

Digitalisation in the Health Sector: A South African Public Law Perspective

F Cachalia* and J Klaaren**

Online ISSN
1727-3781

P·E·R

Pioneer in peer-reviewed,
open access online law publications

Author

Firoz Cachalia
Jonathan Klaaren

Affiliation

University of Witwatersrand,
South Africa

Email

firoz.cachalia@wits.ac.za
jonathan.klaaren@wits.ac.za

Date Submitted

17 December 2021

Date Revised

30 September 2022

Date Accepted

30 September 2022

Date Published

17 November 2022

Editor Prof C Rautenbach

How to cite this article

Cachalia F and Klaaren J
"Digitalisation in the Health Sector:
A South African Public Law
Perspective" *PER / PELJ* 2022(25)
- DOI
<http://dx.doi.org/10.17159/1727-3781/2022/v25i0a12979>

Copyright



DOI

<http://dx.doi.org/10.17159/1727-3781/2022/v25i0a12979>

Abstract

The landscape of the health sector in South Africa as seen from a regulatory perspective is rapidly changing under the disruptive impact of digitalisation. Drawing on a paradigm of "strong rights" protection, particularly a robust privacy law fit for the digital age and sourced in the nation's Constitution, the operationalisation and application of health privacy regulation in post-apartheid society is briefly described. The note then enumerates and assesses several specific digital health technologies currently in use in interventions in South Africa. To do so, we adopt the international World Health Organisation (WHO) classification of digital health interventions. We also cover the recent South African response to the COVID-19 pandemic, noting the establishment in South Africa of the COVID-19 Tracing Database and subsequent technological interventions aimed at enhancing contact tracing and other responses to the pandemic. The establishment of the initial database was a development at the interface of the law enforcement and health sectors, which raised concerns regarding its risks to privacy, but it also raised hopes regarding its potential rewards in protecting public health.

Keywords

Digital health; privacy protection; regulation; risk; surveillance; technology; South Africa.

.....

1 Introduction

The impact of digitalisation on society poses and re-poses several significant questions which require regulatory intervention: What should the limits be on information stored by the government and by private actors, developed with and/or extracted from its citizens? How can that information be appropriately shared with persons and firms in the private sector in order to unlock its economic and social value? Why does it seem as if the technology changes faster than the law can respond, and consequently what are the implications of "regulatory lags"? In this age of human rights, what rights, including constitutional rights, does an individual have and should an individual have in the information about that individual?

In our view, while any particular legal system may often lag behind technological change, the law constitutes an adaptive resource that can and should respond to disruptive technological change by re-examining existing concepts and creating new, more adequate concepts. Our regulatory perspective is informed by what we call a "public law perspective", which we have more fully articulated elsewhere but which we also briefly outline here.¹ In our reading, South Africa's "transformative" Constitution reframes privacy law as both a private and a public good essential to the functioning of a constitutional democracy in the era of digitalisation. South Africa's Constitution has particularly apt characteristics for balancing the risks and benefits of "digitalisation" in the health sector. These include "strong rights" which cannot simply be traded or exchanged on a utilitarian calculus, the principles of constitutional supremacy and subsidiarity which establish a clear hierarchy of legally enforceable norms, and the component of "horizontality" which renders constitutional norms applicable to both public and private actors. These characteristics and our Constitution's conceptual structure make it possible to mesh and calibrate legal frameworks at constitutional, common law, legislative, regulatory and judge-made levels of

* Firoz Cachalia. BA BA Hons LLB LLM HDip. Adjunct Professor and Director, Mandela Institute, School of Law, University of the Witwatersrand, South Africa. Email: firoz.cachalia@wits.ac.za. ORCID: <https://orcid.org/0000-0001-7212-4406>.

** Jonathan Klaaren. BA MA JD LLB PhD. Professor, School of Law, University of the Witwatersrand, South Africa. Email: jonathan.klaaren@wits.ac.za. ORCID: <https://orcid.org/0000-0002-8732-3771>. The authors would like to acknowledge the helpful comments of the anonymous peer reviewers as well as those of Beatriz Kira. Funding for an earlier version of this paper was provided through the Digital Pathways programmes at Blavatnik School of Government, University of Oxford.

¹ Cachalia and Klaaren 2021 https://doi.org/10.35489/BSG-DP-WP_2021/04.

law. This includes the currently fragmented "codes" adopted by various private entities engaged in the health sector.

In this note we use this public law perspective to examine some of the regulatory challenges posed by the introduction of certain significant digital technologies in the South African health sector. We do so because this sector is important in its own right – public health is necessary for a healthy society – and also to further explore how and to what extent the South African constitutional framework provides resources at least roughly adequate for the challenges posed by the current era of technological change.² Others have recently explored the commercialisation of data in South Africa in the health sector, emphasising the need for sensitising the South African public to the financial and other value of their health information.³

The theoretical perspective we employ is certainly relevant to digitalisation's impact in the health sector. The social, economic and political progress that took place in the 20th century was strongly correlated with the technological changes of the first three industrial revolutions.⁴ The technological innovations associated with what many are terming "the fourth industrial revolution" are also of undoubted utility in the form of new possibilities for enhanced productivity and wealth creation, as well as the enhanced efficacy of public action to address society's basic needs such as education and public health.⁵ Of course, there are also many associated risks including those of excessive surveillance and increased social polarity.

As Part Four explores more fully below, digitalisation's potential for societal impact was on full display during the current COVID-19 pandemic. While many factors influenced social responses to the pandemic, and we do not suggest a direct relationship between digital infrastructure and effectiveness, we also note that some countries with advanced digital

² Digitisation – the storing of information in digital as opposed to analogue or paper-based forms, e.g. storing information in computers as strings of zeros and ones – has had social and economic impacts since at least the 1960s. The pace and depth of these impacts has increased since around the middle of the first decade of this 21st century. Many speak now of a process of digitalisation as a social and economic process in its own right. Appadurai and Alexander *Failure*.

³ Botes, Olckers and Slabbert 2021 *PELJ* 1-35.

