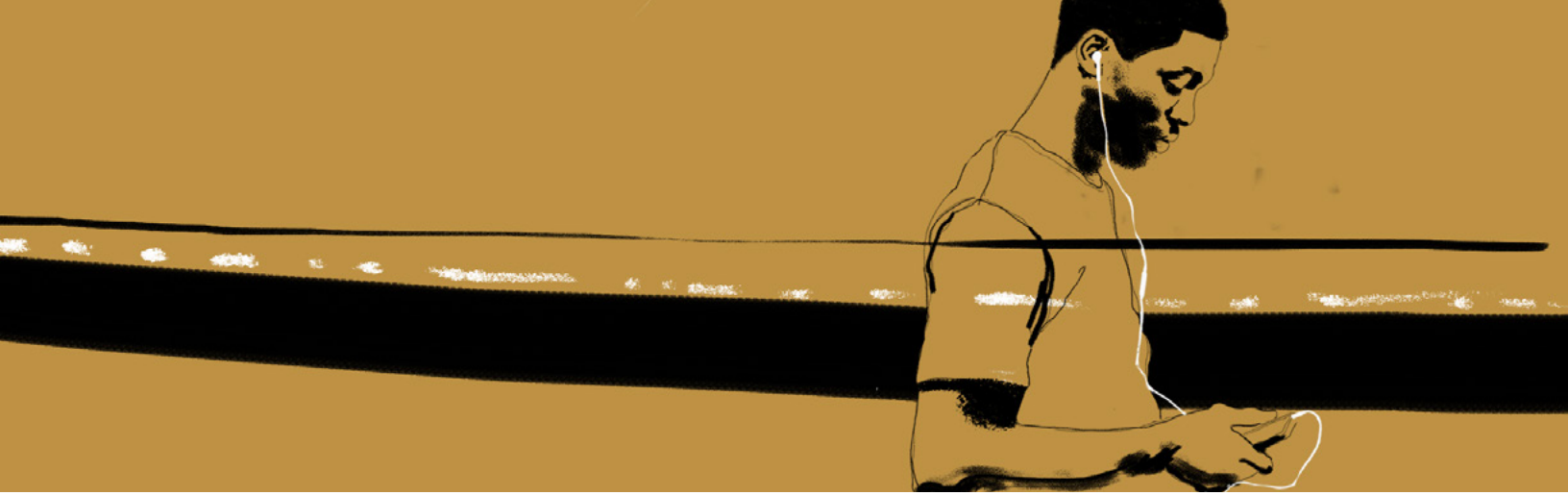

Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solutions

AUTHOR: Tomiwa Ilori

1. INTRODUCTION

Data protection in Africa can still be described to be in its nascent stage. Most African states do not have a data protection law. Countries on the continent are divided along the lines of countries with a data protection law, countries with fragmented frameworks, and countries without any semblance of a law. Out of the 55 states on the continent, only 28 countries have a data protection law, of which 15 have set up data protection authorities (DPAs) to enforce the law.[1]

The focus of this paper is two-fold. The first objective is to consider the status of data protection in Africa, while the second objective focuses on the impact of public emergencies like the COVID-19 pandemic on data protection in Africa. This is done by considering both international and national contexts on data protection in Africa. The countries being focused on are: Nigeria, Senegal, Uganda, Kenya, Morocco, Tunisia, South Africa and Mauritius. The choice of national contexts is premised on language and differences in legal systems across each of Africa's sub-regions.

The paper finds that the status of data protection in Africa is inadequate. This inadequacy is due to many reasons such as dependence of DPAs, financial constraints, lack of institutional capacity and others. These defects are further exacerbated by the COVID-19 pandemic, thereby increasing calls for privacy reforms in Africa. In order to correct these effects while also planning for future dynamics like the COVID-19 pandemic, solutions such as legislative reforms, fiscal viability and multistakeholder partnerships are proffered.

1 Dahir, A. L. (2018, 8 May). Africa isn't ready to protect its citizens personal data even as EU champions digital privacy. *Quartz*. https://qz.com/africa/1271756/africa-isnt-ready-to-protect-its-citizens-personal-data-even-as-eu-champions-digital-privacy; a repository of data protection laws in Africa is available at: https://dataprotection.africa

2. REGIONAL FRAMEWORK AND INSTRUMENTS

2.1 AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION (MALABO CONVENTION) 2014

The Malabo Convention sets a strong intention for the protection of personal data and ensuring cybersecurity in Africa.[2] The Convention seeks to establish a credible framework for cybersecurity in Africa through organisation of electronic transactions, protection of personal data, and promotion of cybersecurity, e-governance and combating cybercrime.[3]

The Convention provides fair information principles, legal basis, and rights of data subjects recognised under other international instruments.[4] It also mandates member states to set up independent data protection authorities.[5] The Malabo Convention provides a personal data protection framework which African countries may potentially transpose into their national legislation for it to have the full force of the law, and encourages African countries to recognise the need for protecting personal data.[6] The Convention will come into effect 30 days after the 15th ratification by a member state.[7] Currently, it has been signed by 14 member states, ratified by five, and deposited to the African Union Commission by six out of 55 members states.[8]

2.2 AFRICAN DECLARATION ON INTERNET RIGHTS AND FREEDOMS

Though not a binding instrument, the African Declaration on Internet Rights and Freedoms has become a regional resource in terms of its policy direction and influence in Africa. The African Declaration emphasises the responsibility of African states to respect, protect and fulfil human rights online for all people.[9] It comprises 13 principles that aim to engender the promotion of fundamental rights of Africans on the internet. The eighth principle provides for privacy and data protection.

