Mapping and Analysis of

Privacy Laws and Policies in Africa

Summary Report

July **2021**

CIPESA

Table of Contents

1.0 Introduction

Privacy in the digital age has become a preeminent human rights issue, given its intricate connection with, and its being a foundation for the realisation of other rights such as freedoms of expression, information, assembly, and association. Yet, while privacy has become ever more crucial in the world where digital technologies are key to livelihoods and the promotion of other rights, there are insufficient protections for the right to privacy in many African countries. Indeed, many countries in the region have steadily taken measures to undermine this right.

Over the years, many African countries have enacted laws and adopted policies that impact on privacy, including those that facilitate surveillance and the collection of biometric data, and others that limit the use of encryption. This has facilitated increased state surveillance across the continent that is accelerating interference with various rights and freedoms. In many countries, surveillance is increasingly being used to entrench political control including through spying on activists, journalists, and dissidents. Related phenomena such as the limitation or prohibition of encryption, building of biometric databases, and data localisation requirements, also have a bearing on citizens' rights to privacy and other digital rights. While prohibition on encryption services undermines citizens' rights to communicate anonymously[1] - a key necessity for free expression particularly in authoritarian countries - data localisation and biometric databases could, in the absence of robust legal and practical safeguards, further facilitate efforts by state and non-state actors to undermine privacy-related rights.

In many African countries, the advent of the COVID-19 pandemic has exacerbated the privacy concerns yet in several of them, digital rights were already under steady attack, including via internet shutdowns, criminalisation of "false news", misinformation and disinformation campaigns by state and non-state actors, harassment and prosecution of social media users, and growing state surveillance. In responding to the pandemic, countries adopted regulations and practices, including deploying surveillance technologies and untested applications, to enable authorities collect and process personal data for purposes of tracing, contacting, and isolating suspected and confirmed cases of the virus. These measures were adopted in haste, often without adequate regulation or independent oversight.

Given the foregoing, it is crucial to map and analyse the laws and policies that impact on privacy, notably those that regulate surveillance, data localisation, biometric databases and encryption. This analysis can inform remedial and mitigatory steps to protect the right to privacy, which may include strategic litigation, capacity building, and advocacy for legislative and policy reforms. Moreover, the results of this analysis are also crucial for monitoring developments and trends on privacy regulation and practice in the region.

.....

1 *Submission to the UN Special Rapporteur on freedom of expression – anonymity and encryption in digital communications, February 2015 https://www.ohchr.org/Documents/Issues/Opinion/Communications/PrivacyInternational.pdf*

1.1 **Methodology**

The research employed a qualitative approach, including legal and policy analysis, literature review, and key informant interviews to establish the laws in place that are relevant to privacy. Specific interest was in provisions on surveillance, data localisation, biometric databases, and limitations on encryption. The research reviewed the gaps, safeguards and remedies in the legislation and how they measure up to international human rights laws and standards that protect individual privacy from unsanctioned surveillance on digital platforms. The study covered 19 countries - Cameroon, Chad, Egypt, Ethiopia, Kenya, Ghana, Malawi, Mali, Mozambique, Namibia, Nigeria, Rwanda, Senegal, Tanzania, Tunisia, Uganda, Zambia, Zimbabwe, and South Africa.

In assessing the various laws and policies, the study employed the African Commission on Human and Peoples' Rights (ACHPR) Declaration on Principles of Freedom of Expression and Access to Information in Africa[2] (hereinafter "the Declaration"), as the frame of reference. The Declaration is an important instrument as it sets common benchmarks that African countries should comply with to protect and promote citizens' rights in the online domain.

Using a recognised and standardised continental Declaration as the frame for the analysis makes the results directly relevant to litigation and advocacy and also enhances the possibilities for further research and documentation. In particular, principles 37-42 of the Declaration were identified as the principal lens of analysis. These principles focus on the rights to freedom of expression and access to information in the internet age.