⁴ See Frey *Technology Trap*.

⁵ The potential social and economic benefits of digitalisation are also stressed by some writers on the political left. See for instance Unger *Knowledge Economy*, who foresees the possibility of a knowledge economy for the many; and Mozorov 2019 *New Left Review*, discussing theories that postulate the possibility of Socialist economic planning because of information technologies and predictive analytics.

infrastructure, such as Korea, were able to respond relatively effectively in the early days of the pandemic. As an immunologist writing in the *Financial Times* observed recently: "Efficient testing, tracing and containment was a soluble technological and organisational problem."⁶ The negative costs of "technological lags" were also made plain in the case of South Africa. The government struggled to implement a technology-based contact tracing solution based on smartphone capability, which impaired its response to the public health crisis.⁷ Delays in the migration from analogue to digital broadcasting constrained the ability of our education authorities to expand online learning in disadvantaged communities under the lockdown regulations.

This note focusses only on the health sector. Our aim is to demonstrate our argument about the significance of a regulatory perspective on privacy in the age of "digitalisation plus" through raising and discussing several issues raised by digitalisation's impact in the particular sector of health. It would be possible and valuable to extend its analysis beyond health into any of numerous spheres of social life – from energy to education, and from policing to childcare. This note mainly covers technologies that have health benefits and privacy costs, but we also recognise that certain technologies have health costs and privacy benefits. Our main point is to demonstrate the value a constitutional right to privacy can bring to the regulation of digital technologies in a variety of legal frameworks and technological settings – from public to private, and from the law of the Constitution to the "law" of computer coding. As should be clear in the above, our regulatory perspective on privacy takes account of and welcomes the important and significant statute of data protection somewhat recently enacted in South Africa, the *Protection of Personal Information Act* (POPIA). But our perspective also goes beyond the set of issues to which that legislation applies.

The POPIA is an Act of Parliament with direct links to and support from the right to privacy contained in section 14 of the Constitution. The most significant operative provisions of the POPIA came into effect in 2020. POPIA established an Information Regulator responsible for enforcing both this legislation and the *Promotion of Access to Information Act* (PAIA),

⁶ Carvalho 2021 <https://www.ft.com/content/cda27366-7de5-4a90-aa17-7bf4c3981d0e>. But some states also used the COVID-19 pandemic to increase their powers of surveillance over their citizens. China went so far as to install CCTV cameras inside people's homes or just outside their front doors, according to Veliz *Privacy is Power* 30.

⁷ Klaaren and Ray 2022 *SAJHR* 12-21.

taking over responsibility for the latter law from the South African Human Rights Commission. POPIA is largely a data protection act, modelled in significant measure on the EU's General Data Protection Regulation (GDPR). It regulates the processing of personal information by making a list of principles applicable to that activity including notice and consent, correction, data minimisation, limitations of data storage and use, and access to personal information by the data subject. The legislation also provides for offences and penalties as well as data protection remedies for individuals. In response to the COVID pandemic, the Information Regulator issued a guidance note in terms of the POPIA.⁸ As the POPIA is further and comprehensively enforced by the Information Regulator through the mechanisms of litigation, POPIA codes of conduct and regulator guidance notes, it is likely to significantly transform the regulation of privacy in the health sector.

This note proceeds in three further substantive sections. Part Two begins with our public law perspective and surveys the regulatory landscape of the health sector in South Africa. We briefly describe the operationalisation and application of health privacy regulation in post-apartheid society. This prepares us to note and assess in Part Three several specific digital health technologies currently in use in interventions in South Africa. To survey and assess instances of digitalisation's impact on health, we adopt the international WHO classification of digital health interventions. This part thus is adopting a global conceptual structure to assist in the assessment of the current state of a national sector. In Part Four we focus on the recent response to the COVID-19 pandemic and discuss the establishment in South Africa of the COVID-19 Tracing Database and subsequent technological interventions aiming to enhance contact tracing and other responses. The establishment of the initial database was a development at the interface of the law enforcement and health sectors, which raised concerns regarding its risks to privacy but also raised hopes regarding its potential rewards in protecting public health.

2 The health sector in South Africa – a regulatory overview

The challenges that change in digital technology pose to existing legal frameworks (including but not limited to privacy law) require the articulation of a regulatory perspective on the constitutional right to privacy. In South Africa accomplishing this task is enabled by the Constitution. This

⁸ Information Regulator 2020 <https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf>.

Constitution has two particularly relevant and developed doctrines – horizontality and subsidiarity – that are crucial to engaging with digitalisation and articulating an adequate framework of privacy law. Additionally, with the POPIA in 2013 South Africa authorised a regulator spanning the policy domains of privacy and access to information. A further crucial set of legal resources (separate from POPIA) consists of the common law's capacity to continue to deal with many of the harms associated with digitalisation, and the potential of the constitutional right to privacy to specifically address collective harms, in addition to comprehensively overseeing privacy law.

The components of horizontality and subsidiarity are particularly relevant to the health sector in the age of digitalisation. For instance, the potential power wielded by electronic platforms is a good context for the horizontal application of rights, such as the right to health and the right to privacy. Therefore, there is a question specific to the South African context – a concept and debate that has receded to some degree from doctrinal discussions over constitutional rights in South Africa from its earlier prominence in the early 1990s, when the Constitution and the Bill of Rights were being drafted – should horizontality come back into our current discussion over privacy (and health) in South Africa as a useful and progressive concept? As for subsidiarity, its conceptual structure mirrors the comprehensive and powerful logic of digital technology, building its very coherence and structure as a network out of numerous individual links – for example, from the Constitution to legislation, from legislation to subordinate legislation, from subordinate legislation to regulatory interpretation, from regulatory interpretation to judge-made decisions and the like. Both components are, we argue, crucial for enabling law to respond to the costs and benefits of digitalisation.

South Africa's health sector has seen considerable change in the past 25 years. It has moved significantly in the direction of becoming a deracialised, comprehensive and integrated health system. As the government has recently noted,⁹

[a]verage life expectancy at birth declined over the first decade of democracy, largely due to the devastating impact of the HIV and AIDS epidemic, reaching a low of 54 years in 2005. Since then, however, it has improved steadily, reaching 64.6 years in 2019.