The African Declaration restates that everyone has the right to privacy online, including the right to the protection of their personal data. The right

---

2 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf; unlike the EU's General Data Protection Regulation (GDPR), which can be transposed nationally, the lawmaking process in Africa is different, which means Africa-wide instruments do not automatically take effect when in force.

3 Ibid.

4 Articles 13, 16-19.

5 Article 11.

6 Deloitte. (2017). *Privacy is Paramount: Personal Data Protection in Africa.* https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

7 Article 36

8 Status of adoption of the Malabo Convention as of 28 June 2019: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

9 https://africaninternetrights.org/wp-content/uploads/2015/11/African-Declaration-English-FINAL.pdf

extends to anonymous communication on the internet, and the use of appropriate technologies to ensure the security and anonymity of such communication. However, the right does not exist without restrictions, which must be subject to limitations provided by law, be recognised under international human rights law, and be necessary and proportionate in pursuance of a legitimate aim. The processing of personal data must be done with respect to the principles of data processing established under relevant data protection law.

The ninth principle of security, stability and resilience of the internet impacts data protection. Confidentiality and integrity are principles recognised under data protection laws. The Declaration extends to protection against unlawful surveillance, monitoring, unlawful interception of communication by both state and non-state actors and any measure that can undermine security and trust on the internet.

2.3 SADC MODEL LAW ON DATA PROTECTION, 2010

The Southern African Development Community (SADC) developed the model law in 2010 and adopted it in 2013 to promote the protection of human rights in member states. Its preamble acknowledges that the safeguarding of data protection rights aids the preservation of other rights like freedom of expression, movement and association. The model law mandates member states to create an independent data protection authority while also providing for its core mandates and duties and powers to impose sanctions.[10] The law establishes principles of data processing which include data minimisation, accuracy, storage limitations, lawfulness and fairness, purpose limitation and accountability.[11]

It also creates an obligation to notify the supervisory authority when there is a data breach without undue delay and to ensure the rights of data subjects.[12]

2.4 ECOWAS SUPPLEMENTARY ACT A/SA.1/01/10 ON PERSONAL DATA PROTECTION, 2010

The Economic Community of West African States (ECOWAS) Act gives member states direction on what should be provided for in their national data protection laws, while also urging member states to enact data protection laws without prejudice to the interest of the state.[13] The Act demands the setting up of an independent data protection authority by member states. Also, the Act creates a high threshold for protection of special categories of data like genetic data and health research, data relating to offences, sentences or security measures,

10 Articles 5, 3(5) and 9 of the SADC Model Law on Data Protection.

11 Articles 11, 12, 13 and 30 of the SADC Model Law on Data Protection.

12 Article 25 and Part 7 of the SADC Model Law on Data Protection. The data processor is expected to notify the data controller.

13 The ECOWAS member states are Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo. https://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf

↑ A woman raises the black power fist with the South African flag while wearing a facemask. Source: Thema Hadebe

biometric data, and data processed for public interest reasons.[14] It additionally sets out the guiding principles on processing of personal data.

The Act was signed by 13 countries. According to Greenleaf and Georges, this is the only binding regional data protection agreement yet in force in Africa. In addition, once this framework is completed, it may be enforced by the ECOWAS Court of Justice.[15]

2.5 EAC LEGAL FRAMEWORK FOR CYBERLAWS, 2008

The East African Community (EAC) Framework is divided into two parts. The first addresses thematic issues like electronic transactions and electronic signatures, cybercrime, data protection and privacy and consumer protection.[16] The second part addresses intellectual property, competition, e-taxation and information security. Framework I commenced in 2007 and was completed in 2008 and approved in 2010. Framework II started in 2010 and was completed in 2011, and approved in 2013. The implementation is still ongoing. Out of the five countries that are member states, only Kenya and Uganda have a proper data protection act. Rwanda has a splintered framework, while Burundi and Tanzania do not have adequate data protection law.[17]

14 Article 12 of the ECOWAS Supplementary Act on Personal Data Protection.

15 Greenleaf, G., & Georges, M. (2014). African regional privacy instruments: Their effects on harmonization. 132 Privacy Laws and Business International Report 19-21. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566724

16 http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?sequence=1&isAllowed=y

17 The three countries have a data protection bill at different stages.

↑ A man's temperature is being measured with a thermometer gun while wearing a facemask. Source: Themba Hadebe

2.6 DECLARATION OF PRINCIPLES ON FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION IN AFRICA

Perhaps a more direct and binding instrument, the Declaration of Principles on Freedom of Expression and Access to Information in Africa is sourced from the African Charter on Human and Peoples' Rights (ACHPR). The ACHPR is the most primary human rights instrument in Africa, which all African countries are party to and obligated to abide by. Article 9 of the Charter provides for the right to freedom of expression and access to information, which has in turn produced more guidelines on both rights in the digital age.

