Data Protection in Zimbabwe with Reference to the Covid-19 Pandemic and International Law

O Saki*

Online ISSN
1727-3781

P·E·R
Pioneer in peer-reviewed, open access online law publications

Author

Otto Saki

Affiliation

University of Western Cape, South Africa

Email

4119180@myuwc.ac.za

Date Submitted

22 January 2024

Date Revised

17 April 2024

Date Accepted

17 April 2024

Date Published

11 December 2024

Guest Editor

Prof BM Mupangavanhu

Journal Editor

Prof C Rautenbach

How to cite this contribution

Saki O "Data Protection in Zimbabwe with Reference to the Covid-19 Pandemic and International Law" *PER / PELJ* 2024(27) - DOI http://dx.doi.org/10.17159/1727-3781/2024/v27i0a17744

DOI
http://dx.doi.org/10.17159/1727-3781/2024/v27i0a17744

Abstract

The corona virus that caused the COVID-19 disease defied geographical boundaries, spreading faster than the measures to contain its transmission. The processing of personal health-related data became widespread as a measure to respond to the pandemic. This triggered new concerns about the possibility of there being a data crisis. Individuals suspected to be infected by COVID-19 were forced to undertake mandatory testing that involved the collection of health-related data. To limit the spread of the disease, the collection of personal data extended to secondary contacts. Personal health-related data are very prone to abuse, and this data included secondary data inconsistent with initial collection purposes. Admittedly, such risks are not new. Prior to the pandemic, health-related data were processed through electronic health (e-health) platforms. The health-related data processing methods during the pandemic were insufficient to meet the data protection principles of consent, transparency, purpose and storage, potentially violating the right to privacy. Globally, expectations are that countries should have data protection laws informed by established principles regulating the processing of personal data. While, Zimbabwe had not enacted the *Cyber and Data Protection Act* (CDP Act), which lists some of the data principles, this paper relies on existing laws to determine whether Zimbabwe is still abiding by constitutional and international human rights standards in protecting personal data privacy. The paper examines the development of data principles and their application in Zimbabwe in respect of health-related data protection during the pandemic. The paper 1) analyses the existing laws and their protection of personal health-related data; 2) explores the incorporation of data principles in COVID-19-related responses including in national laws as informed by international laws; and 3) highlights the gaps in both law and practice as they relate to the handling of personal health-related data in Zimbabwe during the pandemic. The paper concludes that even if the existing laws on data privacy were not comprehensive and even if the CDP Act came too late, the global regulations, the sectoral laws and other guidance accessible to Zimbabwe in responding to the pandemic would have sufficed to avert a data pandemic during the health pandemic and allowed Zimbabwe to be compliant with international data protection standards.

Keywords

COVID-19; pandemic; processing; data subject; privacy; sensitive personal data; health-related data; Zimbabwe.

.....

1 Introduction

On the 17th of March 2020 Zimbabwe declared the COVID-19 pandemic a national disaster.[1] The *Civil Protection Act* section 27 provides that the President may declare a state of disaster triggering assistance to persons affected or likely to be affected by the disaster.[2] Under the *Civil Protection Act* the declaration of a state of disaster must be for three months and may be extended before its expiration.[3] Before the expiration of the disaster declaration, the government declared COVID-19 a formidable epidemic through the Minister of Health, basing the declaration on section 68 of the *Public Health Act* 11 of 2018 (PHA).[4] The specification of COVID-19 as a formidable epidemic triggered the implementation of public health standards and measures (PHSMs) to curb the virus from spreading. As expected, the PHSMs limited the population's constitutional rights, including the rights to privacy, assembly, association and trade, the purposes being to reduce and limit the virus transmission vectors. Additional modalities for the tracing of medical contacts which relied on the collection of personal health data were introduced.

Prior to the pandemic, medical institutions were implementing e-health solutions which are cost-effective information and communication technologies deployed in support of health and health-related fields and are dependent on the processing of health-related data.[5] As the pandemic response measures included physical distancing, the use of e-health increased exponentially.[6] E-health has also advanced in other contexts. For instance, medical institutions use data driven technologies for effective medical care such as use of oxygen monitoring devices or smart beds, enabling the provision of real time monitoring and patient assistance.[7]

For Zimbabwe, the paper identifies a major limitation in the use of e-health platforms as being the lack of data protection mechanisms and infrastructure.[8] This article aims to understand the nature and extent of data

* Otto Saki. LLB Hons (Uni Zim) LLM Human Rights Law (Columbia University, USA) LLM Information Communication Technology Law (Open University, Tanzania) LLD Candidate, University of the Western Cape, South Africa. Email: otto.saki@caa.columbia.edu. ORCiD: https://orcid.org/0009-0002-8924-9365.

1 Statutory Instrument 76 of 2020: Civil Protection (Declaration of State of Disaster: Rural and Urban Areas of Zimbabwe) (COVID-19) Notice, 2020.

2 Section 27 of the *Civil Protection Act*, 1989 (Chapter 10:06).

3 Section 27(2) of the *Civil Protection Act*, 1989 (Chapter 10:06).

4 Statutory Instrument 77 of 2020: Public Health (COVID-19 Prevention, Containment and Treatment) Regulations, 2020.

5 Tsiko 2019 https://www.herald.co.zw/telemedicine-revolutionises-zim-healthcare.

6 PSMI 2020 https://www.psmi.co.zw/2020/06/08/192323/.

7 Ghersi, Mariño and Miralles 2018 *BMC Medical Informatics and Decision Making* 1-12.

8 Furusa and Coleman 2018 *South African Journal of Information Management* 1; Khumalo 2017 *Library Philosophy and Practice* 1-18.

processing in Zimbabwe during the pandemic and the consistent application of data processing principles, even before the *Cyber and Data Protection Act* (CDP Act) was gazetted. The paper undertakes an analysis of processing personal data during a health pandemic, informed by the evolution of data principles which are internationally accepted parameters for data processing. The paper proceeds to analyse three principles, namely those of consent, the purpose of the limitation, and transparency, that were considerably impacted or waived during the pandemic. The paper explores the most relevant human rights instruments, national laws and comparative responses to the pandemic. It concludes with specific recommendations on the gaps in the law and in practice that require immediate attention to avert a data pandemic.

1.1 Re-defining personal data under COVID-19

The response to COVID-19 depended on the collection of personal data, which is any information that relates to an identified or identifiable natural person.[9] This includes information that is directly or indirectly attributable to an individual such as a person's physical, physiological, mental, economic, cultural or social identity.[10] These personal details can determine or influence the way in which a person is treated or evaluated.[11] The critical elements of designating personal data is the content of the data, the purpose of the data and the results obtained from the processing of personal data. Once one of these three elements is satisfied, then such information constitutes personal data.[12]

Zimbabwe passed its data protection law on 3 December 2021. The Zimbabwe CDP Act[13] describes personal information as including blood type or inheritable characteristics, and information about a person's health care history, including the person's physical or mental disabilities.[14] The CDP Act further defines sensitive data to include health information and genetic information about an individual.[15] What classifies personal data as sensitive data are risk levels associated with unauthorised processing and

---

9 *Amann v Switzerland* ECHR App No 27798/95 (16 February 2000) para 65; s 1 of the *Protection of Personal Information Act* 4 of 2013 defines personal data to include an identifiable juristic person; Art 4 of the *General Data Protection Regulation* (2016) (GDPR).

10 EU Data Protection Working Party 2007 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf 4.

11 EU Data Protection Working Party 2005 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf 8.

12 These three elements (content, purpose and result) must be considered alternative conditions, not cumulative ones. See EU Data Protection Working Party 2007 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf 10-11.

13 *Cyber and Data Protection Act*, 2021 (Chapter 12:07) (CDP Act).

14 Section 3 of the CDP Act.

15 Section 3 of the CDP Act.

disclosure. This categoric statement is not oblivious of the difficulties in defining what constitutes sensitive data, due to contextual factors.[16] However, there is consensus that health-related data constitutes sensitive personal data, and the CDP Act draws that conclusion.[17] Therefore, if the reaction to the COVID-19 pandemic was premised on the processing of sensitive health data, then the unauthorised processing of health-related data had a significant impact on the data subject's fundamental rights and freedoms.[18]

Human rights courts have observed that individuals are generally reluctant to provide their health-related data for fear of stigma and discrimination.[19] In responding to the pandemic, government authorised public and private medical institutions to collect personal health data. As of September 2021 Zimbabwe had approved over 134 testing facilities.[20] All public facilities such as supermarkets, banks and hardware stores were required to take temperature readings and record the relevant personal information of clients.[21] This presented a huge risk to the health-related data of consumers and the public as many of these public and private entities did not have the requisite training and infrastructure for confidentiality.[22] The confidentiality of health information advances patient's privacy and reinforces confidence in medical services, especially where there are medical conditions that might result in discrimination.[23] Other than stigma, health-related data are easily commodified and commercialised. This is one of the reasons why data protection principles emerged.

2 Evolution and implementation of data principles

Data protection principles emerged in the USA as the Code of Fair Information Practices in Health, Education and Welfare report of 1973.[24] At

16 Lloyd *Information Technology Law* 44; *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), as revised in 2013 (*OECD Guidelines*) Explanatory Memorandum 19.

17 *Report of the Special Rapporteur on the Right to Privacy, Joseph A Cannataci* UN Doc A/76/220 (2021).

18 Recital 51 of the GDPR. This is why the general position on sensitive personal data is first to prohibit processing, then to approve it based on exceptions under Art 9(1) of the GDPR.

19 *Z v Finland* 1997 ECHR 10 para 96.

20 Chipendo *et al* 2022 *Pan African Medical Journal* 2.

21 This was done manually with basic thermometers, infrared temperature readings or mobile applications such as Quick Response (QR) codes or bar codes used to check in to venues, hospitals and public places.

22 Article 9(3) of the GDPR; the processing of health data for medical purposes under Art 9(2)(h) must be done by a professional who is bound by professional confidentiality.

23 As the pandemic was first recorded in China, Chinese nationals, foreigners and travelers were perceived as vectors.

24 USA Department of Health 1973 https://aspe.hhs.gov/reports/records-computers-rights-citizens.

the time the US government was grappling with the proliferation of public and private databases containing important personal data including sensitive health data. The report disclosed that some health datasets had "50 million characters of data, or approximately 3,500 characters per patient-record."[25] This was in 1973, when computing capacity was in its infancy. The vast amount of this information confirms that health-related data have broad characteristics and with technological advances, more characters of data are easily identified and generated.