One significant and celebrated feature of South Africa's health system is its relatively high rates of use of healthcare services. For instance, in 2015 94%

⁹ DPME 2019 https://www.gov.za/sites/default/files/gcis_document/201911/towards25yearreview.pdf.

of pregnant women received antenatal care, 96% delivered in a healthcare facility, and 97% were attended at delivery by a skilled medical practitioner.¹⁰ In terms of absolute number, the use of public healthcare has increased dramatically, to some extent addressing an apartheid-era healthcare deficit. The number of such healthcare visits per annum has increased from 67 million in 1998 to "close to 120 million annually by March 2019" with 71.5% of households using public sector clinics in 2018.¹¹ Persistent challenges that remain include addressing the inequalities of the cost and level of care between the public and the private healthcare sectors, the explosion of litigation and claims related to medical negligence against the state in recent years, and the declining levels of community participation in healthcare provision.¹²

In addition to the professional and statutory bodies overseeing the work of the professionals and other personnel key to the health sector, several other statutory bodies exist to regulate various non-personnel aspects of activity in the health sector. These include the South African Health Products Regulatory Authority (SAHPRA) and the Office of Health Standards Compliance (OHSC). SAHPRA has statutory authority to regulate clinical trials, medicines, and health devices. OHSC monitors health establishments' compliance with health standards. Significant activities, such as the establishment, licensing and funding of hospitals remain regulated by officials in the national and provincial line departments of health, which share constitutional jurisdiction over this competence and implement the *National Health Act* 61 of 2003 and other sector legislation.¹³ Other regulatory bodies set up by their own empowering statutes include the Compensation Commissioner for Occupational Diseases and the Road Accident Fund.¹⁴

To understand the privacy-related issues raised by the intervention of digital technology in the health sector (as discussed further in Part Three) we need to understand the regulation of health devices.¹⁵ This is within the competence of SAHPRA, a body built from the Medicines Control Council.¹⁶ As currently implemented, SAHPRA's regulatory model has several key

¹⁰ Pillay and Motsoaledi 2018 *BMJ Global Health* 1.

¹¹ DPME 2019 https://www.gov.za/sites/default/files/gcis_document/201911/towards25yearreview.pdf at 101.

¹² Klaaren *et al* 2020 *SAMJ* 1-4.

¹³ Stevenson *National Health Act Guide* 68-99.

¹⁴ Carstens and Pearmain 2009 *Medicine and Law* 94.

¹⁵ Tomlinson 2020 <https://www.dailymaverick.co.za/article/2020-09-03-the-tangled-web-of-medical-device-regulation-in-sa/>.

¹⁶ Klaaren 2021 *Journal of Asian and African Studies* 82.

components, including the regulation of establishments and regulation through reliance. SAHPRA currently licenses establishments, though it does not require them to prove that their quality management systems are up to international standards. SAHPRA also regulates the devices that such establishments (as well as ones outside South Africa's borders) produce through the key mechanism of reliance – meaning that, especially for high-risk products, if evidence is presented that the relevant devices are registered in one of six recognised jurisdictions, the device is eligible to meet the standards of section 21 authorisation and thus to be marketed in South Africa. Reliance here refers to "relying" on registration or authorisation in other countries".¹⁷

An alternative route to these six jurisdictions is for a device to be pre-qualified by the WHO. The six jurisdictions are: Australia, Brazil, Canada, the EU, Japan, and the USA. This reliance component to health sector regulation is similar to the reliance component of Information and Communications Technology (ICT) regulation by South Africa's telecommunications and broadcasting regulator, the Independent Communications Authority of South Africa (ICASA). SAHPRA has demonstrated some capacity to respond to the COVID-19 pandemic with some agile regulatory arrangements, although it does not appear to be well co-ordinated with other important government entities such as the National Treasury and the National Department of Health (NDOH).¹⁸

International health regulations approved by the World Health Assembly, part of an international treaty system linked to the WHO, generally become part of South African law via the *International Health Regulations Act 28 of 1974*. Those international regulations were used by the WHO Director-General to declare the COVID-19 pandemic a public health emergency of international concern and to co-ordinate a global response.

This note does not examine in any detail the regulatory instruments and processes by which it is possible that some (or even many) risks to privacy may be actively mitigated. Such processes may include the use of privacy and data protection impact assessments as employed in comparative jurisdictions.¹⁹ For instance, section 19(2) of POPIA requires a risk assessment that might be interpreted (or supplemented, as was the case

¹⁷ Tomlinson 2020 <https://www.spotlightnsp.co.za/2020/09/03/in-depth-the-tangled-web-of-medical-device-regulation-in-sa/>.

¹⁸ Tomlinson 2020 <https://www.spotlightnsp.co.za/2020/09/03/in-depth-the-tangled-web-of-medical-device-regulation-in-sa/>.

¹⁹ Clarke 2009 *CLS Rev* 123-135; Wright and Raab 2004 *IRLCT* 277-298.

with the Stellenbosch University Privacy Regulation) to include a privacy impact assessment.²⁰ The 2018 regulations enacted in terms of the POPIA empower information officers to conduct such privacy impact assessments.²¹

3 Digital health interventions in South Africa

The impact of digital technology globally has been considerable, and its impact on the health sector in South Africa has been no exception. Since around 2000 the term "digital health" has been used to recognise and evaluate this development.²²

In official discourse the digitalisation of health services is a policy priority in order to achieve integration and transformation towards a primary care-based health system and overcome apartheid-era legacy divides.²³ South Africa adopted its second generation policy in this policy document, the National Digital Health Strategy for South Africa, 2019–2024, in 2019.²⁴ As early as 2014 the sector had gazetted a National Health Normative Standard Framework for Interoperability in eHealth, e.g. an interoperability framework.²⁵ As of 2021 59 million individuals were reported by the national department to be registered on the Health Patient Registration System, drawing these registrations from 3,220 primary health care facilities and 52 hospitals.²⁶

While it is not necessary here to dive fully into the related literature, one helpful line of analysis in gaining insight into the challenges and opportunities posed in this sector has been developed by the WHO as an aid for policymakers. In 2018 the WHO classified the full range of different digital health interventions by user type as a tool towards understanding the impact of digital technology in health.²⁷

²⁰ Staunton *et al* 2020 *IDPL* 13.