Since the ACHPR does not provide for the right to privacy, and given the gaps that could be created by such a lacuna, especially in the digital age, the Declaration of Principles, together with the other above-mentioned instruments, further links Africa's most fundamental law on human rights to privacy rights. Principle 40 of the Declaration provides for the protection of people's personal information. Principles 41 and 42 address privacy and communication surveillance and establish the legal framework for the protection of personal information in Africa.

Principle 40 provides that there shall be no indiscriminate storage or sharing of a person's personal information. Sub-section 2 requires that communication surveillance shall only be authorised by law and such law must comply with international human rights law. The last part of the Principle mandates that such law must ensure prior authorisation by a judicial authority, due process, period of use, notification, transparency and an independent oversight mechanism.

Principle 41 focuses on the general scope of what a data protection legislation must protect. The provisions lay out how personal information must be handled, the rights of data subjects, notification, online harms, legal redress and oversight mechanisms.[18]

18 https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf

3. DATA PROTECTION LANDSCAPE IN AFRICA

The continent is divided along the line of countries with a framework, an insufficient framework, and no framework. In some instances, a country like Botswana has a data protection law but the law is yet to take effect, or yet to set up a data protection authority, or a combination of both. The divergent framework creates a fractured terrain for data protection and enforcement of the law across the continent.

However, the protection of the right is as good as the strength of the law. A good number of data protection laws in Africa are considered weak. As will be further discussed below, many countries like Nigeria, Senegal, Kenya and others do not have some key principles of data protection provided for in their respective framework.

This becomes even more evident with concerns around cross-border transfer of data. Most African countries' data protection law mandates the transfer of data to third party states only when the state is considered to have adequate data protection law to protect the rights of individuals. This would be a challenge as the continent looks to closer integration on trade through the African Continental Free Trade Agreement (AfCFTA).[19]

In evaluating the strengths of the laws under focus, there would be recourse to international best practices and standards established under notable international instruments like the Modernised Convention 108+ of the Council of Europe, the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data,[20] the Asia-Pacific Economic Cooperation Privacy Framework,[21] the European Union General Data Protection Regulation (GDPR), the United Nations Guidelines Concerning Computerized Personal Data Files, and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).[22] Although there are common trends in the data protection laws, there are principles that diffe significantly from country to country.

19 Ridwan, O. (2019, 20 March). Africa Continental Free Trade Agreement and cross-border data transfer: Maximising the trade deal in the age of digital economy. *African Academic Network on Internet Policy.* https://aanoip.org/the-africa-continental-free-trade-agreement-and-cross-border-data-transfer-maximising-the-trade-deal-in-the-age-of-digital-economy

20 https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflow-sofpersonaldata.htm

21 https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

22 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

3.1 DATA PROTECTION ACROSS FOUR MAJOR SUB-REGIONS IN AFRICA

Table 1.

Key data protection issues	Senegal	Nigeria	Kenya	Uganda	Morocco	Tunisia	South Africa	Mauritius
Legislation (Status)	[23] ✓ (Enforced)	[24] ✓ (Enforced)	[25] ✓ (Not yet enforced)	[26] ✓ (Not yet enforced)	[27] ✓ (Enforced)	[28] ✓ (Enforced)	[29] ✓ (Partially enforced)	[30] ✓ (Enforced)
Rights of data subjects	✓	✓	✓	✓	✓	✓	✓	✓
Data protection principles	✓	✓	✓	✓	[31] ✓	✓	✓	✓
Legal basis for processing	✓	✓	✓	✓	✓	✓	✓	✓
Data security	✓	✓	✓	✓	✓	✓	✓	✓
Data breach notification	×	[32] ×	✓	✓	×	×	✓	✓
Cross-border data flow	✓	✓	✓	✓	[33] ✓	[34] ✓	[35] ✓	✓
Registration with supervisory authority	✓	×	✓	×	[36] ✓	✓	×	✓
Data protection impact assessment	×	[37] ×	✓	×	×	×	✓	✓
Privacy by design and default	×	×	✓	×	×	×	×	×
Appointment of data protection officer/information officer [38]	×	✓	✓	✓	×	×	×	✓
Supervisory authority	[39] ✓	[40] ✓	[41] ✓	[42] ✓	[43] ✓	[44] ✓	[45] ✓	[46] ✓
Remedies, enforcement and sanctions	✓	✓	✓	✓	✓	✓	✓	✓

As may be gleaned from Table 1, while all of the countries have data protection laws, in some the laws are not yet in force. Kenya and Uganda fall into this category. Also, while some are in force, they are not fully enforced. South Africa is an example of such a country.

Some countries do not provide for notification of breaches in their laws, and this includes Senegal, Nigeria, Morocco and Tunisia. Also, though not in force, only Kenya provides for privacy by design in its data protection framework. In addition to this, Senegal, Nigeria, Uganda, Morocco and Tunisia's laws do not provide for data protection impact assessment. These national contexts present a snapshot of the inadequacy of the data protection framework in Africa.