The Code of Fair Information Practices listed five principles of data processing. The first principle challenged the secrecy of personal data record-keeping systems. While for individuals secrecy constitutes an element of informational privacy, for public and private databases secrecy is not maintaining privacy.[26] Secrecy prevents accountability.[27] Secondly, as a principle, all data subjects have to be able to establish how their personal information is being recorded and used.[28] If the database exists in secrecy, then this principle is moot. Thirdly, information collected for a specific purpose had to be used only for that purpose unless the data subject consented to other uses. This purpose limitation principle is still relevant, despite the emergence of newer data purposes without the data subject's knowledge and consent.[29] Fourthly, the principles required every individual to have the ability to correct or amend recorded personal information. This is an equally relevant principle in modern times and is enshrined in many data protection frameworks.[30] Lastly, databases had to assure data integrity, and prevent misuse.[31] Notwithstanding their limitations, the fair information practices heralded the development of revised and improved data processing principles.[32] Though groundbreaking, the Code of Fair Information Practices was confounded by the conceptual vagueness of the notion of privacy, the challenges to the achievement of data anonymity, and re-identification of health-related data.[33] Technical data safeguards such as anonymisation proved

25 USA Department of Health 1973 https://aspe.hhs.gov/reports/records-computers-rights-citizens. US medical facilities had databases containing administrative information on patients, the statistical reporting of ailments, lists of high-risk groups needing special attention, and records of medical tests.

26 Solove 2002 *CLR* 1087.

27 Mokrosinska 2020 *Critical Review of International Social and Political Philosophy* 415.

28 The USA already had a *Freedom of Information Act* passed in 1966.

29 Esayas 2017 *IJLIT* 139.

30 Section 16(1) of the *Protection of Personal Information Act* 4 of 2013; Art 5(1)*(d)* of the GDPR.

31 *S and Marper v United Kingdom* 2008 ECHR 1581 para 103.

32 USA Department of Health 1973 https://aspe.hhs.gov/reports/records-computers-rights-citizens.

33 Hoofnagle 2014 https://ssrn.com/abstract=2466418.

insufficient to protect privacy as re-identification through the mixing of data sets and computational analysis increased.[34]

In 1980 the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* incorporating fair information practices were adopted.[35] The *OECD Guidelines* include provisions on collection limitation, data quality, purpose specification, use limitation, security safeguards, individual participation and openness. The principle of accountability was introduced in 2013 as nations responded to technological changes which raised newer challenges. The accountability principle is contentious as a standalone principle as it is more of an omnibus and primary principle for data processing.[36] The *OECD Guidelines* provide member states with a wide margin of manoeuvre in enacting domestic frameworks.[37] That said, the strength of these non-mandatory guidelines was in their persuasive influence in many data protection standards beyond OECD member states.[38]

The limitations of fair information practices necessitated their coding into principles of enforceable treaty provisions. The Council of Europe (CoE) introduced the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (*Convention 108*), which entered into force in 1981. *Convention 108* is the first global instrument on data protection for CoE members and non-members.[39] Zimbabwe has not been invited to join. The CoE adopted the 1973 and 1974 resolutions on data protection principles in the private and public sectors[40] and on automated databanks respectively.[41] The CoE resolutions paved the way for

34 Rocher, Hendrickx and De Montjoye 2019 *Nature Communications* 1-9.

35 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

36 Article 5(2) of the GDPR provides that "the controller shall be responsible for and be able to demonstrate compliance with paragraph 1 [art 5(1)*(a)-(f)* which lists the 6 principles on data processing]."

37 *OECD Guidelines* para 19(a)-(e).

38 *OECD Guidelines* para 2; Kirby 2011 *IDPL* 7, 10; Alunge "Consolidating the Right to Data Protection" 192-207.

39 The *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data* (1981) (*Convention 108*). Some of the non-Council of Europe members include Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Russian Federation, Senegal, Tunisia and Uruguay. *Convention 108* was amended by the *Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (2018) (*Convention 108+*).

40 *Council of Europe Committee of Ministers Resolution (73) 22 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector* (1973), adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies.

41 *Council of Europe Committee of Ministers Resolution (74) 29 on the Protection of the Privacy of Individuals* vis-à-vis *Electronic Data Banks in the Public Sector* (1974), adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.

Convention 108, which was geared towards advancing the compatibility of national laws and practices among CoE states.[42] Compared with the earlier standards development efforts, the *Convention 108* had the strength to influence the national accommodation of the data protection principles and practices.[43] The CoE *Convention 108* was brought up to date and a new convention adopted in 2018, which is due to enter into force in October 2023. The modernised *Convention 108+* incorporates technology-driven privacy management measures such as privacy by design.[44] This confirms the importance of adopting proactive approaches in managing privacy.[45]

In 1995 the European Union (EU) adopted a data directive expanding on the data protection principles for member states.[46] The application of the directive varied from direct incorporation to incorrect transpositioning by member states, further undermining the harmonisation of data protection.[47] In short, according to Lloyd, the implementation of the directive was fragmented and incongruous.[48] In 2016 the EU adopted the General Data Protection Regulation (GDPR). Though binding, the GDPR provided room for manoeuvre through various opening clauses.[49] For instance Article 8(1) of the GDPR enables state parties to depart from the age of consent in relation to information by changing it from 16 years to 13 years, a permitted lower age.[50] Mindful of the limits of international law, the GDPR continues to seek increased legal harmony in addressing the challenges of the abuse of personal data.[51] In furtherance of this objective the GDPR reaffirms seven data processing principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; integrity and confidentiality; and accountability.[52] The GDPR is touted as the global gold standard on data protection. As of January 2021, according to Greenleaf, over 145 countries had adopted data protection laws evidencing GDPR dominance.[53]

Data protection and privacy are a priority for Africa despite the absence of a specific right to privacy in the *African Charter on Human and Peoples'*

---

42 *Council of Europe Committee of Ministers Recommendation 509* (1968) Assembly Debate on 31 January 1968.

43 Greenleaf 2012 *IDPL* 68.

44 Article 10 of *Convention 108+*.

45 Braman 2011 *New Media & Society* 798.

46 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* OJ L 281/31 (1995).

47 Chen 2016 *IDPL* 315.

48 Lloyd *Information Technology Law* 37.

49 Chen 2016 *IDPL* 314 lists several opening clauses in the GDPR which give Member States wide discretion.

50 Treaties allow for reservations. See Art 2(1)(d) of the *Vienna Convention on the Law of Treaties* (1969).

51 Waltraut 2014 *IDPL* 274.

52 Article 5(1)-(2) of the GDPR.

53 Greenleaf 2021 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348 3-5.

Rights (the Charter).[54] The African Union *Convention on Cyber Security and Personal Data Protection* (the *Malabo Convention*) entered into force on 8 June 2023.[55] The *Malabo Convention* is a comprehensive treaty covering electronic transactions, personal data protection, cyber security and cybercrime. Article 13 of the *Malabo Convention* specifies six principles on data processing, namely consent and legitimacy; lawfulness and fairness; purpose, relevance and storage; accuracy; transparency; and confidentiality and the security of personal processing. These principles are like those of the GDPR and CoE *Convention 108*. The *Malabo Convention* prohibits the processing of sensitive personal data including the state of health of the data subject unless there is consent, or information in the public domain, or it is required for public interest purposes.[56] In addition, the *Malabo Convention* incorporates the data subject's rights to access, objection and erasure.[57]

The GDPR, the CoE *Convention 108+* and the *Malabo Convention* are the binding instruments on data protection incorporating the data principles essential in data protection. The *OECD Guidelines* are equally persuasive for member states from an economic perspective. Zimbabwe is not a signatory to the *Malabo Convention*, and neither has it been invited to join the CoE *Convention 108+*. The *OECD Guidelines* and GDPR are relevant from an economic perspective, with the GDPR being more frequently referenced in national laws. This is the proverbial "Brussels effect".[58] This article will examine consent, purpose and storage limitation, and transparency as the overarching principles advancing the privacy of health-related data and as those most implicated during the response to the COVID pandemic in Zimbabwe.

2.1 The making and implementation of data principles in Zimbabwe

Zimbabwe adopted a data protection law in 2021, after years of deliberation.[59] This paper will not exhaust the issues with the data protection

---

54 The *African Charter on Human and Peoples Rights* (1981) has no specific provision on privacy; but this can be read into the Charter through Art 60 of the Charter and principle 40(1) of the African Commission on Human and Peoples Rights *Declaration of Principles on Freedom of Expression and Access to Information* (2019), which provides: "everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information." Zimbabwe ratified the Charter. The *African Charter on the Rights and Welfare of the Child* (1990) protects the right to privacy of the child in Art 10, and Zimbabwe is a state party.

55 *African Union Convention on Cyber Security and Personal Data Protection* (2014) (the *Malabo Convention*).

56 Article 14 of the *Malabo Convention*.

57 Articles 9-23 of the *Malabo Convention*.

58 Bradford 2012 *North Western University Law Review* 1.

59 The first public move in this direction was recorded during the attempt at the Harmonisation of ICT Policies in Sub-Saharan Africa (HIPSSA) supported by the International Communication Union, European Union, and the African Union. A

law, but a few aspects are relevant.[60] The CDP Act retains most of the provisions based on the data principles reflected in international standards but fails to incorporate data protection by design as a principle. The data protection by design requires technologies to incorporate data privacy from the outset.[61] This principle was particularly relevant to the pandemic response, which used mobile applications for surveillance and tracing. Other principles are covered as follows: data quality is covered in section 7; the purpose and generality in sections 8-9; and sections 13-14 provide for the duties of data controllers and the rights of data subjects. The CDP Act provides for security (section 18), openness of processing (section 23) and accountability (section 24) as principles. The Act is clumsily drafted as these principles could have been sequential. However, more worrying is the fact that the Act then takes a security approach to data protection which is premised on the state rather than the data subject. The CDP Act of Zimbabwe has as its objective:

> to increase cyber security in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects.[62]

This statement of the objective of a data protection law cannot begin with the need to increase cyber security in the interest of the security of the state. This assumes that cybersecurity improves data protection, yet cyber security is only one element of data protection. An earlier version of the Act was the *Data Protection Act*, which had its title and objective changed in the *Cyber and Data Protection Act*.[63] The objective of the recalled *Data Protection Act* was "to increase data protection in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects."[64]

The difference between "increase[ing] cyber security" and "increase[ing] data protection" appears to be minor, whereas it is in fact essential. For example, the Act gives wide powers to the Minister responsible for the Cyber Security and Monitoring Centre, and the Minister for Information "may give directions" on the implementation of the provisions relative to the processing of sensitive information affecting national security or the

---

mission to Zimbabwe for the transposition of the Southern African Development Community (SADC) Cybersecurity Model Laws took place from 15-19 July 2013.