²¹ Regulations Relating to the Protection of Personal Information in GN 1383 in GG 42110 of 14 December 2018.

²² Mathews *et al* 2019 *Npj Digital Medicine* 1-9.

²³ Abrahams and Burke 2022 <https://www.wits.ac.za/media/wits-university/research/tayarisha/documents/SA-EU-Dialogue-ODG-SA-experience.pdf> 13.

²⁴ Abrahams and Burke 2022 <https://www.wits.ac.za/media/wits-university/research/tayarisha/documents/SA-EU-Dialogue-ODG-SA-experience.pdf> 13.

²⁵ Abrahams and Burke 2022 <https://www.wits.ac.za/media/wits-university/research/tayarisha/documents/SA-EU-Dialogue-ODG-SA-experience.pdf> 14.

²⁶ Abrahams and Burke 2022 <https://www.wits.ac.za/media/wits-university/research/tayarisha/documents/SA-EU-Dialogue-ODG-SA-experience.pdf> 14.

²⁷ WHO 2018 <https://apps.who.int/iris/bitstream/handle/10665/260480/WHO-RHR-18.06-eng.pdf>.

Therefore, we use here the classification scheme of digital health interventions proposed by the WHO to identify some of the current constitutional issues in the South African health sector occasioned by digitalisation. The WHO's overview of digital technologies helpfully distinguishes four types based on the targeted primary user: health clients; healthcare providers; health system or resource managers; and data services. In this part of this publication, we identify and briefly discuss a significant digital health intervention in each of these four primary WHO categories.

3.1 Health clients

Interventions directed at health clients include targeted client communication, personal health tracking, and on-demand information services. While there are many examples that could (and should) be examined further in this category,²⁸ we identify just one here: a client-focussed technology developed in a public/private partnership: MomConnect.

The laudable and celebrated high rate of use of health services by pregnant women in South Africa is associated with a significant digital health intervention – MomConnect, technology developed by the NDOH and a range of implementers including the Praekelt Foundation, a private non-profit corporation.²⁹ The MomConnect service provides twice-weekly health information messages to pregnant women and allows them to submit compliments and complaints about the health services they have received at local level. MomConnect is argued to be innovative, in particular in incorporating the registration of the pregnancies and in using interoperable technology.³⁰ Looked at through a global lens, MomConnect is one of only five mobile health information messaging programmes to have scaled to

²⁸ For instance, as Cohen *et al* 2020 *The Lancet* 163 observed: "[t]hese technological offerings can address unmet healthcare needs by circumventing traditional intermediaries, such as payers (eg, insurance companies and governments), clinicians, employers, and the pharmaceutical industry, and provide patients with direct access to health-related data and services. Like other industries that empower consumers with easily accessible information and services, direct-to-consumer digital health might similarly transform healthcare. Fitness trackers, sleep monitors, and wearables that detect arrhythmias are the current leading technologies. Direct-to-consumer healthcare already represents a US\$700 billion industry and includes over-the-counter drugs, care management in retail clinics, hearing aids, glasses, contact lenses, and nutraceuticals."

²⁹ Pillay and Motsoaledi 2018 *BMJ Global Health* 1.

³⁰ Pillay and Motsoaledi 2018 *BMJ Global Health* 1.

over one million beneficiaries. Further, it is the only programme across the world to have attained population-level coverage of more than 60%.

There are, however, privacy issues with this programme. It "collects the user's identification number and facility code during registration, enabling future linkages with other health and population databases and geolocated feedback."³¹ As Barron *et al* noted:

[t]he privacy, data security and confidentiality aspects of holding individual patient information in a national system in South Africa ... came to the fore for the first time in MomConnect.

These issues have not gone unnoticed but still remain live. Rules and operating procedures were established for hosting and accessing such data, which are held on secure NDOH-controlled servers and subject to the same rules as other routine data systems.³² From our perspective, above and beyond these issues of informational privacy, the digital technology encompassed in MomConnect represents a significant use of private power, albeit for a public purpose. From a public law perspective, the regulation of this power is largely embedded in agreements and in contractual frameworks rather than in a framework of primary or subordinate legislation. This mode of regulation may pose questions well suited for addressing with doctrines of horizontality, as POPIA may not reach all the privacy issues posed by this technology.

3.2 Healthcare providers

Digital health interventions directed at healthcare providers include client health records, referral co-ordination, and prescription and medication management. One challenge evident through the healthcare sector in South Africa is that of patient and healthcare worker autonomy and potential infringements on individual privacy. While using technology to facilitate the quality and delivery of healthcare, digital technologies may of course infringe on rights to privacy, intruding in particular into the liberal zones of individual privacy. Informational privacy issues may be associated with healthcare workers as well as with patients and research participants.

In respect of personal health records stemming from healthcare services, the advent of digital health has raised particular issues.³³ One issue is the

³¹ Barron *et al* 2018 *BMJ Global Health* 1.

³² Barron *et al* 2018 *BMJ Global Health* 4.

³³ Els and Cilliers 2018 *African Journal of Science, Technology, Innovation and Development* 725-734; Abrahams and Burke 2022

access of patients to their own medical records in situations where a third party had an interest in those records. At least in part in response to changing business models enabled by digital technology, "[h]ealthcare practitioners are increasingly called upon to step out of their usual clinical roles to evaluate and report on claimants for non-clinical purposes, such as eligibility for insured benefits".³⁴ For the most part, the challenges posed by this second set of technologies may be addressed through a combination of statutory and regulatory instruments. Going forward, the key statute will be POPIA and its interaction with the regulatory framework of the *National Health Act*. While the constitutional right to privacy will play a background and supervisory role, it is unlikely to need to provide the primary role in this category.