23 Law No. 2008-12.

24 Nigeria Data Protection Regulation.

25 Data Protection Act 2019.

3.2 CHALLENGES OF DATA PROTECTION IN AFRICA

In our assessment of the laws, it could be seen that even in the countries that have enacted a data protection law, the law is inadequate in protecting rights and other key data protection principles due to the challenges highlighted below.

3.2.1 DEPENDENCE OF DATA PROTECTION AUTHORITIES

The absence of full independence to discharge their duties limits the capability for enforcement. Our findings revealed that the constitution of some supervisory authorities is contrary to recognised international standards.[47]

As an example, the Nigerian data protection supervisory authority is an agency of the government, with members of the executive arm of the government constituting its governing board. This is contrary to articles 11(1)(b) and 11(1)(6) of the Malabo Convention,[48] which states that membership of the data protection authority shall be incompatible with membership of government.[49] In Mauritius, the DPA is materially and institutionally dependent on the Prime

26 Data Protection Act 2019.

27 Law No. 09-08 and Decree No. 2-09-165.

28 Organic Act No. 2004-63. The law is limited in application to private organisations. There is no obligation on public organisations.

29 Protection of Personal Information Act 2013.

30 Data Protection Act 2017.

31 Does not include data minimisation principle.

32 This was not addressed in the Regulation, but is mentioned in the Data Protection Draft Implementation Framework that is yet to be adopted.

33 Needs authorisation of the National Data Protection Commission (CNDP).

34 Needs authorisation of the CNDP.

35 Needs approval of the information regulator.

36 Prior to processing data, the National Authority for Protection of Personal Data (INPDP) must be notified.

37 This was not addressed in the Regulation, but mentioned in the Data Protection Draft Implementation Framework that is yet to be adopted.

38 The South Africa Protection of Personal Information Act refers to it as an information officer.

39 Commission of Personal Data (CDP).

40 National Information Technology Development Agency (NITDA).

41 Not yet set up. A data protection commissioner is yet to be appointed.

42 Not yet set up. It will be domiciled within the National Information Technology Authority (NITA). Its independence has been questioned.

43 Data Protection National Commission (CNDP).

44 National Authority for Protection of Personal Data (INPDP).

45 Information regulator.

46 Office of the Data Protection Commissioner.

47 In Uganda, though yet to be set up, the Office of the Privacy Commissioner is domiciled inside another government agency. The situation is the same in Kenya.

48 Nigeria is yet to sign and ratify the Convention.

49 See also Article 14(2) and 16 of ECOWAS Supplementary Act on Personal Data Protection, Article 16(5) of the Council of Europe Modernised Convention 108 and Article 52 of the EU General Data Protection Regulation.

Minister's Office and is unable to administer fines to offenders. Similarly, in Ghana, the governing body of the DPA may receive ministerial directives on policy matters. The lack of independence would limit the effectiveness of the regulator.[50]

There are no immediately available best standard structures that ensure the independence of DPAs in Africa. What may, however, serve for introspection with respect to ensuring independence for DPAs in Africa will be what Senegal is currently seeking to do, which is legal reform to address the gaps identified since the law was passed in 2008.[51] While the proposed law does not address all of the problems identified in this section, it identifies the need to ensure more independence for the Commission on Personal Data.

3.2.2 FINANCIAL CONSTRAINTS

Lack of funding to exercise statutory functions will limit the capability of data protection regulators to ensure people's data protection rights. A poorly funded DPA will also lack the requisite resources to employ the best brains, conduct audits, investigate, issue sanctions effectively, and carry out other statutory functions. This could be partly responsible for why some countries have yet to set up their data protection authorities.

3.2.3 INADEQUACY AND LACK OF IMPLEMENTATION OF LAWS

Kenya, Uganda, Botswana, Equatorial Guinea, Seychelles and Madagascar are examples of countries that have passed laws and are yet to set up their DPAs. The absence of the regulator to enforce the law leaves data protection rights unprotected.

Also, there are countries that do not have any law on data protection, or inadequate law. As an example, Nigeria uses a secondary legislation and the president is yet to assent to the Data Protection Bill that was passed in 2019.[52] In contrast, countries like Tanzania, Sudan, Ethiopia, Libya and Djibouti do not have any law. The absence of law does not offer any protection to citizens of such a country. Similarly, such a country will be considered inadequate for transfer of data, which could impact trade and economy.

---

50 In July 2019, NITDA announced the investigation of the Nigeria Immigration Services over exposure of the passport page of a Nigerian citizen through its Twitter account. Almost a year on, it is yet to issue a sanction or go public with the status of the investigation. This Day. (2019,13 July). NITDA investigating banks, telcos, immigration for privacy rights violation. https://www.thisdaylive.com/index.php/2019/07/13/nitda-investigating-banks-telcos-immigration-for-privacy-rights-violations

51 Senegal Digital Strategy (2016-2025). https://www.sec.gouv.sn/sites/default/files/Stratégie%20Sénégal%20Numérique%202016-2025.pdf