60 This is the subject of the author's PhD thesis on data protection in Zimbabwe, in which ch. 5 specifically examines these issues. Part of this analysis is reflected in that chapter.

61 European Data Protection Board 2020 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

62 Section 2 of the CDP Act.

63 The Act was gazetted on 3 December 2021 and re-gazetted with the correct title and chapter number on 11 March 2022 by GN 492/2022.

64 Section 2 of the CDP Act.

interests of the state.[65] Under the CDP Act, the designated data protection authority, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ),[66] is accountable to the Minister, and not independent.[67] Transparency and accountability as data principles are fundamental to data protection, and impact on a wide range of other principles, such as consent.

2.2 Consent

The processing of personal data under the Zimbabwe CDP Act must take place when there is consent. This applies to both sensitive and non-sensitive data.[68] The CDP Act defines consent as "any manifestation of specific unequivocal, freely given, informed expression of will by which the data subject or his or her legal, judicial or legally appointed representative accepts that his or her data be processed."[69]

There are four conditions of consent that must be satisfied.[70] First, consent must be unambiguous, meaning that there must be no doubt about what the data subject intends. This is called unambiguous consent.[71] Secondly, there must be clear affirmative action. Unequivocal steps should be taken, beyond completing a form or ticking a box, to constitute informed consent.[72] Thirdly, consent must be freely given by an individual capable of consenting, if it is to constitute capable consent. There must be no coercion or external pressure in the processing of personal information. If consent is obtained on false or inaccurate information, that consent is invalid. Lastly, consent must be specific and informed. This means that one must be informed of one' rights as a data subject.

Consent is the basic authorisation for a data controller to process the data subject's personal information. Hurd talks of the moral magic of consent in transforming rights and obligations.[73] The morality of the consensual process is notable, but more important is what one might call the legal magic

65 Section 11(4) of the CDP Act.
66 Section 5 of the CDP Act
67 The *Postal and Telecommunications Act*, 2000 (Chapter 12:05) constitutes the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ). Although the CDP Act says that POTRAZ is independent of directions from anyone, provisions of the *Postal and Telecommunications Act* give wide powers to the Minister, such as s 25 on directives on national interests, or conditions of service determined by the President under s 7.
68 Sections 10 and 11 of the CDP Act.
69 Section 3 of the CDP Act.
70 Article 7(1)-7(4) of the GDPR, as well as Recital 32, 33, 42, and 43.
71 Schermer, Custers and Van der Hof 2014 *Ethics Information and Technology* 175.
72 Schermer, Custers and Van der Hof 2014 *Ethics Information and Technology* 174-175.
73 Hurd 1996 *Legal Theory* 121.

of consent. Consent is how legal acts are constituted.[74] When consent is granted, it alters criminal conduct into legitimate and acceptable conduct. With the processing of COVID-19 personal data, individuals were assumed to have given their unequivocal consent.

The CDP Act prohibits the processing of sensitive data unless consent is provided, and other exceptions apply.[75] The exceptions include that "the processing is necessary for the promotion and protection of public health, including medical examination of the population",[76] or for the purposes of preventative medicine or medical diagnosis.[77] Consent is therefore not the only ground for the lawful processing of sensitive health data under data protection laws. That notwithstanding, for the processing of sensitive personal data section 11 of the CDP Act requires a data subject's explicit written consent, unless exceptions apply.[78] Explicit consent means that the data subject agrees with the particular use or disclosure of his/her personal information. The data subject needs to respond actively to the request for consent.[79] During a pandemic, obtaining explicit consent is a disproportionate effort to make and largely impractical.[80] For instance, the provision of medical care for minors must have the guardian's consent.[81] If a guardian denies consent, then data controllers can rely on other legitimate grounds.[82] In summary, consent is desirable as a condition for processing health-related data but it cannot be the only lawful ground. What is required in Zimbabwe is the specification of the various conditions in which the processing of sensitive data may be undertaken as provided in section 12(5) of the CDP Act. These conditions were not made public during the pandemic. The government issued several statutory instruments on the pandemic response but failed to provide guidance in terms of what constituted consent, even under other laws such as the PHA.[83]

---

74 Schermer, Custers and Van der Hof 2014 *Ethics Information and Technology* 171.

75 CDP Act s 11(1): written consent to process sensitive personal data; s 12(1): the processing of genetic data, biometric data and health data is prohibited unless the data subject has given written consent for the processing thereof.

76 Section 12(3)(c) of the CDP Act.

77 Section 12(3)(j) of the CDP Act.

78 Also see Art 9(1) of the GDPR.

79 Schermer, Custers and Van der Hof 2014 *Ethics Information and Technology* 175 note that high-risk categories data subjects need to take a more active and affirmative decision.

80 Section 13(e) of the CDP Act requires that a valid explanation is given for the collection of personal data.

81 Article 8 of the GDPR has specific protection requirements for children as they are less aware of the risks of processing personal data.

82 Dove and Chen 2020 *IDPL* 117.

83 *Public Health Act* 11 of 2018 (PHA).

2.3 Purpose and storage limitation

Having observed the limits of consent, the data controller must comply with other data principles. In that context, the purpose of the data processing becomes pertinent.[84] The CDP Act requires under section 9(1) that:

> data is collected for specified, explicit and legitimate purposes and, taking into account all relevant factors, especially the reasonable expectations of the data subject and the applicable legal and regulatory provisions, that the data is not further processed in a way incompatible with such purposes.[85]

This provision cannot be faulted; however, it must be bolstered by practice directives to data controllers as specific codes of conduct under the CDP Act.[86] The collection of sensitive data requires the imposition of additional safeguards and measures to ensure privacy. The screening of potential COVID-19 patients documented and exposed other health conditions which ordinarily were not disclosed or known. The processing of the data for further purposes which are incompatible with the original purpose is not permitted unless it is for research, scientific or historical purposes.[87] There are real risks of abuse of this data even when used for scientific purposes. For instance, the data may be shared with insurance companies for health risk assessments.[88] This is why the GDPR recitals notes:

> processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.[89]

If personal data is to be used for a specific purpose, it must be relevant, adequate and accurate. This principle is reflected in the CDP Act section 7(1)(*a*), quality of data and duty of controller and data processor, under section 13(*d*). Certainly, data controllers have duties and responsibilities, and describing this as a duty might have been designed to repackage the principle as an enforceable rule than an aspirational standard. During the response to the COVID pandemic, the principle was violated in several instances as governments generally and Zimbabwe in particular collected information, which was not relevant, and collecting irrelevant information constitutes a violation of privacy, as that information will not meet the purpose that it was designed to address. The word “relevant” when applied to personal data means no more than what is necessary to achieve an

---

84 Koops 2021 *Law, Innovation and Technology* 29.

85 Section 13(c)-(d) of the CDP Act repeats this provision but as a duty of the data controller or processor.

86 Section 30 of the CDP Act provides for the adoption of codes of conduct in certain categories of data controllers. This provision supplements s 12(5), which allows the data protection authority to specify conditions for processing sensitive personal data.

87 Section 9(2) of the CDP Act.

88 See the section below on how electoral voters rolls in the custody of a constitutional body were used in a campaign by the ruling party.

89 Recital 54 of the GDPR.

objective. For instance, the unlabelled data forms which were deployed during the pandemic at Zimbabwe international airports required travellers to provide information on their social relationships, their family members, and their hair and eye colours, which added very little to the effectiveness of the pandemic response.[90] In fact, it cannot be described as either necessary or proportionate.[91] This collection of personal data by an unspecified data controller vitiates consent in that a data subject will not be able to identify who the controller is or the purpose of the collection of the data, and the data subject is unable to object to the processing without detriment to his/her safety or interests. During a pandemic the health ministry as the data controller must process data only for the specified purpose of responding to the pandemic. Data processors such as medical laboratories processing health-related data on delegated authority must abide by the purpose limitation applicable to data controllers. If information is not relevant, then it is neither adequate nor accurate for the purpose and must not be processed.

The storage of personal data is a thorny issue, as databases and data warehouses are viable businesses.[92] The commodification of health-related data is inevitable. Health-related data are highly susceptible to manipulation and use for other purposes.[93] In South Africa, for instance, cybercriminals are targeting medical institutions for health-related data troves.[94] It is possible that Zimbabwe has faced similar targetting of health institutions, but no relevant information is publicly available.[95] It therefore follows that processed health-related data must be destroyed as soon as the pandemic declaration is lifted. Zimbabwe lifted the public health emergency status on 9 June 2023 through Statutory Instrument 102 of 2023.[96] Unfortunately, the instrument was silent on directives about handling the personal data collected. Zimbabwe could have been inspired by South Africa, which under

90 The copy had no official stamp or indication of which department was responsible for the collected information. The forms were titled "Data Forms". There was a separate form from the Ministry of Health.

91 *Report of the Special Rapporteur on the Right to Privacy, Joseph A Cannataci* UN Doc A/76/220 (2021) para 54 commenting on South Korea COVID-19 contact tracing applications. The UN Special Rapporteur on Privacy noted that "it would be less useful to disclose the personal profile of the confirmed person and their social relationships, such as family or acquaintances."

92 Blume 2004 *Scand Stud L* 306. Blume observes that the possession of personal data is more than an economic asset, but is probably a necessity for most corporations capable of trading on the internet

93 Zwitter and Gstrein 2020 *Journal of International Humanitarian Action* 4.

94 Mungadze 2020 https://www.itweb.co.za/content/rW1xLv59YPGvRk6m.

95 Section 19 of the CDP Act requires a data controller to notify the Authority of a data breach within 24 hours of its occurrence.

96 Statutory Instrument 102 of 2023: Public Health (COVID-19 Prevention, Containment and Treatment) (National Lockdown) (No 22) (Amendment) Order, 2023 (No 44).

its disaster management team gave directives on data management post the pandemic.[97]

The CDP Act provides that data controllers shall ensure that data processed is "retained in a form that allows for the identification of data subjects, for no longer than necessary with a view to the purposes for which the data is collected or further processed."[98] This provision should have been invoked the moment the state of disaster had ended.[99] The pandemic declaration was the necessity for data collection, as now COVID-19 is still present but not as a state of disaster, and compulsory testing has been waived. Data subjects must be granted access to the necessary information to verify and prove that the health-related data processing has stopped. Individual verification requires access to data controllers and their databases, meaning that the data controllers must be identified.[100] Of course, it might be impossible for every data subject to verify this, so an independent oversight mechanism for the certification of the fact that processing has ceased is necessary.[101] These steps would be consistent with the requirement of the transparency of the processing of personal data.[102]

2.4 Transparency

Transparency is an overarching data principle evident throughout the data life cycle.[103] What does transparent data processing mean in respect of COVID-19? This principle is also open to contextual interpretation. That said, data controllers processing health-related data must be transparent in their practices. They must disclose their reasons for processing the personal data. Any institution collecting health-related data must be known and identifiable.[104] For instance, Article 8(1) of *Convention 108+* requires that all

97 Regulation 11H of the South African Regulations Issued in terms of Section 27(2) of the *Disaster Management Act* 57 of 2002 (GN 318 in GG 43107 of 18 March 2020, as amended) (the COVID-19 Regulations).