3.3 Health system or resource managers

Digital health technologies directed at health system or resource managers include technologies for supply chain management, public health event notification, civil registration and vital statistics, and health financing. At least one continued type of operation of South Africa's second-generation pandemic response technologies fits in this category as a public health event notification to health system managers – the use of data at the aggregate level for population mobility and COVID-19 hotspot mapping. As the successive technologies to the COVID-19 Tracing Database (discussed further in Part Four) have been developed and deployed, there has remained a residual thread of operations continuing at (among others) the Council for Scientific and Industrial Research (CSIR), the public organisation initially chosen to house the database, and which is in touch with a range of key public health entities including the NDOH. Since May 2020 one of the major South African telecommunications companies, Vodacom, has provided aggregate data for use in population mobility estimates to several public entities including the CSIR, the National Institute for Communicable Diseases (NICD), the City of Cape Town, and the Free State and Eastern Cape Provincial Departments of Health.

These estimates do not include individual contact tracing data. In a separate operation the CSIR uses anonymised contact tracing data from the NICD to compile approximated COVID-19 hotspot maps.³⁵ This hotspot mapping – which was also an ambition of the tracing database – may be addressed

<https://www.wits.ac.za/media/wits-university/research/tayarisha/documents/SA-EU-Dialogue-ODG-SA-experience.pdf> 14.

³⁴ Van Niekerk 2019 *South African Journal of Bioethics and Law* 32-37.

³⁵ Klaaren and Ray 2022 *SAJHR* 20.

from the point of view of the recently proposed group right to reasonable inferences from data. In a related policy debate, some have asked whether the practice of disclosing specific infection statistics implicates a group right of privacy.³⁶ Where the POPIA proves inadequate or runs out, the regulation of these technologies may primarily be a matter of the constitutional right to health and its interaction with the general limitations clause, section 36.

The purpose of most of the digital technologies in this third classification is to advance public health through the effective and efficient use of limited resources. However, the implementation of this effort is done through the full variety of statutory, regulatory and private law-based instruments, as well as instruments not usually thought of as classically regulatory, such as information technology standards and computing languages and coding protocol. This welter of texts (and codes) is reflective of the fast-changing health sector in the 21st century. As can be inferred from the parallel surveillance context of the *AmaBhungane* case,³⁷ the constitutional right to privacy may well find employment here via either or both of the horizontality and the subsidiarity doctrines noted above.

3.4 Data services

Digital health technologies directed towards data services include data collection, management and use, data coding, locational mapping, and data exchange and interoperability. One practice in this category that poses issues at the interface of technology and privacy is biorepository (or biobank) research in Africa. Biorepository research is based on the collection, processing, storage, and distribution of biological materials for future health research. Spreading globally and growing rapidly since around 1990, in part due to the facilitation and acceleration of digital technology, several biorepositories have been established in Africa in the last 20 years, associated with the development of bioinformatics and computational biology. Treading in sensitive terrain from the point of view of decoloniality as well as dignity and privacy, the pending application of South Africa's privacy law to its biorepository research facilities raises important questions of lawfulness as well as the continuing ability of South African facilities to collaborate with their African counterparts in jurisdictions without robust privacy laws and enforcement.³⁸ There are between ten and twenty

³⁶ Wachter and Mittelstadt 2019 *Colum Bus L Rev* 494-620.

³⁷ *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC* 2021 3 SA 246 (CC).

³⁸ Staunton *et al* 2020 *IDPL* 160-179; Staunton *et al* 2019 *SAMJ* 468-470.

biorepositories in South Africa that currently fall under the somewhat ambiguous regulation of the NDOH and the National Health Laboratory Service.³⁹

The now-inoperative COVID-19 Tracing Database – with its avowed purpose of using geolocational data for contact tracing – also falls squarely in this final WHO category and is discussed further in Part Four. The regulation of this set of technologies includes cross-border agreements with both public and private entities and falls at the intersection of the constitutional rights of privacy, health, and academic freedom (the right to research).

Unsurprisingly, technological developments along the above lines resulted in several recent disputes in the South African courts. One pitted two South African health and life insurers against each other in the High Court, debating whether the publicly available scoring system of one could be used commercially by the other.⁴⁰ Another dispute has seen an enquiry (launched in July 2019) by several well-respected senior advocates into the question of whether medical schemes' data analysis practices have unlawfully discriminated against claims lodged by African and Indian medical practitioners, resulting in an interim report and threats of court actions.⁴¹ Both of these cases fall within the category of data services.

Informed by the doctrines of horizontality and subsidiarity, a privacy law developed by the public law perspective we have detailed elsewhere and outlined above in Part One can provide a powerful and flexible instrument for engaging with the issues posed by the digital technologies of all these types. A fundamentally reconceptualised privacy right cannot on its own address the regulatory issues identified in the health sector, but it can engage with private power, such as that on display in several instances above, perhaps most notably in the technologies directed at data services. And it is able to interact with the multiple obstacles and opportunities posed at multiple legal levels: by other constitutional rights, by statutes including but not limited to POPIA and the *National Health Act*, by subordinate legislation, by professional rules (including those made in terms of the regulations of the Health Professions Council of South Africa),⁴² by

³⁹ Andanda and Govender 2015 *Journal of Law, Medicine and Ethics* 787-800.

⁴⁰ *Discovery Ltd v Liberty Group Ltd* 2020 4 SA 160 (GJ).

⁴¹ Mabelane 2020 <https://www.power987.co.za/news/report-into-medical-aid-schemes-racial-profiling-yet-to-be-released/>.

⁴² HPCSA 2016 https://www.hpcsa.co.za/Uploads/Professional_Practice/Conduct%20%26%20Ethics/Booklet%209%20Keeping%20of%20Patient%20Records%20September%20202016.pdf.

agreements and other instruments using private law to accomplish public ends, and even by some avenues of control not usually thought of as within the purview of a Constitution at all, such as industrial standards and model computing codes.