52 The subsidiary legislation is weaker, compared to an Act of Parliament.

3.2.4 LACK OF INSTITUTIONAL CAPACITY

Data protection is a nascent development in the larger part of the continent. The regulators are still learning to bite, and would still need to invest in capacity development to function optimally. As an example, one year on after releasing the Nigeria Data Protection Regulation, the National Information and Technology Development Agency (NITDA) – the government agency that released the regulation – is yet to publish its Data Protection Draft Implementation Framework or issue any guide, guideline or guidance. A strong institution with independence and human capacity will aid the enforcement of data protection rights across the continent. According to a report by ID4Africa, DPAs in African jurisdictions currently range from as few as three to as many as 11.[53]

3.2.5 DUPLICATED AUTHORITIES

This is a problem in countries where data collection is done by multiple government authorities and where data protection laws are in sector-specific pockets. In Nigeria, the personal data of citizens is collected by multiple government agencies, and by extension, this makes those agencies regulators in respect of such data. Similarly, government agencies like the Federal Competition and Consumer Protection Commission and the Central Bank of Nigeria could have limited jurisdiction regulating data protection infringement. This, if not properly managed, could create overlaps and confusion.

3.2.6 LEGISLATIVE STANDARDS

The quality of law in some African countries is not in touch with modern reality on data protection. In Tunisia and Morocco, organisations need to submit requests to the regulator to transfer data outside the country. In Tunisia, the approval could take two months, and this could hurt digital trade that needs the mobility of data in real time. Similarly, in 2018, an EU delegation examined the Moroccan law and identified a number of shortcomings, such as the absence of references to biometric data or sexual orientation, no right to data portability, no detailed conditions related to the validity of consent, the lack of requirements to notify the authority of data breaches, the absence of a data minimisation principle, and limits of powers granted to the Moroccan data protection authority, the CNDP.[54]

It can be gleaned from the countries under focus that some do not have modern data protection measures like privacy by design and default, which only appeared in the Kenyan law. Data protection impact assessment is only

53 ID4Africa. (2019). Roundtable of African Data Protection Authorities: Status and response to privacy risks in identity systems. https://www.id4africa.com/2019/files/RADPA2019_Report_Blog_En.pdf

54 Chenaoui, H. (2018, 11 September). Moroccan data protection law: Moving to align with EU data protection? *International Association of Privacy Professionals.* https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection

present in the Kenyan and Mauritius law and absent in the four other countries.[55] Similarly, data breach notification is absent in the laws of Senegal, Tunisia and Morocco. Lastly, accountability from organisations is hampered when there is no legal obligation to appoint a data protection officer; Senegal, Morocco and Tunisia do not have such requirements.

4. COVID-19 AND DATA PROTECTION IN AFRICA

The outbreak of the novel cononavirus continues to strike the core of the world's existence, spreading along its trail pressured healthcare systems and devastating socioeconomic impacts.

Africa is not spared from the dispersion of the virus; the continent recorded its first case in February in Egypt.[56] On 11 March 2020, the World Health Organization declared COVID-19 a pandemic.[57] In containing, detecting, preventing and combating the virus, governments are imposing urgent measures. In Africa, 45 countries have introduced different legislative measures, and 37 countries have imposed various limitations on human rights.[58] Due to the measures that many countries have had to carry out against the pandemic, it has become necessary to ensure that such measures adhere to human rights protection, most especially, data protection.[59]

Combating the virus implies that the government may deploy a number of measures that could possibly impact on people's fundamental rights, and specifically data protection rights. Of the 18 African countries that had declared states of emergency in response to fighting the pandemic at the time of writing, only seven countries have data protection laws in force.[60] The effect of a state of emergency is the derogation of civil liberties until peace and order is restored. It is, however, not a blanket derogation of all liberties and rights. The enforcement of extreme measures is not grounds for total erosion of fundamental rights or unlimited suppression of rights and freedoms under the garb of public interests.

Protecting these rights becomes more important knowing the penchant of African states for information censorship, surveillance, excessive data retention, interception of communication, and internet shutdowns. There is also fear of normalisation of some of the emergency measures currently adopted. Some of the emerging issues identified by the International Centre for Not-For-Profit

55 Though this is contained in the Data Protection Draft Implementation Framework in Nigeria, the framework is yet to be adopted.

56 WHO. (2020, 25 February). A second COVID-19 case is confirmed in Africa. https://www.afro.who.int/news/second-covid-19-case-confirmed-africa

57 WHO. (2020, 11 March). WHO Director-General's opening remarks at the media briefing on COVID-19. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

58 The governments of Botswana, Sierra Leone and Senegal declared a public health emergency.

59 According to the United Nations, the pandemic is becoming a human rights crisis. United Nations. (2020). COVID-19 and Human Rights: We are all in this together. https://www.un.org/sites/un2.un.org/files/un_policy_brief_on_human_rights_and_covid_23_april_2020.pdf

60 These are Cape Verde, Côte d'Ivoire, Senegal, Botswana, Guinea, Angola and Equatorial Guinea.

Law (ICNL) are the limited oversight on the scope of emergency measures, the impact of emergency measures on vulnerable populations, the use of legislation that regulates freedom of expression and access to information, and the use of digital technologies during and post COVID-19.[61]