98 Section 7(1)(*c*) of the CDP Act. Any further processing must be compatible with the initial purposes unless it is for scientific, statistical or historical purposes as provided under s 9(2) of the CDP Act.

99 Regulation 11H(17) of the South African COVID-19 Regulations. The information collected, if intended for other uses, must be de-identified, and all un-de-identified information must be destroyed within six weeks of the lapsing of a declaration of disaster.

100 Zimbabwe has data centres whose locations are not publicly disclosed: Murwira 2021 https://www.herald.co.zw/new-dawn-for-zim-as-president-launches-data-centre-to-anchor-govt-operations.

101 Section 14(b) of the CDP Act.

102 Once certified, health-related data may be archived for scientific, historical or medical research purposes, provided that personal identifiers are safeguarded.

103 Article 5(1)*(a)* of the GDPR; *OECD Guidelines* para 14, Accountability principle: "A data controller should be accountable for complying with measures which give effect to the principles stated above."

104 The data forms handed out in Zimbabwe airports do not specify who the data controller is. The forms are titled "Data Forms".

controllers must inform the data subjects of their identities and habitual residences. The Zimbabwe CDP Act has similar provisions.[105]

The data controller must provide concise information in plain language on what data is being processed.[106] One observes that during the COVID pandemic the use of military language often pertaining to an invisible enemy or war[107] in responding to the pandemic induced a sense of fear in the population and enabled clandestine and excessive data collection. Data processing cannot be lawful and fair if it is not transparent. Equally, this means that any user terms on digital platforms must be clear and simple.[108] For instance, if digital tracing applications are used, they must provide sufficient information on what personal data is being collected, and how. This also requires that the privacy notices associated with these digital tools be in plain language.[109] The data controllers must notify the data subjects when processing health-related data, as it constitutes a greater risk to the rights of the individuals concerned.[110] To exercise transparency, the data controllers must enable the data subjects to access their collected data. This is the convergence of the right to privacy and the right to access to information.[111] The right to information provides oversight of what would ordinarily be opaque data processing. This was critical under COVID-19, as a state of disaster promulgated in response to an emergency is largely an executive instrument with limited independent oversight of how it plays out. To remedy this situation, transparency as a data collection principle should have been exercised throughout the period of the COVID-19 pandemic. It was through the observance of these principles that a human rights approach to the pandemic would have been feasible.

3 Human rights frameworks and the pandemic

There are a number of human rights instruments and positions taken by treaty bodies that are relevant for this consideration. First is the United Nations' *International Covenant on Civil and Political Rights* (ICCPR).[112] The ICCPR provides for a range of rights including the right to life, to respect for inherent dignity and to privacy, among others. The ICCPR provides for the derogation of certain rights, meaning that during emergencies these

105 Sections 15 and 16 of the CDP Act.
106 Article 12(1) of the GDPR.
107 Mhazo and Maponga 2022 *BMJ Global Health* 7.
108 Recital 58 of the GDPR. Also see *Deliberation of the Restricted Committee No SAN-2020-012 of 7 December 2020 Concerning the Companies Google LLC and Google Ireland Limited* (CNIL - French Data Protection Agency).
109 Article 12(7) of the GDPR, as well as Recital 58.
110 Recital 89 of the GDPR abolishes general notification obligations.
111 Section 15 of *Freedom of Information Act* 1 of 2020. Individuals are allowed access to medical health records.
112 *International Covenant on Civil and Political Rights* (1966) (ICCPR).

rights can be limited.[113] Regardless of such limitations,[114] the ICCPR provisions must be respected and promoted. Zimbabwe is a state party to the ICCPR.[115] However, Zimbabwe is a dualist state, which means that treaty law must be domesticated through an Act of Parliament to be enforceable.[116] On the domestication of international laws the *Constitution of Zimbabwe* in section 327(2) provides that

> An international treaty which has been concluded or executed by the President or under the President's authority (a) does not bind Zimbabwe until it has been approved by Parliament; and (b) does not form part of the law of Zimbabwe unless it has been incorporated into the law through an Act of Parliament.

Section 34 of the *Constitution of Zimbabwe* provides that "the State must ensure that all international conventions, treaties and agreements to which Zimbabwe is a party are incorporated into domestic law." In addition, section 46 of the Constitution requires that when interpreting the Declaration of Rights, courts and tribunals "must take into account international law and all treaties and conventions to which Zimbabwe is a party." If there is no domestication, courts must refer to the treaty as ratification even without domestication creates obligations.[117] The ICCPR provisions are sufficiently incorporated into Zimbabwean law for the purposes of the protection of personal data and privacy. Zimbabwe has domesticated the provisions of the ICCPR in its domestic laws, including the Constitution; especially the provisions that protect fundamental rights and freedoms such as the right to privacy.[118]

In addition to specific treaty provisions, the ICCPR Human Rights Committee issues general comments. The general comment on the right to privacy recommends that states store information for known purposes.[119] Dragnet data collection as occurred under COVID-19 prompted the UN special rapporteurs to raise an alarm about scope creep.[120] This form of

---

113 Article 4 of the ICCPR.

114 Articles 6, 7, 8(1) and (2), 11, 15, 16 and 18 of the ICCPR are non-derogable.

115 Ratified on 13 May 1991.

116 Section 326 of the *Constitution of Zimbabwe Act* 1 of 2013 (the Constitution) provides for the application of customary international laws applicable without domestication.

117 Tuovinen 2013 *CCR* 435.

118 There are court decisions that reaffirm the domestication of international law and its application. See, for instance, the case of *Jestina Mukoko v Attorney-General* (SC 11/12 Const Application No 36/09) [2012] ZWSC 11 (19 March 2012), which references the absolute prohibition of torture under international law and the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (1984) (CAT), despite the fact that Zimbabwe is not a state party to CAT. Only Zimbabwe and Tanzania are not CAT members as of 21 February 2023.

119 Human Rights Committee 1988 https://www.refworld.org/legal/general/hrc/1988/en/27539 (General Comment 16).

120 UN 2020 https://www.ohchr.org/Documents/HRBodies/SP/COVID19_and_SP_28_April_2020.pdf.

mass data collection defies a known purpose, is unnecessary and disproportionate. Further, the general comment requires that data subjects must control their files and must have the ability to ascertain the nature of the information stored by public and private authorities, including the ability to rectify or eliminate it.[121] Every private or public institution processing personal data must be regulated by law.[122] For health-related data processing, the general comment requires that this be conducted by trained medical personnel.[123] There is no specific general comment on public health emergencies. This has created a lack of uniformity in state practices during public health emergencies and with regard to COVID-19 measures in particular, prompting the UN to issue COVID-19 and human rights guidance focussing on the implementation of measures that are lawful, necessary, proportionate, time-bound and justified by legitimate public health objectives.[124]

The second relevant instrument is the *African Charter*.[125] Zimbabwe ratified the Charter in 1986.[126] Unlike other international human rights instruments, the Charter has one major limitation; the right to privacy is not enshrined.[127] This is premised on the unique attribute of the Charter of providing for communal and peoples' rights.[128] And privacy is seen as individualistic and un-African. Is it? The Charter does recognise enforceable individual rights in many of its provisions, confirming that the individual is as important as the community.[129] The Charter also contains other rights constituting essential elements of privacy such as the dignity and integrity of the person.[130] Of course, dignity and integrity are not privacy; these are separate and linked rights.[131] Furthermore, the African Commission on Human and People's Rights (the Commission) as the implementing organ of the Charter has observed that human rights treaties benefit from holistic interpretation,[132] if not a living interpretation approach.[133] In fact, there is

121 General Comment 16 para 10.
122 General Comment 16 paras 8, 10.
123 General Comment 16 para 8.
124 UN 2020 https://unsdg.un.org/sites/default/files/2020-04/COVID-19-and-Human-Rights.pdf.
125 *African Charter on Human and Peoples' Rights* (1981) (the Charter).
126 30 May 1986.
127 Makulilo 2016 *Beijing Law Review* 198.
128 Dersso 2006 *AHRLJ* 333.
129 Makulilo 2016 *Beijing Law Review* 199 reiterates that Arts 2 to 17 of the Charter specifically incorporate individual rights as each of these provisions starts with "every individual".
130 Articles 4 and 5 of the Charter.
131 Neethling 2005 *SALJ* 23-24.
132 *Legal Resources Foundation v Zambia* 2001 AHRLR 84.
133 A living instrument interpretation rule incorporates the changing present-day environment and context without resulting in an absurd interpretation advancing a rights dispensation. It was deployed in the European Court of Human Rights case of *Tyrer v United Kingdom* 1978 2 EHRR 1.

nothing stopping the Commission from reading privacy into the Charter, as has been done with other "missing rights."[134] The Charter and the Commission cannot ignore the technological advancements that are threatening human rights, including the right to privacy.[135]

The dignity, integrity and privacy of data subjects have been affected by the reaction to pandemics in Africa. For instance, the HIV and Aids pandemic trigged mandatory testing resulting in the unauthorised disclosure of health-related data, violating privacy rights and increasing stigma.[136] These violations informed the proclamation of the UN global guidelines on HIV and Aids.[137] Mindful of the absence of a specific right to privacy in the Charter, the Commission has passed a resolution relating to personal data protection during the COVID-19 epidemic.[138] This resolution has reinforced the importance of data processing principles such as prior informed consent, privacy, the protection of health-related data, and dignified treatment.[139] These standards are consistent with the World Health Organization (WHO) *International Health Regulations*.

The last and most relevant instrument is the WHO's *International Health Regulations* (IHR).[140] The WHO assembly adopted the IHR in 1969 and revised it again in 2005. The IHR creates a framework for responding to international pandemics, including medical surveillance.[141] The IHR implementation must be informed by and protective of fundamental human rights and freedoms.[142] The IHR protects health-related data processing between the WHO and member states.[143] The Regulations assumes that WHO members will have national laws protecting health-related data. It is indeed the responsibility of nation states to develop national laws to that effect. The IHR incorporates the international data principles on purpose limitation, confidentiality, data accuracy and the rights of data subjects,

134 Singh and Power 2019 *African Human Rights Yearbook* 202.

135 Articles 60 and 61 of the Charter allow the African Commission on Human and People's Rights to use other international law sources.