4 The COVID-19 Tracing Database and subsequent technological initiatives to enhance digital contact tracing in South Africa

In addition to the more gradual change caused by the onset of digital technology in the health sector, the sudden onset and extensive duration of the COVID-19 pandemic has sparked sharp change, much of this also taking place through digital technology. One prominent example in the health sector was the series of attempts by the South African government to enhance and empower state contact tracing capacity. These efforts have raised several privacy issues similar to those identified and discussed in Part Three. The first of these attempts – the COVID-19 Tracing Database – lies in the overlap between the health sector and law enforcement.

While these developments are covered in depth elsewhere,⁴³ a brief overview of this series of technological interventions helps to identify potential risks and rewards and to understand how these are assessed in the current regulatory privacy regime. It also demonstrates the key argument of our public law perspective on constitutional privacy law in the era of digitalisation – that South Africa's constitutional regime possesses the legal resources, although not the decided body of case law, to engage with the full spectrum of benefits (social and economic) as well as harms (surveillance and dissemination) that are emerging in contemporary South African and global society.

In response to the COVID-19 pandemic South Africa engaged in a sequence of attempted technological enhancements to the crucial pandemic-fighting function of contact tracing. Each of these attempts presents a case of pushing the integration of digital technology into existing systems (or the creation of a new system) to protect and promote public health. In the first of these efforts, the government established a tracing database in March and April 2020. This technology aimed to collect both aggregated and individualised mobility and geolocational data on COVID-19 cases and their contacts. With its broad and deep evidence base, the database had the potential to assist health system managers with policy

⁴³ Klaaren and Ray 2022 *SAJHR* 12-21.

formulation and to provide a database to assist with contact tracing, thus falling into the third and fourth of the WHO's classifications. The database came with both risks and rewards, including the significant potential to assist with public health.⁴⁴

About four months into South Africa's pandemic response the NDOH announced that the tracing database was no longer operating, although the legal machinery for the database and its oversight remains in place. As things happened, while there were no judicial responses to the privacy risks of the tracing database, it turned out that a privacy-guaranteeing regulatory structure – the appointment of a designated judge with a mandate to oversee privacy protection and make recommendations to government – was instrumental in noting and communicating the inability of the tracing database to perform its function due to the lack of precision in the key category of data it had decided to collect – geolocational data. In layman's terms, the triangulated information gathered from cell phone towers simply was not clean or precise enough to assist materially with contact tracing.⁴⁵ This is an example of a "technological lag", one arguably negatively impacting South Africa's response to the pandemic.

South Africa's replacement initiative in this space was COVIDConnect, a technology developed by Telkom/BCX and the Praekelt Foundation partnering with the NDOH.⁴⁶ According to BCX, the COVIDConnect app

[a]llows the public to screen for COVID-19 on WhatsApp ...; [s]hares test results and provides advice to those who have tested positive for COVID-19 through GovChat's LetsTalk line [a]n SMS is sent to inform when results are available; [and a]nonymously alerts people who may have been in close contact with someone who tests positive for COVID-19.

Further, COVIDConnect

[d]raws data from various data sources and provides district health teams with the ability to search for individuals via a table interface, giving them direct communication with the individual via SMS [through building] a map view of SA with functionality to filter by province and include all primary infected individuals listed on the system, whilst identifying the close contacts and [h]eat map overlays indicate the volumes of infected relative to population estimates.

COVIDConnect differs from applications used elsewhere by relying on persons testing positive with COVID-19 to voluntarily provide the names and

⁴⁴ Klaaren *et al* 2020 *SAMJ* 1-4.

⁴⁵ Wachter and Mittelstadt 2019 *Colum Bus Rev* 494-620.

⁴⁶ BCX 2020 <https://www.bcx.co.za/insights/bcx-and-the-department-of-health-partner-to-launch-covidconnect/>.

contact details of their contacts.⁴⁷ Its power to engage in hotspot mapping – which was also an ambition of the tracing database – is within the ambit of one part of the developing concept of privacy noted above, the right to reasonable inferences from data. With its dual focus on clients as well as healthcare managers, this second technological intervention straddles the first and the third of the WHO's categories discussed in Part Three (health clients; and health system or resource managers).⁴⁸

In its third major technological intervention, on 1 September, the government launched COVID Alert SA, a Bluetooth application and part of the Google/Apple Exposure Notification (GAEN) system operated by Google and Apple. This was stated to be part of the COVIDConnect platform.⁴⁹ With its strong privacy protections and its limited aims, this technology fits squarely back in the WHO's first category – digital health interventions directed at health clients. South Africa's ambitions to technologically support contact tracing – at least judging by the high-profile technological interventions surveyed here – have been directed to clients and health system managers and not to healthcare providers, nor to the data systems providers. Furthermore, their development appears to be more significantly influenced by the capacity of the state to work with the private sector to devise such initiatives as well as the availability of the technologies than by any clearly defined campaign to counter new threats to privacy or a popular backlash along such lines.⁵⁰ This matter will be one worthwhile to monitor.

5 Conclusion

This note has briefly surveyed the regulatory structures in the South African health sector and some of the interventions made by digital technologies impacting in that sector. We have drawn from both a South African regulatory perspective on the constitutional law of privacy in the era of digitalisation and from a global regulatory classification of digital health technologies. The note has also presented an account of the series of technological attempts that the South African Government embarked on to enhance and empower state contact tracing capacity early in the COVID-19 pandemic.

⁴⁷ Voigt 2020 <https://www.dailymaverick.co.za/article/2020-07-28-the-trial-and-error-of-covid-19-digital-contact-tracing-in-south-africa/>.

⁴⁸ Wachter and Mittelstadt 2019 *Colum Bus Rev* 494-620.

⁴⁹ NDOH 2020 <https://sacoronavirus.co.za/2020/09/01/download-the-app-every-covid-alert-sa-app-download-means-more-lives-saved-in-sa/>.

⁵⁰ Wachter and Mittelstadt 2019 *Colum Bus Rev* 494-620.