4.1 ADDRESSING COVID-19 AND THE IMPACT ON HUMAN RIGHTS

The emergency measures adopted by different African countries in combating the pandemic present an opportunity for violation of human rights. The imposition of full or partial restriction of movement and public gatherings impacts on the freedom of movement and association. The use of location-based data impacts on the right to privacy and data protection. Isolation and quarantining of patients impacts on the right to personal liberty. Addressing the public health crisis is one of the acceptable instances for restrictions and conditions where rights can be limited. However, countries like Malawi, Kenya, Nigeria, Zimbabwe and Rwanda have militarised the enforcement of limitations on public gatherings, resulting in killings, brutality and abuse of citizens.[62]

The United Nations (UN) Secretary General, in a recent address, declared the response taken by some countries as a human right crisis.[63] This is borne out of the fear that human rights could be suppressed under the garb of combating the virus. These measures could impact the rights of people when implemented without lawful safeguards. According to UN High Commissioner for Human Rights Michelle Bachelet:

> Emergency measures may well be needed to respond to this public health emergency. But an emergency situation is not a blank check to disregard human rights obligations. Emergency measures should be necessary and proportionate to meet that need. People should be fully informed about the emergency measures and told how long they will remain in effect. The enforcement of emergency measures needs to be applied fairly and humanely.[64]

4.2 DATA PROTECTION AND THE RESPONSE TO COVID-19: IMPACT ON THE CONTINENT

In the light of the outbreak, some countries' data protection authorities have issued guidance, guidelines or some other policy direction, clearly laying out a blueprint for both public and private organisations on how to respect the data protection rights of their citizens. In countries with regulators but without guid-

61 African Government Responses to COVID-19: https://www.icnl.org/post/analysis/african-government-response-to-covid-19

62 There are also reports of suppression of journalists in Zimbabwe and Nigeria using "fake news" and cybercrime laws, respectively, to criminalise information against public officials in the frontline.

63 United Nations. (2020). Op. cit.

64 UN High Commissioner for Human Rights. (2020, 9 April). COVID is "a colossal test of leadership" requiring coordinated action. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25785&LangID=E

ance, the implication is that recourse will be made to the letters of the extant law to prevent abuse of data protection rights.

In contrast, countries with inadequate or non-existing law risk violations of the freedoms and rights of their citizens. The absence of a data protection law exposes them to gross abuse, indiscriminate surveillance, lack of transparency and accountability with processing of information, violation of their rights without redress, and other real or imminent risk.

Another challenge is the limited oversight of the procedures for processing information and the technology deployed, and exposure of vulnerable groups like refugees and the poor. According to the UN, it is important to factor in vulnerable persons while responding to the pandemic in order to adequately protect rights.[65]

4.3. MEASURES TAKEN BY AFRICAN DATA PROTECTION AUTHORITIES ON COVID-19

The data protection authorities in South Africa,[66] Mali,[67] Senegal,[68] Mauritius,[69] Morocco,[70] Tunisia,[71] Burkina Faso[72] and Nigeria[73] have issued guidance or statements, urging both public and private organisations to be responsible with data processing. There is relative similarity in the approaches by governments – the minimum requirement is that data can only be used during this period according to the safeguards provided by law. Data must be processed lawfully and strictly for the purpose of combating the virus. Also, organisations are required to be accountable by processing personal information of data subjects in a responsible manner during the management of COVID-19 and to keep proper documentation,

65 Ibid.

66 Information Regulator (South Africa). (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://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf

67 Niang, B. (2020, 1 April). Covid-19: the APDP's warnings on the collection of personal data and the protection of people's privacy. APDP. https://apdp.ml/covid-19-les-mises-en-garde-de-lapdp-sur-la-collecte-de-donnees-personnelles-et-la-protection-de-la-vie-privee-des-personnes

68 Commission de Protection des Données Personnelles. (2020, 24 April). "Press release: The protection of personal data in the context of the COVID-19 pandemic. https://www.cdp.sn/content/communique-sur-la-protection-des-donnees-personnelles-dans-le-contexte-de-la-pandemie-liee

69 Data Protection Office. (2020, 17 April). Guide on data protection for health data and artificial intelligence solutions in the context of the Covid-19 pandemic. http://dataprotection.govmu.org/English/Documents/Guide%20on%20Data%20Protection%20for%20health%20data%20and%20AI.pdf

70 Commission Nationale de Contrôle de Protection des Données à Caractère Personnel. (2020, 22 April). Press release of 04/22/2020. https://www.cndp.ma/fr/presse-et-media/communique-de-presse/668-communique-de-presse-du-22-04-2020.html

71 Instance Nationale de Protection des Données Personnelles. (2020, 27 March). Recommendations of the National Personal Data Protection Office relating to the protection of personal data in the COVID-19 period. https://globalprivacyassembly.org/wp-content/uploads/2020/04/COMMUNIQUE-DE-LINPDP-COVI D-19.pdf

72 Ouedraogo-Bonane, M. (2020, 4 April). Message from the CIL on the coronavirus pandemic (COVID-19). https://globalprivacyassembly.org/wp-content/uploads/2020/04/Message-de-la-CIL-CORRIGEcongo.pdf