136 Gumedze 2004 *AHRLJ* 181.

137 OHCHR and UNAIDS *International Guidelines* para 105.

138 *Resolution on Human and Peoples' Rights as Central Pillar of Successful Response to COVID-19 and Recovery from Its Socio-Political Impacts* AU Doc ACHPR/Res 449 (LXVI) (2020).

139 *Resolution on Human and Peoples' Rights as Central Pillar of Successful Response to COVID-19 and Recovery from Its Socio-Political Impacts* AU Doc ACHPR/Res 449 (LXVI) (2020) para 1(h).

140 Articles 21(a) and 22 of the *Constitution of the World Health Organization* (1946) confer authority on the World Health Assembly to adopt regulations for containing the international spread of a disease.

141 Articles 19, 20, 23 of the *International Health Regulations* (2005) (IHR).

142 Article 3 of the IHR.

143 UN institutions have separate data processing principles. The UN, as the maker of norms, has issued guidelines to member states that are unenforceable, let alone persuasive.

among others.[144] In the light of the human rights issues raised under COVID-19, the WHO seventy-fourth assembly made specific recommedations for collaboration with UN human rights bodies to monitor state actions during health emergencies, and the protection of personal data and privacy as provided in the IHR.[145] Zimbabwe is a member of the WHO and has domesticated the IHR into national law, the PHA.[146]

4 Analysing the public health laws

Since the CDP Act entered into force after the pandemic, this section explores the existing laws and the extent of the protection of sensitive health data, especially the PHA, that govern public health responses. The *Constitution of Zimbabwe* as the supreme law[147] enshrines fundamental rights including the right to health care, privacy and dignity.[148] The right to health care during public emergencies must be afforded to every citizen, though the Constitution does not specify what emergency medical treatment is.[149] These provisions are repeated in section 33 of the PHA without specifying the actual elements of emergency medical treatment. During the COVID-19 pandemic it was essential for Zimbabwe to adopt a human rights approach to the provision of emergency medical treatment, grounded in the accessibility of health facilities for vulnerable populations, and supported by access to essential medicines, with all this articulated in a national emergency strategy.[150] The provision of emergency medical services must safeguard privacy to be consistent with the indivisibility of human rights. In the absence of a human rights-focussed interpretation of emergency medical treatment, sensitive health data are at risk of unauthorised processing. This is consistent with the Constitution of Zimbabwe, that provides for the right to privacy of individual's with health conditions.[151] The violation of patients' privacy impairs their dignity, which the Constitution protects under section 51.[152] Even if the Zimbabwe CDP Act came into force

144 Articles 45(1), 45(2) and 45(3) of the IHR.

145 *WHO Report of the Review Committee on the Functioning of the International Health Regulations (2005) during the COVID-19 Response* WHO Doc A74/9 Add.1 (2021).

146 Zimbabwe is a state party to the IHR and the provisions are incorporated in the PHA.

147 Section 2 of the Constitution.

148 Sections 76, 51 and 57 of the Constitution.

149 Section 29 and 76 of the Constitution.

150 *Emergency Care Systems for Universal Health Coverage: Ensuring Timely Care for the Acutely Ill and Injured. Report by the Director-General* WHO Doc A72/31 (2019).

151 The Zimbabwean Constitution mirrors those of South Africa and Kenya, but the specific addition of health conditions is unique to Zimbabwe. The *Constitution of Kenya*, 2010 s 31(c) has an addition: "information relating to their family or private affairs unnecessarily required or revealed".

152 Section 51 of the Constitution on the right to human dignity states that "every person has inherent dignity in their private and public life, and the right to have that dignity respected and protected."

after the declaration of the pandemic, compliance with the provisions of the Constitution was required.

The COVID-19 emergency laws compelled compulsory testing,[153] and authorised the disclosure of people's COVID-19 status.[154] The COVID-19 disaster declaration limited individual rights to decide on medical testing and bodily integrity as protected under section 52(2)(c) of the Constitution. Of course, informed consent before any medical or scientific experiments, extraction or use of bodily tissue is required under international law[155] and under the CDP Act. That said, consent, let alone medical consent, remains a myth, and in medical public emergencies the requirement is waived.[156] During the pandemic the regulations adopted in most countries required medical professionals, while being bound to keep their medical records confidential, to disclose their patients' COVID-19 status to authorities.[157] This disclosure was not unlawful, but concerns about unauthorised disclosure were present due to use of non-medical personnel in the process. The Zimbabwe CDP Act provides that health-related data may be processed only under the responsibility of a health-care professional, unless there is written consent or imminent danger or mitigation of a specific criminal offence.[158] In Zimbabwe the securitised response worsened by the deployment of non-medical personal to assist in the process increased the chances of the mishandling of sensitive personal data.[159] There is no evidence of data subjects giving written consent to have non-medical professionals process their data. Certainly, while there was danger, the question of whether or not it was imminent is debatable. The processing of sensitive health data must be done by a professional who is bound by professional confidentiality.[160]

The Constitution allows for the limiting of rights under various circumstances including public health emergencies, a circumstance which COVID-19

153 Section 6 of Statutory Instrument 77 of 2020: Public Health (COVID-19 Prevention, Containment and Treatment) Regulations, 2020 provides for compulsory testing if one is suspected of having COVID-19.

154 Section 6 of Statutory Instrument 77 of 2020: Public Health (COVID-19 Prevention, Containment and Treatment) Regulations, 2020

155 *UN General Assembly, Special Rapporteur on the Right of Everyone to the Enjoyment of the Highest Attainable Standard of Physical and Mental Health* UN Doc A/HRC/22/53 (2013) paras 28-29.

156 Tschider 2019 *Washington University Law Review* 1505.

157 McQuoid-Mason 2020 *SAMJ* 461.

158 Section 12(4) of the CDP Act.

159 Mhlanga 2020 https://www.newsday.co.zw/2020/11/military-nurses-take-over-hospitals/.

160 Section 12(7) of the CDP Act provides that "For the purposes of processing personal information under this section, the health professional and his or her agents are subject to the duty of professional secrecy." This section is similar to Art 9(3) of the GDPR. The processing of health data for medical purposes under Art 9(2)(h) must be done by a professional who is bound by professional confidentiality.

satisfied.[161] Consistent with international human rights standards, the right to privacy is not absolute. However, its limitation must be justifiable, in pursuit of a legitimate aim acceptable in a democratic society. Moreover, the limitation must be in the public (health) interest.[162] Public welfare is a paramount principle underpinning any constitution, and balances of rights of individuals against those of the state.[163] The state's public health interests limited the individual's right to take personal decisions and to enjoy informational privacy, as these rights became subservient to the public welfare interests.[164]

To limit these rights in the service of greater public welfare, Zimbabwe invoked PHA section 68, declaring COVID-19 a formidable epidemic disease. The limitations were part of the PHSMs, which according to the PHA must be guided by respect for human rights and international public health commitments.[165] This is the categoric domestication of the WHO IHR and other attendant rights. However, the extent to which human rights were respected and enforced during this period is debatable.[166] Furthermore, individual rights can be waived if the individual or patient puts others at risk, or there is a risk or irreparable damage to an individual's life.[167] This was the case with the pandemic in respect of health-related data processing. This, however, does not condone the use of health-related data beyond the purposes of addressing the pandemic. The provisions of the PHA require oversight. The Minister is supposed to report to Parliament annually on progress made on the implementation of the rights in relation to public health set out in the Constitution.[168] This provision is consistent with Zimbabwe's obligations under domestic and international law, but the provision has not been utilised. The provision notwithstanding, Zimbabwe passed several regulations in response to COVID-19. Unfortunately, these regulations were silent on the topic of the protection of health-related data despite the proliferation of public and private institutions collecting sensitive personal information.

Due to the PHA provisions, excessive health-related data processing is inevitable through community medical surveillance. The PHA requires every

161 Section 86 of the Constitution.
162 Section 86(2)(b) of the Constitution.
163 Makwaiba 2021 *AHRLJ* 311.
164 Makwaiba 2021 *AHRLJ* 315, 318, 319.
165 Sections 31(1)(a) and 31(1)(j) of the PHA.
166 Zimbabwe Human Rights NGO Forum *180 Days of What?* 10.
167 Section 35 of the PHA; also see s 7(1)*(d)* of the South African *National Health Act* 61 of 2003. It details the circumstances in which treatment may be administered without the consent of the patient, including a case where failure to treat the patient (or group of patients) would lead to a serious public health or safety risk. This was litigated in *Minister of Health v Goliath* 2009 2 SA 248 (C).
168 Section 30 of the PHA.

individual who suspects or comes into contact with a suspected patient or case of a formidable disease to notify the district medical officer.[169] Worse is the fact that COVID-19 symptoms were presenting as common colds, and communities could easily be divided on whether or not to report a person as being ill, as a failure to notify constituted a criminal offence. It is important for the PHA provisions on medical surveillance to be consistent with the provisions of the CDP Act, which though not presented as a superior law, must be prioritised on issues of sensitive data protection.[170]

While the PHA anchors the surveillance by the medical community, the infamous *Interception of Communications Act* regulates surveillance generally in Zimbabwe.[171] The *Interception of Communications Act* mandates telecommunication service providers to create capabilities within their infrastructure that allow for the real-time interception or monitoring of communications by installing telecommunication traffic monitoring systems.[172] The monitoring system collects metadata, those being the subscriber data, the service data and the traffic data.[173] Metadata have greater chances of disclosing users' personal identity and therefore violating individual privacy. In addition, during COVID the PHSMs required temperature readings and the recording of mobile phone numbers for contact tracing. This information could be cross-referenced with the subscriber databases held by mobile network operators or POTRAZ. The central subscriber information database easily discloses health-related data.[174] This information could easily be used for other purposes.[175] These surveillance laws and regulations have weak oversight, undermining the transparency and accountability in personal data processing.[176] No public

169 Section 65 of the PHA.

170 Section 4(1) of the CDP Act fails to insist on the superiority of this Act and that any other laws, such as the PHA, must subsist below it unless the PHA provides better protection, which it does not.

171 *Interception of Communications Act* 6 of 2007 (Chapter 11:20).

172 Statutory Instrument 95 of 2021: Postal and Telecommunications (Telecommunications Traffic Monitoring System) Regulations, 2021.

173 Metadata refers to all the information associated with a communication, apart from the actual substance of the communication.

174 Section 8 of Statutory Instrument 95 of 2021: Postal and Telecommunications (Telecommunications Traffic Monitoring System) Regulations, 2021. The Postal and Telecommunications Regulatory Authority (POTRAZ), established under the *Postal and Telecommunications Act*, 2000 (Chapter 12:05), mandated compulsory registration of subscriber identity modules (SIMs) and the establishment of a database.