There are several policy implications that flow from this research. Perhaps the most important is the need to acknowledge the entangled public and private nature of the social action at issue in these questions. This need is shown in the above account of the South African technological responses to the COVID-19 pandemic as well as in the overview of the numerous technological interventions in the health sector. Policymakers who examine exclusively either the public or the private sides of these social questions and their potential answers are unlikely to enable an adequate and effective response.

Second, we endorse the call for legislation on cybersecurity and regulations to promote open data initiatives for the re-use of public sector information to be enacted. -- beyond the POPIA and legislation on cybercrimes -- in order to provide an environment within which South Africa can take best advantage of digitalisation.⁵¹

Third, policymakers should acknowledge and monitor the costs these technologies are causing our society to incur as against the benefits arising from them. Policy instruments such as privacy impact assessments should be given more prominence and considered as important instruments aiding in social and economic regulation. Such assessments could be used to guide social and economic regulatory choices prior to health care activities as large as pandemics and as small as routine care, and to document, chart and assess the complexity of the impacts of the technologies afterwards.

Bibliography

Literature

- Andanda and Govender 2015 *Journal of Law, Medicine and Ethics*
Andanda P and Govender S "Regulation of Biobanks in South Africa" 2015 *Journal of Law, Medicine and Ethics* 787-800
- Appadurai and Alexander *Failure*
Appadurai A and Alexander N *Failure* (Polity Cambridge 2019)

⁵¹ Abrahams and Burke 2022 <https://www.wits.ac.za/media/wits-university/research/tayarisha/documents/SA-EU-Dialogue-ODG-SA-experience.pdf>.

Barron *et al* 2018 *BMJ Global Health*

Barron P *et al* "Mobile Health Messaging Service and Helpdesk for South African Mothers (MomConnect): History, Successes and Challenges" 2018 *BMJ Global Health* 1-6 DOI: <http://dx.doi.org/10.1136/bmjgh-2017-000559>

Botes, Olckers and Slabbert 2021 *PELJ*

Botes M, Olckers A and Slabbert ML "Data Commercialisation in the South African Health Care Context" 2021 *PELJ* 1-35

Carstens and Pearmain 2009 *Medicine and Law*

Carstens P and Pearmain D "The Regulatory Framework of the South African Health System: Comparative Health Systems Reform" 2009 *Medicine and Law* 91-124

Clarke 2009 *CLS Rev*

Clarke R "Privacy Impact Assessment: Its Origins and Development" 2009 *CLS Rev* 123-135

Els and Cilliers 2018 *African Journal of Science, Technology, Innovation and Development*

Els F and Cilliers L "A Privacy Management Framework for Personal Electronic Health Records" 2018 *African Journal of Science, Technology, Innovation and Development* 725-734

Frey *Technology Trap*

Frey CB *The Technology Trap: Capital, Labor and Power in the Age of Automation* (Princeton University Press Princeton 2019)

Klaaren 2020 *Journal of Asian and African Studies*

Klaaren J "Regulatory Politics in South Africa 25 Years After Apartheid" 2020 *Journal of Asian and African Studies* 79-91

Klaaren and Ray 2022 *SAJHR*

Klaaren J and Ray B "South Africa's Technologies Enhancing Contact Tracing for Covid-19: A Human Rights and Techno-Politics Assessment" 2022 *SAJHR* 1-23

Klaaren *et al* 2020 *SAMJ*

Klaaren J *et al* "South Africa's COVID-19 Tracing Database: Risks and Rewards of Which Doctors Should Be Aware" 2020 *SAMJ* 1-4 DOI: <https://dx.doi.org/10.7196/SAMJ.2020.v110i7.14852a>

Mathews *et al* 2019 *Npj Digital Medicine*

Mathews S *et al* "Digital Health: A Path to Validation" 2019 *Npj Digital Medicine* 1-9 DOI: <https://doi.org/10.1038/s41746-019-0111-3>

Mozorov 2019 *New Left Review*

Mozorov E "Digital Socialism: The Calculation Debate in the Age of Big Data" 2019 *New Left Review* 33-67

Pillay and Motsoaledi 2018 *BMJ Global Health*

Pillay Y and Motsoaledi PA "Digital Health in South Africa: Innovating to Improve Health" 2018 *BMJ Global Health* 1-3 DOI: <http://dx.doi.org/10.1136/bmjgh-2018-000722>

Staunton *et al* 2019 *SAMJ*

Staunton C *et al* "Safeguarding the Future of Genomic Research in South Africa: Broad Consent and the Protection of Personal Information Act No 4 of 2013" 2019 *SAMJ* 468-470

Staunton *et al* 2020 *IDPL*

Staunton C *et al* "Protection of Personal Information Act 2013 and Data Protection for Health Research in South Africa" 2020 *IDPL* 160-179

Stevenson *National Health Act Guide*

Stevenson S (ed) *The National Health Act Guide* 3rd ed (Siber Ink Cape Town 2019)

Unger *Knowledge Economy*

Unger R *The Knowledge Economy* (Verso Brooklyn 2019)

Veliz *Privacy is Power*

Veliz C *Privacy is Power: Why and How You Should Take Back Control Over Your Data* (Penguin London 2020)

Van Niekerk 2019 *South African Journal of Bioethics and Law*

Van Niekerk M "Providing Claimants with Access to Information: A Comparative Analysis of the POPIA, PAIA and HPCSA Guidelines" 2019 *South African Journal of Bioethics and Law* 32-37

Wachter and Mittelstadt 2019 *Colum Bus L Rev*

Wachter S and Mittelstadt B "A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI Survey: Privacy, Data, and Business" 2019 *Colum Bus L Rev* 494-620

Wright and Raab 2014 *IRLCT*

Wright D and Raab C "Privacy Principles, Risks and Harms" 2014 *IRLCT* 277-298

Case law

AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC 2021 3 SA 246 (CC)

Discovery Ltd v Liberty Group Ltd 2020 4 SA 160 (GJ)

