator, South Africa. Guidance note on the processing of personal information in the management and containment of COVID-19 pandemic in terms of the Protection of Personal Information Act 4 of 2013 (POPIA). No date. https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf (accessed 15 April 2020).
30. Ienca M, Vayena E. On the responsible use of digital data to tackle the COVID-19 pandemic. Nat Med 2020;26:463-465. https://doi.org/10.1038/s41591-020-0832-5
31. National Department of Health, South Africa. Ethics in Health Research: Principles, Processes and Structures. Pretoria: NDoH, 2015.

Accepted 5 May 2020.