175 Mhlanga 2018 https://www.newsday.co.zw/2018/07/zanu-pf-breaks-into-zec-database/.

176 The Minister issues warrants of interception in terms of s 6 and the warrants are reviewed by the Attorney General annually in terms of s 19 of the *Interception of Communications Act* 6 of 2007 (Chapter 11:20).

privacy impact assessments of these databases were conducted,[177] and in fact they constitute privacy violations as "the systematic collection, processing and retention of a searchable database of personal information, even of a relatively routine kind, involves a significant interference with the right to respect for private life."[178]

5 Digital surveillance and the pandemic

Admittedly, the medical surveillance infrastructure is premised on the WHO global health architecture.[179] At the barest minimum, surveillance during pandemics entails the systematic and ongoing collection, collation, and analysis of data to inform the public health responses.[180] Technology-enabled surveillance assumed a largely positive societal value, bringing efficiency and effectiveness to the response to the pandemic.[181] Several countries adopted mobile platforms to indicate the proximate contacts of COVID-19 patients.[182] The use of contact tracing applications, despite the concerns about data privacy, contributed somewhat to controlling the transmission of COVID-19.[183] The COVID-19 contact tracing applications have a wide range of health-related data-driven capabilities: information sharing, self-testing, sharing the experiences of patients, monitoring symptoms, quarantine, and contact tracing.[184]

To augment the manual training systems, Zimbabwe designed and implemented a digital contact tracing application.[185] The ZimCOVID safe application includes a COVID-19 screening tool, general information on vaccination and testing centres, and the short message service (SMS)-based solution. The application's privacy policy indicates that the ZimCOVID application is "to provide updates with regards to Country's Situation on Covid-19 and Contact them in case of a suspected case of COVID-19 to help reduce the spread of Covid-19."[186] Further, the privacy

177 Sections 2 and 10(2) of Statutory Instrument 95 of 2014: Postal and Telecommunications (Subscriber) Regulations, 2014 provide for a private impact form and define it as a form which evaluates the entire project from a privacy perspective and identifies risks and mitigation strategies throughout. The form is not publicly provided in the Statutory Instrument.

178 *Catt v ACPO* 2012 EWHC 1471 44.

179 French 2009 *Surveillance & Society* 101.

180 Article 1 of the IHR.

181 Independent Panel 2021 https://theindependentpanel.org/wp-content/uploads/2021/05/COVID-19-Make-it-the-Last-Pandemic_final.pdf.

182 Klaaren *et al* 2020 *SAMJ* 617.

183 Baraniuk 2020 *BMJ* 1-3.

184 Borra "COVID-19 Apps" 11-17.

185 Moyo-Ndlovu 2021 https://www.herald.co.zw/health-ministry-launches-covid-19-app/. Most of the application's functions are not fully described on either the Google or Apple store, which raises the question of how much of their functionality meets the required data protection standards.

186 Dencroft date unknown https://dencroft.com/zimcovid-safe-app-policy.

policy states that "all data collected or shared (with you) is completely managed and stored by ministry of health."

First, there are limitations to the privacy policy. It does not indicate the type of data collected by the Health Ministry. In addition, the PHA and the various COVID statutory instruments are silent on how the collected sensitive personal health data will be used, stored and or destroyed by the data controller, the health ministry. The application requests minimal personal information on registration, such as a mobile number.[187] This is commendable but futile in that databases in the custody of public authorities like POTRAZ are easily accessible to state-linked actors, who may violate individual privacy.[188] POTRAZ is again the data protection authority. Further, mobile network operators (MNOs) are capable of using subscriber databases to disseminate health public information, as seen during COVID-19, much to the chagrin of subscribers.[189] Secondly, upon further testing of the application on an android platform it emerged that it accesses personal data stored on devices. The application is capable of modifying, deleting and reading the stored data on such devices. The application is capable of preventing a mobile device from sleeping (temporary sleep), it can view network connections, and it has full network access.[190] Arguably, these capabilities constitute a criminal offence in that the application is accessing unauthorised data which are not needed for its purposes and irrelevant to its proper functioning. This is unlawful interference with data and data storage media in terms of section 163B(1) of the *Criminal Law (Codification and Reform) Act*.

Thirdly, the application's privacy policy removes data processor liability for data security and the integrity of the information. The data processor, Dencroft, is immunised, no pun intended. The privacy policy fails to indicate how the data controller, being the Health Ministry, is using technical and organisational measures to secure data confidentiality as required under section 39 of the PHA and in terms of section 18 of the CDP Act. While the use of digital tracing contacts and techno-based solutions was touted as a

187 The reference to the collection of personal data "including but not limited to phone number" is purportedly for the better application user experience, and that information is retained by the Health Ministry. Dencroft date unknown https://dencroft.com/zimcovid-safe-app-policy.

188 Mhlanga 2018 https://www.newsday.co.zw/2018/07/zanu-pf-breaks-into-zec-database/.

189 An urgent application was brought by Sikhumbuzo Mpofu against Econet Wireless network for unsolicited public notices on COVID-19, which Mr Mpofu alleged were violating his rights, including his right to privacy.

190 *ZimCovidSafe Mobile Application Security Assessment Report* (10 September 2021) (on file with the author). The assessment was conducted by a certified digital security expert.

solution to the pandemic,[191] Zimbabwe's contact tracing application did not seem to serve any purpose other than risking users' health-related data privacy. Even as Zimbabwe deployed the contact tracing application, no privacy impact assessments were conducted. The application's privacy policy was shallow, fuelling existing digital mistrust and the fear of surveillance, and heightening the risk of the abuse of health-related data. South Africa provides a compelling comparative experience of how pandemic- and health-related data were processed as against received data principles.

6 Comparative pandemic responses

South Africa's Constitution and jurisprudence has contributed to the development of Zimbabwe's legal system. Despite their shared legal histories, South Africa has progressed in terms of health-related data protection. South Africa spent more than a decade in developing the *Protection of Personal Information Act* 4 of 2013.[192] Zimbabwe, on the other hand, after several iterations of data protection law, finally passed the CDP Act in 2021. To achieve this feat, Zimbabwe participated in several regional efforts at harmonising cybercrime and data protection laws, informed by regional model laws.[193] That said, immediately after the gazetting of the CDP Act in 2021, several steps could have been taken to enable compliance with the data protection law. First, POTRAZ should have issued guidelines for all data controllers and personnel processing health data on what was expected of them. Secondly, the Minister of Health, who was the data controller for the COVID-19 application, should have issued clear directives on how data processors such as medical facilities, immigration officials or ports of entry, or even public spaces that were recording visitors or users temperatures and personal phone numbers were required to store or destroy this information. For instance, South Africa's data protection authority, the Information Regulator (IR), issued guidelines articulating such data processing parameters.[194] No similar efforts were attempted or recorded in Zimbabwe.

---

191 One example of success in using technological solutions is Taiwan, with a high digital connectivity rate and the use of mobile devices that allow cellular location tracking as an effective means to enforce quarantine. See Eigen, Wang and Gasser 2020 https://cyber.harvard.edu/story/2020-07/country-spotlight-taiwans-digital-quarantine-system.

192 The South African Law Reform Commission considered the inclusion of a discussion on privacy and data protection on 17 November 2000. SALRC *Discussion Paper 109* 1.

193 The *SADC Model Law on Data Protection* (2013) was the product of support under HIPSSA to review its laws and follow a model law on data protection.

194 IR 2020 https://documentportal.george.gov.za/storage/level-five-covid-documents/August2020/qeyctYy1dBMmLgVwI1c5.pdf.

Although laws regulating the COVID-19 public health emergency are temporary, data protection mechanisms for health-related data need not be temporary. At the very least, a sector-specific data protection authority or a national data protection authority must be put in place.[195] South Africa's *Protection of Personal Information Act* establishes the Information Regulator (IR),[196] while Zimbabwe's CDP Act designates an existing regulating entity, POTRAZ,[197] as the data protection authority and cybersecurity centre.[198] The IR oversight, its appointment and its removal is subjected to parliamentary processes.[199] In contrast, in Zimbabwe POTRAZ is largely an executive establishment enjoying wide and unfettered powers, and discretion.[200] The data protection authorities should carry out oversight on data controllers and processors. This is impossible for POTRAZ as it is an interested party.[201] Zimbabwe's approach of designating an existing and not independent data institution as a data protection authority is unlikely to instill confidence that health-related data processing is satisfying data processing principles consistent with international principles. Executive or government control or government membership of a data protection authority is incompatible with data processing principles and practices.[202] Even without an enforceable data protection law at the time of the declaration of the pandemic, Zimbabwe's Health Ministry as the sector-specific data controller should have issued health-related data processing guidelines consistent with PHA and IHR public health standards and measures. The existing laws and associated regulatory bodies might not provide adequate protection, but certainly are sufficient as building blocks for the enforcement of the right to privacy in general and the confidentiality of health conditions as a constitutional right.

---

195 In the absence of a national data protection law, a sectoral law will suffice; for instance, the Health Ministry becomes the data controller and manager for all COVID-19-related data as the PHA provides for data protection.

196 Section 39 of the *Protection of Personal Information Act* 4 of 2013: establishment of the Information Regulator (IR); s 41: appointment of the IR under the *Protection of Personal Information Act* 4 of 2013.

197 POTRAZ is established under s 3 of the *Postal and Telecommunications Act*, 2000 (Chapter 12:05).

198 *Cybersecurity and Data Protection Bill* (undated layman draft) ss 5-6 on the Cybersecurity Centre; ss 7-8 on designation as Data Protection Authority.

199 Sections 40(1)(*b*)(iv), 41(2) and 41(6) of the *Protection of Personal Information Act* 4 of 2013.

200 Section 25 of the *Postal and Telecommunications Act*, 2000 (Chapter 12:05): the Minister may give policy directions; s 26: the Minister may direct the Board to reverse, suspend or rescind its decisions or actions.

201 For instance, the revenue for POTRAZ operations comes from MNOs' fees; and it is common knowledge that MNOs is one of the largest data controllers.