Legislation

Constitution of the Republic of South Africa, 1996

International Health Regulations Act 28 of 1974

National Health Act 61 of 2003

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

Government publications

GN 1383 in GG 42110 of 14 December 2018

Internet sources

Abrahams and Burke 2022 <https://www.wits.ac.za/media/wits-university/research/tayarisha/documents/SA-EU-Dialogue-ODG-SA-experience.pdf>

Abrahams L and Burke M 2022 *Report on the South African Experience in Open Digital Governance* <https://www.wits.ac.za/media/wits-university/research/tayarisha/documents/SA-EU-Dialogue-ODG-SA-experience.pdf> accessed 24 August 2022

BCX 2020 <https://www.bcx.co.za/insights/bcx-and-the-department-of-health-partner-to-launch-covidconnect/>

BCX 2020 *BCX and the Department of Health partner to launch COVIDConnect* <https://www.bcx.co.za/insights/bcx-and-the-department-of-health-partner-to-launch-covidconnect/> accessed 19 January 2022

Cachalia and Klaaren 2021 https://doi.org/10.35489/BSG-DP-WP_2021/04

Cachalia F and Klaaren J 2021 *Digitalisation, the "Fourth Industrial Revolution" and the Constitutional Law of Privacy in South Africa: Towards a Public Law Perspective on Constitutional Privacy in the Era of Digitalisation* https://doi.org/10.35489/BSG-DP-WP_2021/04 accessed 9 September 2022

Carvalho 2021 <https://www.ft.com/content/cda27366-7de5-4a90-aa17-7bf4c3981d0e>

Carvalho T 2021 *What We Have Learnt About the Limits of Science* <https://www.ft.com/content/cda27366-7de5-4a90-aa17-7bf4c3981d0e> accessed 26 September 2022

Cohen *et al* 2020 *The Lancet*

Cohen AB *et al* "Direct-to-Consumer Digital Health" 2020 *The Lancet* DOI: [https://doi.org/10.1016/S2589-7500\(20\)30057-1](https://doi.org/10.1016/S2589-7500(20)30057-1)

DPME 2019 https://www.gov.za/sites/default/files/gcis_document/201911/towards25yearreview.pdf

Department of Planning, Monitoring and Evaluation 2019 *Towards a 25 Year Review: 1994-2019* https://www.gov.za/sites/default/files/gcis_document/201911/towards25yearreview.pdf accessed 19 January 2022

HPCSA 2016 https://www.hpcsa.co.za/Uploads/Professional_Practice/Conduct%20%26%20Ethics/Booklet%209%20Keeping%20of%20Patient%20Records%20September%20%202016.pdf

Health Professions Council of South Africa 2016 *Guidelines for Good Practice in the Health Care Professions: Guidelines on the Keeping of Patient Records, Booklet 9* https://www.hpcsa.co.za/Uploads/Professional_Practice/Conduct%20%26%20Ethics/Booklet%209%20Keeping%20of%20Patient%20Records%20September%20%202016.pdf accessed 24 August 2022

Information Regulator 2020 <https://info regulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf>

Information Regulator 2020 *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)* <https://info regulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf> accessed 24 August 2022

Mabelane 2020 <https://www.power987.co.za/news/report-into-medical-aid-schemes-racial-profiling-yet-to-be-released/>

Mabelane K 2020 *Report into Medical Aid Schemes' Racial Profiling Yet to Be Released* <https://www.power987.co.za/news/report-into-medical-aid-schemes-racial-profiling-yet-to-be-released/> accessed 19 January 2022

NDOH 2020 <https://sacoronavirus.co.za/2020/09/01/download-the-app-every-covid-alert-sa-app-download-means-more-lives-saved-in-sa/>

National Department of Health 2020 *Download the App – Every COVID Alert SA App Download Means More Lives Saved in SA* <https://sacoronavirus.co.za/2020/09/01/download-the-app-every-covid-alert-sa-app-download-means-more-lives-saved-in-sa/> accessed 19 January 2022

Tomlinson 2020 <https://www.dailymaverick.co.za/article/2020-09-03-the-tangled-web-of-medical-device-regulation-in-sa/>

Tomlinson C 2020 *The Tangled Web of Medical Device Regulation in SA* <https://www.dailymaverick.co.za/article/2020-09-03-the-tangled-web-of-medical-device-regulation-in-sa/> accessed 19 January 2022

Voigt 2020 <https://www.dailymaverick.co.za/article/2020-07-28-the-trial-and-error-of-covid-19-digital-contact-tracing-in-south-africa/>

Voigt E 2020 *The Trial and Error of Covid-19 Digital Contact Tracing in South Africa* <https://www.dailymaverick.co.za/article/2020-07-28-the-trial-and-error-of-covid-19-digital-contact-tracing-in-south-africa/> accessed 19 January 2022

WHO 2018 <https://apps.who.int/iris/bitstream/handle/10665/260480/WHO-RHR-18.06-eng.pdf>

World Health Organisation 2018 *Classification of Digital Health Interventions v1.0* <https://apps.who.int/iris/bitstream/handle/10665/260480/WHO-RHR-18.06-eng.pdf> accessed 19 January 2022

List of Abbreviations

BMJ Global Health

British Medical Journal Global Health

CLS Rev

Computer Law and Security Review

Colum Bus L Rev

Columbia Business Law Review

CSIR

Council for Scientific and Industrial Research

DPME

Department of Planning, Monitoring and Evaluation

GAEN	Google/Apple Exposure Notification
GDPR	General Data Protection Regulation
HPCSA	Health Professions Council of South Africa
ICASA	Independent Communications Authority of South Africa
ICT	Information and Communications Technology
IDPL	International Data Privacy Law
IRLCT	International Review of Law, Computers and Technology
NDOH	National Department of Health
NICD	National Institute for Communicable Diseases
OHSC	Office of Health Standards Compliance
PAIA	Promotion of Access to Information Act
PELJ	Potchefstroom Electronic Law Journal
POPIA	Protection of Personal Information Act
SAHPRA	South African Health Products Regulatory Authority
SAJHR	South African Journal on Human Rights
SAMJ	South African Medical Journal
WHO	World Health Organisation