73 IT Edge. (2020, 30 March). COVID-19 Data Collection Complies With NDPR, Says NITDA. http://itedgenews.ng/2020/03/30/covid-19-data-collection-complies-with-ndpr-says-nitda/

and take technical and organisational security measures to protect the data.[74] Data should only be stored for the duration of the pandemic, and can only be retained beyond the period for research, statistical or historical purposes.[75] Data can be used for other purposes if it is necessary to prevent a serious and imminent threat to public safety or public health. The Senegalese authority also urged that ethics should play a role.[76]

Health data is categorised as sensitive personal data and the processing prohibited subject to few exceptions. For example, in South Africa, under the recently published Guidance Note on the Processing of Personal Information in the Management and Containment of the COVID-19 Pandemic:

> [M]edical professionals, healthcare institutions or facilities or social services may process special personal information of a data subject, if such processing is necessary for the proper treatment and care of a data subject in the context of covid-19.[77]

On the legal basis for processing, public interest, vital interest, and existence of a legal obligation was a common thread. However, the South African Information Regulator included the legitimate interest of a controller or a third party. South Africa permits electronic communication service providers to provide the government with mobile location-based data of data subjects and the government can use such personal information in the management of the spread of COVID-19.[78] In Nigeria, the NITDA stated that the collection of information being carried out to address the spread of the virus is justifiable on the legal basis of vital interest and public interest, and conforms to the Nigerian data protection framework.[79] The regulator is yet to issue comprehensive guidance on the intersection of data protection and COVID-19.

4.4 DATA PROTECTION AND COVID-19 RESPONSE

Some of the technological measures deployed in the fight against the COVID-19 pandemic leverage on personal data and could impact on data protection. Under most data protection laws on the continent, health data, biometric data and genetics are considered sensitive personal data, whose processing is usually expressly prohibited, except in limited circumstances.[80] These circumstances

74 The data should be archived or deleted after the pandemic.

75 Mauritius requires this to be documented in a record of processing activities.

76 Commission de Protection des Données Personnelles. (2020, 24 April). Op. cit.

77 Such as vital interest of the patient, public health, existence of legal obligation, etc. See generally Section 4.11.1 of the Guidance Note on the Processing of Personal Information in the Management and Containment of the COVID-19 Pandemic. https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf

78 The guidance allows the use of location data for mass surveillance to manage the spread of the virus, when such data is anonymised or de-identified.

79 IT Edge. (2020, 30 March). Op. cit.

80 Nigeria, Senegal, Burkina Faso, Kenya, Mauritius, etc.

include responding to public health crises, and when the data is processed under the vital interest or legitimate interest of a data subject.

In South Africa, telecom location data is being used to aid contact tracing.[81] In Nigeria, it was reported that the country's governors' forum is collaborating with one of the telecommunication companies on measures to combat the virus[82] and the Minister of Communications and Digital Economy was reported to have said that data mining of SIM cards and national biometric bank verification numbers will be used to determine the vulnerable population.[83]

A response without respect for lawful safeguards raises apprehension of excessive and long-term surveillance and its possible normalisation post COVID-19.[84] There is fear of discrimination without an avenue for accountability and the historical lack of transparency from the government.[85] The fear is aggravated with the number of African countries with poor human rights records, where the government is happy to justify the extreme measure of surveillance under the garb of public interest or national security. There is fear the pandemic could be used as a basis for the government to retain data beyond the pandemic and for other purposes including unlawful surveillance and discrimination.[86]

Responding to the crisis is not sufficient grounds to completely suppress the data protection rights of citizens. The discourse is not between public health or data protection, it is public health *and* data protection. The two extremes are fatal to the effort to combat the epidemic.

The fight against COVID-19 involves the collection and processing of vast amounts of personal data. Data protection laws do not hinder this processing, but require that it be done with appropriate legal bases and taking data protection principles into account. The pandemic is a public health crisis necessitating urgent measures to curb and eradicate it. Nonetheless, upholding data protection is equally crucial for the preservation of human rights before, during and after the pandemic. Governments must take every measure to preserve civic and democratic space and help to build and preserve trust in institutions. Measures deployed must be non-intrusive, limited in time and purpose, and abide by the

---

81 Kahla, C. (2020, 26 March). SA government will be tracking mobile phones to curb COVID-19. *The South African.* https://www.thesouthafrican.com/news/government-tracking-mobile-phones-curb-covid-19/

82 Nigeria Communications Week. (2020, 7 April). Governors, MTN Partner to Halt Spread of COVID-19 with Data. https://www.nigeriacommunicationsweek.com.ng/governors-mtn-partner-to-halt-spread-of-covid-19-with-data

83 Adanikin, O. (2020, 24 April). COVID-19: Controversy trails Ministers' decision to mine data of phone users without consent. *International Centre for Investigative Reporting.* https://www.icirnigeria.org/covid-19-controversy-trails-ministers-decision-to-mine-data-of-phone-users-without-consent

84 Wintour, P. (2020, 23 April). Coronavirus pandemic is becoming a human rights crisis, UN warns. *The Guardian.* https://www.theguardian.com/world/2020/apr/23/coronavirus-pandemic-is-becoming-a-human-rights-crisis-un-warns