202 See Arts 11(1)(*b*) and 11(1)(6) of the *Malabo Convention*. Zimbabwe has not ratified the *Malabo Convention*.

Of equal importance is the oversight of surveillance. Zimbabwe and South Africa's histories are replete with cases of unlawful surveillance.[203] Zimbabwe's surveillance architecture remains inspired by the colonial order, with no oversight and accountability.[204] Notably, though, in 2004 the Supreme Court struck down as unconstitutional sections of the *Postal and Telecommunications Act* which conferred "unfettered powers to intercept correspondence and communications" without "legal recourse or safeguard" and no "mechanisms for accountability."[205] Despite this ruling, the interception of communications law was passed in 2007, reviving a legacy of unfettered surveillance powers. Even at parliamentary level, no surveillance or intelligence committee exists.[206] In addition to the existing mechanisms, during the pandemic South Africa introduced and designated a judge who received weekly updates on the collection and usage of personal data and issued directives for the protection of privacy.[207]

7 Conclusion

As unprecedented as it has been, the pandemic has surfaced existing and newer issues on the processing of sensitive health-related data. Globally, government responses were similar with variations in the intensity of the emergency measures adopted and the deployment of digital contact tracing. These measures limited citizens' fundamental rights, including the right to privacy. Granted, the right to privacy is not absolute and public health emergencies constitute a legitimate and justifiable limitation. However, any form of limitation of the right to privacy through the collection of personal data requires consent, disclosure of the purpose of the data collection, secure storage and destruction, the transparent conduct of the data controllers, and oversight of any surveillance measures. Admittedly Zimbabwe had no effective data protection law until December 2021. Notwithstanding this regulatory weakness the supreme law, the Constitution, remained valid and in force, and provisions of the PHA and the dozens of COVID designed instruments should have been interpreted to protect sensitive health data. Any pandemic disaster declaration should have been constitutionally compliant, safeguarding the fundamental right to privacy. It cannot be gainsaid that the pursuit of the right to health must be

203 Kwet "Surveillance in South Africa" 98.

204 MISA Zimbabwe 2019 https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/MISA_ZIMBABWE.pdf.

205 *Law Society of Zimbabwe v Minister of Transport and Communications* (unreported) case number SC 59/03 of 2 March 2004. The court stated that "similar legislation in other jurisdictions provides or is required to provide, for prior scrutiny, independent supervision of the exercise of such powers and effective remedies for possible abuse of the powers. The Act provides for no such safeguards."

206 Zimbabwe's Parliament Committee System does not include an intelligence and oversight committee, as in South Africa.

207 Regulation 11H(14) of the South African COVID-19 Regulations.

viewed as consistent with the right to privacy and the protection of sensitive personal data. The urgent need to respond to any pandemic must not create a data pandemic were health-related data is abused, as the consequences will always outlast the pandemic.

Bibliography

Literature

Alunge "Consolidating the Right to Data Protection"
Alunge R "Consolidating the Right to Data Protection in the Information Age: A Comparative Appraisal of the Adoption of the OECD (Revised) Guidelines into the EU GDPR, the Ghanaian Data Protection Act 2012 and the Kenyan Data Protection Act 2019" in Thorn J, Gueye A and Hejnowicz A (eds) *Innovations and Interdisciplinary Solutions for Underserved Areas* (Springer Cham 2020) 192-207

Baraniuk 2020 *BMJ*
Baraniuk C *Covid-19 Contact Tracing: A Briefing* 2020 *BMJ* 1-3

Borra "COVID-19 Apps"
Borra S "COVID-19 Apps: Privacy and Security Concerns" in Joshi A, Dey N and Santosh K (eds) *Intelligent Systems and Methods to Combat Covid-19* (Springer Singapore 2020) 11-17

Blume 2004 *Scand Stud L*
Blume EP "Data Protection in the Private Sector" 2004 *Scand Stud L* 297-318

Bradford 2012 *North Western University Law Review*
Bradford A "The Brussels Effect" 2012 *North Western University Law Review* 1-69

Braman 2011 *New Media & Society*
Braman S "Privacy by Design: Networked Computing, 1969-1979" 2011 *New Media & Society* 798-814

Chen 2016 *IDPL*
Chen J "How the Best-Laid Plans Go Awry: The (Unsolved) Issues of Applicable Law in the General Data Protection Regulation" 2016 *IDPL* 310-323

Chipendo *et al* 2022 *Pan African Medical Journal*
Chipendo T *et al* "Implementation of the COVID-19 Laboratory Testing Certification Program (CoLTeP), Zimbabwe, 2021" 2022 *Pan African Medical Journal* 1-8

Dersso 2006 *AHRLJ*
Dersso AS "The Jurisprudence of the African Commission in Human and People's Rights with Respect to People's Rights" 2006 *AHRLJ* 333-357

Dove and Chen 2020 *IDPL*
Dove SE and Chen J "Should Consent for Data Processing be Privileged in Health Research? A Comparative Legal Analysis" 2020 *IDPL* 117-131

Esayas 2017 *IJLIT*
Esayas YS "The Idea of 'Emergent Properties' in Data Privacy: Towards a Holistic Approach" 2017 *IJLIT* 139-178

French 2009 *Surveillance & Society*
French MA "Woven of War-Time Fabrics: The Globalization of Public Health Surveillance" 2009 *Surveillance & Society* 101-115

Furusa and Coleman 2018 *South African Journal of Information Management*
Furusa SS and Coleman A "Factors Influencing E-Health Implementation by Medical Doctors in Public Hospitals in Zimbabwe" 2018 *South African Journal of Information Management* 1-9

Ghersi, Mariño and Miralles 2018 *BMC Medical Informatics and Decision Making*
Ghersi I, Mariño M and Miralles MT "Smart Medical Beds in Patient-Care Environments of the Twenty-First Century: A State-of-Art Survey" 2018 *BMC Medical Informatics and Decision Making* 1-12

Greenleaf 2012 *IDPL*
Greenleaf G "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108" 2012 *IDPL* 68-92

Gumedze 2004 *AHRLJ*
Gumedze S "HIV/AIDS and Human Rights: The Role of the African Commission on Human and Peoples' Rights" 2004 *AHRLJ* 181-200

Hurd 1996 *Legal Theory*
Hurd H "The Moral Magic of Consent" 1996 *Legal Theory* 121-146

Khumalo 2017 *Library Philosophy and Practice*
Khumalo NB "The Need for the Establishment of E-records and eHealth Legislation and Policy Framework in the Health Sector in Zimbabwe" 2017 *Library Philosophy and Practice* 1-18

Kirby 2011 *IDPL*
Kirby M "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy" 2011 *IDPL* 6-14

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* 617-620

Koops 2021 *Law, Innovation and Technology*
Koops BJ "The Concept of Function Creep" 2021 *Law, Innovation and Technology* 29-56

Kwet "Surveillance in South Africa"
Kwet M "Surveillance in South Africa: From Skin Branding to Digital Colonialism" in Vagle J and Kwet M (eds) *Cambridge Handbook of Race and Surveillance* (Cambridge University Press Cambridge 2023) 97-122

Lloyd *Information Technology Law*
Lloyd IJ *Information Technology Law* 7th ed (Oxford University Press Oxford 2014)

Makulilo 2016 *Beijing Law Review*
Makulilo AB "A Person is a Person through Other Persons: A Critical Analysis of Privacy and Culture in Africa" 2016 *Beijing Law Review* 192-204

Makwaiba 2021 *AHRLJ*
Makwaiba BS "Tension between the Individual's Fundamental Human Rights and the Protection of the Public from Infectious and Formidable Epidemic Diseases" 2021 *AHRLJ* 311-334

McQuoid-Mason 2020 *SAMJ*
McQuoid-Mason DJ "COVID-19 and Patient-Doctor Confidentiality" 2020 *SAMJ* 461-462

Mhazo and Maponga 2022 *BMJ Global Health*
Mhazo AT and Maponga CC "Governing a Pandemic: Biopower and the COVID-19 Response in Zimbabwe" 2022 *BMJ Global Health* 1-13

Mokrosinska 2020 *Critical Review of International Social and Political Philosophy*
Mokrosinska D "Why States have no Right to Privacy but May be Entitled to Secrecy: A Non-Consequentialist Defense of State Secrecy" 2020 *Critical Review of International Social and Political Philosophy* 415-444

Neethling 2005 *SALJ*
Neethling J "The Concept of Privacy in South African Law" 2005 *SALJ* 18-28

OHCHR and UNAIDS *International Guidelines*
Office of the United Nations High Commissioner for Human Rights and UNAIDS *International Guidelines on HIV/AIDS and Human Rights. 2006 Consolidated Version* (UN Geneva 2006)

Rocher, Hendrickx and De Montjoye 2019 *Nature Communications*
Rocher L, Hendrickx JM and De Montjoye YA "Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models" 2019 *Nature Communications* 1-9

SALRC *Discussion Paper 109*
South African Law Reform Commission *Discussion Paper 109, Project 124: Privacy and Data Protection* (The Commission Pretoria 2005)

Schermer, Custers and Van der Hof 2014 *Ethics Information and Technology*
Schermer BW, Custers B and Van der Hof S "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" 2014 *Ethics Information and Technology* 171-182

Singh and Power 2019 *African Human Rights Yearbook*
Singh A and Power M "The Privacy Awakening: The Urgent Need to Harmonise the Right to Privacy in Africa" 2019 *African Human Rights Yearbook* 202-220

Solove 2002 *CLR*
Solove DJ "Conceptualising Privacy" 2002 *CLR* 1087-1156

Tschider 2019 *Washington University Law Review*
Tschider C "The Consent Myth: Improving Choice for Patients of the Future" 2019 *Washington University Law Review* 1505-1528

Tuovinen 2013 *CCR*
Tuovinen J "What to Do with International Law? Three Flaws in Glenister" 2013 *CCR* 435-449

Waltraut 2014 *IDPL*
Waltraut K "The Proposal for a New General Data Protection Regulation: Problems Solved?" 2014 *IDPL* 274-281

Zimbabwe Human Rights NGO Forum *180 Days of What?*
Zimbabwe Human Rights NGO Forum *180 Days of What? A Summary Review of the First 180 Days of the COVID-19 National Lockdown in Zimbabwe* (Zimbabwe Human Rights NGO Forum Harare 2020)

Zwitter and Gstrein 2020 *Journal of International Humanitarian Action*
Zwitter A and Gstrein OJ "Big Data, Privacy and COVID-19: Learning from Humanitarian Expertise in Data Protection" 2020 *Journal of International Humanitarian Action* 1-7

Report

ZimCovidSafe Mobile Application Security Assessment Report (10 September 2021) (on file with the author)

Case law

Amann v Switzerland ECHR App No 27798/95 (16 February 2000)

Catt v ACPO 2012 EWHC 1471

Deliberation of the Restricted Committee No SAN-2020-012 of 7 December 2020 Concerning the Companies Google LLC and Google Ireland Limited (CNIL - French Data Protection Agency)

Jestina Mukoko v Attorney-General (SC 11/12 Const Application No 36/09) [2012] ZWSC 11 (19 March 2012)