85 Ebert, I. (2020, 26 March). Commentary: Gathering data through COVID-19 tracking apps can result in discrimination & violations of the right to privacy. *Business and Human Rights Resource Centre.* https://www.business-humanrights.org/en/commentary-gathering-data-through-covid-19-tracking-apps-can-result-in-discrimination-violations-of-the-right-to-privacy

86 The prospective use of "immunity cards" could cause discrimination. Patel, N. V. (2020, 9 April). Why it's too early to start giving out "immunity passports". *MIT Technology Review.* https://www.technologyreview.com/2020/04/09/998974/immunity-passports-cornavirus-antibody-test-outside/

strictest protections and international human rights standard.[87]

5. RECOMMENDATIONS

5.1 LEGISLATIVE REFORM

Countries without legislation will need to enact a data protection law to prevent abuse and protect people. Countries with inadequate or old laws will need to modernise their laws to reflect the new norms and trends in international law. An archaic or inadequate law will remain insufficient in protecting people.

The enactment of the GDPR in Europe is quite commendable and there has been a clamour for a similar shift in Africa. Again, online risks are decentralised and ignore the maturity stage of infrastructure. Africa will need to integrate and harmonise its data protection laws to bring countries from the three categories to a common ground. The signing, ratification and transposition of the Malabo Convention or regional instrument should be the minimum requirement for such harmonisation. This has become more important as the continent is looking to integrate through a common market.[88]

5.2 COLLABORATION

Countries will need to collaborate on efforts to effectively strengthen the regulatory landscape on the continent. DPAs will need to develop intra-continental and, where necessary, international mechanisms for cooperation to facilitate an effective enforcement landscape and data protection. This could be by way of joint investigation, knowledge sharing and capacity building, notification, complaint referral, and other forms of mutually beneficial assistance.[89]

5.3 FISCAL VIABILITY

Financial constraints are among the challenges identified in the countries under consideration. While most data protection authorities are funded by the government, the authorities could explore innovative ways to limit financial dependency on an unwilling government. Inward funding through effective management of monies realised from implementing a data protection law could be an effective way of financing a DPA, for example. This model is a multistakeholder approach, wherein DPAs build stronger collaboration with research institutions and share human resources.

---

87 UN Sustainable Development Group. (2020). *Shared Responsibility, Global Solidarity: Responding to the socio-economic impacts of COVID-19.* https://www.un.org/sites/un2.un.org/files/sg_report_socio-economic_impact_of_covid19.pdf

88 As an example, Morocco has not considered any African country adequate for transfer of data. https://www.cndp.ma/images/deliberations/deliberation-n-236-2015-18-12-2015.pdf

89 There is the Association of Francophone Data Protection Authorities (AFAPDP).

5.4 ACCEDING TO INTERNATIONAL INSTRUMENTS

More African countries need to accede to more international instruments on data protection and different regional instruments. Accession to these instruments will improve the quality of our laws, and bring them abreast with current reality. Ratifying Convention 108 would also ease a signatory state's consideration for an adequacy decision by the European Commission. The adequacy decision will ease the free flow of data and would facilitate transnational trade. Four African countries (Senegal, Tunisia, Mauritius and Cape Verde) have already ratified the Council of Europe Modernised Convention 108.[90]

↓ A man wears a facemask.
Source: Jandro Saayman

5.5 STRENGTHENING INSTITUTIONS

An independent data protection authority is critical to the success of protecting personal data. A supervisory authority that is not independent may cause conflict of interests, will be ineffective and inefficient in enforcement, and would be subject to compromise from other arms of the government. The constitution and the workings of the DPA should be independent according to best practices and standards enunciated in international instruments.

5.6 MULTISTAKEHOLDER APPROACH

The development of data protection in Africa is still ongoing. What this suggests is the need to maximise partnerships while also working towards effective implementation of a strong data protection landscape for Africa. Key stakeholders

90 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=0MQrfqMP

like governments, civil society, the private sector, academia and research and development need to work together. For example, one of the practical ways of implementing such an approach, especially given the current realities, is to establish ad-hoc multistakeholder committees with representatives of each key stakeholder mentioned above.[91] Not only does this ensure a level of transparency, it provides an avenue for accountability on data use and protection.

6. CONCLUSION

The risks posed by technology are many, especially given our realities. This paper considers these risks given the current status of data protection in Africa. It finds that the framework of protection is inadequate. These inadequacies have been highlighted and recommendations on how best to navigate them have also been proffered. What stands out prominently in the paper is how inadequate the data protection landscape is in Africa and how the fight against the COVID-19 pandemic may exacerbate the existing gaps and put data protection rights in danger. What will be required is a smart mix of ideas, and it is hoped that the issues discussed and solutions proffered will be further explored not only to improve data protection in Africa but also to respond to the current needs for protection during the COVID-19 pandemic.

91 Ilori, T., & Adeboye, A. (2020, 20 April). How to protect Nigerians' personal information while combating COVID-19. *Global Voices.* https://globalvoices.org/2020/04/20 how-to-protect-nigerians-personal-information-while-combating-covid-19