Law Society of Zimbabwe v Minister of Transport and Communications (unreported) case number SC 59/03 of 2 March 2004

Legal Resources Foundation v Zambia 2001 AHRLR 84

Minister of Health v Goliath 2009 2 SA 248 (C)

S and Marper v United Kingdom 2008 ECHR 1581

Tyrer v United Kingdom 1978 2 EHRR 1

Z v Finland 1997 ECHR 10

Legislation

Kenya

Constitution of Kenya, 2010

South Africa

Constitution of the Republic of South Africa, 1996

National Health Act 61 of 2003

Protection of Personal Information Act 4 of 2013

United States of America

Freedom of Information Act, 1966

Zimbabwe

Constitution of Zimbabwe Act 1 of 2013

Civil Protection Act, 1989 (Chapter 10:06)

Criminal Law (Codification and Reform) Act, 2019 (Chapter 9:23)

Cyber and Data Protection Act, 2021 (Chapter 12:07)

Freedom of Information Act 1 of 2020

Interception of Communications Act 6 of 2007 (Chapter 11:20)

Postal and Telecommunications Act, 2000 (Chapter 12:05)

Public Health Act 11 of 2018

Government publications

South Africa

GN 318 in GG 43107 of 18 March 2020, as amended (Regulations Issued in terms of Section 27(2) of the *Disaster Management Act* 57 of 2002)

Zimbabwe

Cybersecurity and Data Protection Bill (undated layman draft)

GN 492/2022 of 11 March 2022

Statutory Instrument 95 of 2014: Postal and Telecommunications (Subscriber) Regulations, 2014

Statutory Instrument 76 of 2020: Civil Protection (Declaration of State of Disaster: Rural and Urban Areas of Zimbabwe) (COVID-19) Notice, 2020

Statutory Instrument 77 of 2020: Public Health (COVID-19 Prevention, Containment and Treatment) Regulations, 2020

Statutory Instrument 95 of 2021: Postal and Telecommunications (Telecommunications Traffic Monitoring System) Regulations, 2021

Statutory Instrument 102 of 2023: Public Health (COVID-19 Prevention, Containment and Treatment) (National Lockdown) (No 22) (Amendment) Order, 2023 (No 44)

International instruments

African Charter on Human and Peoples' Rights (1981)

African Charter on the Rights and Welfare of the Child (1990)

African Union Convention on Cyber Security and Personal Data Protection (2014)

Constitution of the World Health Organization (1946)

Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (1984)

Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data (1981) (*Convention 108*)

Council of Europe Committee of Ministers Recommendation 509 (1968)

Council of Europe Committee of Ministers Resolution (73) 22 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector (1973)

Council of Europe Committee of Ministers Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector (1974)

Declaration of Principles on Freedom of Expression and Access to Information (2019)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data OJ L 281/31 (1995)

Emergency Care Systems for Universal Health Coverage: Ensuring Timely Care for the Acutely Ill and Injured. Report by the Director-General WHO Doc A72/31 (2019)

General Data Protection Regulation (2016)

International Covenant on Civil and Political Rights (1966)

International Health Regulations (2005)

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), as revised in 2013

Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (2018) (*Convention 108+*)

Report of the Special Rapporteur on the Right to Privacy, Joseph A Cannataci UN Doc A/76/220 (2021)

Resolution on Human and Peoples' Rights as Central Pillar of Successful Response to COVID-19 and Recovery from Its Socio-Political Impacts AU Doc ACHPR/Res 449 (LXVI) (2020)

SADC Model Law on Data Protection (2013)

UN General Assembly, Special Rapporteur on the Right of Everyone to the Enjoyment of the Highest Attainable Standard of Physical and Mental Health UN Doc A/HRC/22/53 (2013)

Vienna Convention on the Law of Treaties (1969)

WHO Report of the Review Committee on the Functioning of the International Health Regulations (2005) during the COVID-19 Response WHO Doc A74/9 Add.1 (2021)

Internet sources

Dencroft date unknown https://dencroft.com/zimcovid-safe-app-policy
Dencroft date unknown *ZimCOVID Safe App Policy* https://dencroft.com/zimcovid-safe-app-policy accessed 8 September 2021

Eigen, Wang and Gasser 2020 https://cyber.harvard.edu/story/2020-07/country-spotlight-taiwans-digital-quarantine-system
Eigen M, Wang F and Gasser U 2020 *Country Spotlight: Taiwan's Digital Quarantine System* https://cyber.harvard.edu/story/2020-07/country-spotlight-taiwans-digital-quarantine-system accessed 23 March 2024

European Data Protection Board 2020 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
European Data Protection Board 2020 *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020*
https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf accessed 22 March 2024

EU Data Protection Working Party 2007 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
European Union Data Protection Working Party 2007 *Opinion 4/2007 on the Concept of Personal Data* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf accessed 22 March 2024

EU Data Protection Working Party 2005 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf
European Union Data Protection Working Party 2005 *Document No WP 105: Working Document on Data Protection Issues Related to RFID Technology* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf accessed 22 March 2024

Greenleaf 2021 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348
Greenleaf G 2021 *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348 accessed 22 March 2024

Hoofnagle 2014 https://ssrn.com/abstract=2466418
Hoofnagle CJ 2014 *The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems* https://ssrn.com/abstract=2466418 accessed 2 September 2021

Human Rights Committee 1988 https://www.refworld.org/legal/general/hrc/1988/en/27539
Human Rights Committee 1988 *General Comment No 16: Article 17 (Right to Privacy). The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* https://www.refworld.org/legal/general/hrc/1988/en/27539 accessed 23 March 2024

Independent Panel 2021 https://theindependentpanel.org/wp-content/uploads/2021/05/COVID-19-Make-it-the-Last-Pandemic_final.pdf
Independent Panel for Pandemic Preparedness and Response 2021 *COVID-19: Make It the Last Pandemic* https://theindependentpanel.org/wp-content/uploads/2021/05/COVID-19-Make-it-the-Last-Pandemic_final.pdf accessed 16 September 2021

IR 2020 https://documentportal.george.gov.za/storage/level-five-covid-documents/August2020/qeyctYy1dBMmLgVwI1c5.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://documentportal.george.gov.za/storage/level-five-covid-documents/August2020/qeyctYy1dBMmLgVwI1c5.pdf accessed 6 April 2024

Mhlanga 2018 https://www.newsday.co.zw/2018/07/zanu-pf-breaks-into-zec-database/
Mhlanga B 2018 *ZANU PF Breaks into ZEC Database* https://www.newsday.co.zw/2018/07/zanu-pf-breaks-into-zec-database/ accessed 14 September 2021

Mhlanga 2020 https://www.newsday.co.zw/2020/11/military-nurses-take-over-hospitals/
Mhlanga B 2020 *Military Nurses Take over Hospitals* https://www.newsday.co.zw/2020/11/military-nurses-take-over-hospitals/ accessed 14 September 2021

MISA Zimbabwe 2019 https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/MISA_ZIMBABWE.pdf
Media Institute of Southern Africa Zimbabwe 2019 *Submissions to United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/MISA_ZIMBABWE.pdf accessed 8 April 2024

Moyo-Ndlovu 2021 https://www.herald.co.zw/health-ministry-launches-covid-19-app/
Moyo-Ndlovu T 2021 *Health Ministry Launches Covid-19 App* https://www.herald.co.zw/health-ministry-launches-covid-19-app/ accessed 14 September 2021

Mungadze 2020 https://www.itweb.co.za/content/rW1xLv59YPGvRk6m
Mungadze S 2020 *Life Healthcare Reveals Damage Caused by Data Breach* https://www.itweb.co.za/content/rW1xLv59YPGvRk6m accessed 2 November 2021

Murwira 2021 https://www.herald.co.zw/new-dawn-for-zim-as-president-launches-data-centre-to-anchor-govt-operations
Murwira Z 2021 *New Dawn for Zim … as President Launches Data Centre to Anchor Govt Operations* https://www.herald.co.zw/new-dawn-for-zim-as-president-launches-data-centre-to-anchor-govt-operations accessed 14 September 2021

PSMI 2020 https://www.psmi.co.zw/2020/06/08/192323/
PSMI 2020 *PSMI Launches a Telemedicine Platform* https://www.psmi.co.zw/2020/06/08/192323/ accessed 14 September 2021

Tsiko 2019 https://www.herald.co.zw/telemedicine-revolutionises-zim-healthcare
Tsiko S 2019 *Telemedicine Revolutionises Zim Health Care* https://www.herald.co.zw/telemedicine-revolutionises-zim-healthcare/ accessed 14 September 2021

UN 2020 https://www.ohchr.org/Documents/HRBodies/SP/COVID19_and_SP_28_April_2020.pdf
United Nations 2020 *United Nations Special Procedures and Covid-19 Working Document Covering Information as of 28 April 2020* https://www.ohchr.org/Documents/HRBodies/SP/COVID19_and_SP_28_April_2020.pdf accessed 9 September 2021

UN 2020 https://unsdg.un.org/sites/default/files/2020-04/COVID-19-and-Human-Rights.pdf
United Nations 2020 *COVID-19 and Human Rights: We are All in this Together* https://unsdg.un.org/sites/default/files/2020-04/COVID-19-and-Human-Rights.pdf accessed 9 September 2021

USA Department of Health 1973 https://aspe.hhs.gov/reports/records-computers-rights-citizens
United States of America Department of Health, Education and Welfare Records 1973 *Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*

https://aspe.hhs.gov/reports/records-computers-rights-citizens accessed 1 November 2021

List of Abbreviations

AHRLJ	African Human Rights Law Journal
BMJ	British Medical Journal
CCR	Constitutional Court Review
CDP Act	Cyber and Data Protection Act, 2021 (Chapter 12:07)
CLR	California Law Review
CoE	Council of Europe
EU	European Union
GDPR	General Data Protection Regulation
HIPSSA	Harmonisation of ICT Policies in Sub-Saharan Africa
ICCPR	International Covenant on Civil and Political Rights
IDPL	International Data Privacy Law
IHR	International Health Regulations (2005)
IJLIT	International Journal of Law and Information Technology
IR	Information Regulator
MISA	Media Institute of Southern Africa
MNO	mobile network operator
OECD	Organisation for Economic Co-operation and Development
OHCHR	Office of the United Nations High Commissioner for Human Rights
PHA	Public Health Act 11 of 2018
PHSMs	public health standards and measures
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
SADC	Southern African Development Community
SALJ	South African Law Journal
SALRC	South African Law Reform Commission
SAMJ	South African Medical Journal
Scand Stud L	Scandinavian Studies in Law
UN	United Nations
USA	United States of America
WHO	World Health Organization