2 *Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019, https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf*

2.0 Summary of Findings

International human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights provide for the right to privacy in their articles 17 and 12 respectively. At the regional level, the African Charter on Human and Peoples' Rights (ACHPR) has no specific provision on the right to privacy, but provides for the respect for a person's dignity.[3] Further, while the African Union Convention on Cybersecurity and Personal Data Protection, the continent's model instrument on privacy and data protection, provides safeguards for personal privacy and data protection, most states are yet to sign or ratify it.[4] Also, by August 2020, only 31 African countries out of the 55 had adopted specific personal data protection laws.[5] In addition, Senegal, Nigeria, Uganda, Morocco and Tunisia's laws do not provide for data protection impact assessment.[6]

Overall, a review of various African countries' privacy legal frameworks as part of this research shows notable progress but violations of privacy rights by state and non-state actors are on the rise. As the report shows, many of the countries' laws do not measure up to international human rights standards and fail to establish clear and appropriate oversight, redress and remedy mechanisms.

2.1 Growing Surveillance

Principle 41 of the Declaration provides that states shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications. The Principle further states: "States shall only engage in targeted communication surveillance that is authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim."

Additionally, states are required to ensure that any law authorising targeted communication surveillance provides adequate safeguards for the right to privacy, including the prior authorisation by an independent and impartial judicial authority; due process safeguards; and specific limitation on the time, manner, place, and scope of the surveillance. Other safeguards specified are notification of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance; proactive transparency on the nature and scope of its use; and effective monitoring and regular review by an independent oversight mechanism.

.....

3 *African Charter on Human and Peoples' Rights, https://www.achpr.org/legalinstruments/detail?id=49*

4 *African Union Convention on Cybersecurity and Personal Data Protection, "Status List" as at 28th April, 2021, https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf*

5 *Data Protection Laws in Africa: A PanAfrican Survey and Noted Trends https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf*

6 *Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solutions https://africaninternetrights.org/sites/default/files/Tomiwa%20Ilori_AfDec_Data%20protection%20in%20Africa%20and%20the%20COVID-19%20pandemic_Final%20paper.pdf*

Laws in various countries have criminalised illegal surveillance and placed various safeguards on the conduct of state surveillance. However, many of them contain retrogressive provisions that leave scope for intrusion, including enabling state surveillance with limited safeguards.

Indeed, "national security" considerations have been employed in laws in various countries broadly to justify and authorise the interception of communication, restrict privacy rights, grant wide search and seizure powers to law enforcement agencies, mandate intermediaries such as telecommunication service providers to facilitate interception, and to require data localisation. For example, while some countries prohibit unauthorised access to data, state security agents have violated such provisions as happened in Uganda in 2018 when security agents stormed a telecom provider's data centre without a court warrant. Notably, Rwanda references their interception of communication law in the preamble to legislation that requires local data hosting. What is of great concern is that in many African countries, security agencies are known to misuse their surveillance powers, often to target journalists, opposition politicians, and human rights activists rather than to detect, investigate and prevent crime.

The current research has found that most of the laws reviewed do well by requiring a judicial authority to authorise surveillance. The laws in Kenya, Nigeria, Tanzania, Tunisia, Uganda for example, require an interception warrant or order from a judicial officer. However, in a few cases such as in Zimbabwe, authorisation is offered by non-independent and partial actors such as ministers who have power to issue, amend and revoke warrants for interception.

Some countries fall short on the provisions of the Declaration such as manner and scope of surveillance, and transparency on the surveillance activity, including notification requirements. Among the areas of concern is the period of validity of warrants. Notably, Tanzania's cyber crimes law does not state the validity period of the interception order. In Tunisia, section 54(5) of the Organic Act No. 26 of 2015 Relating to the Fight Against Terrorism and the Suppression of Money Laundering provides that an interception order must identify the specific types of communications subject to interception or monitoring, for a period that cannot exceed four months and that can only be renewed once. In Zimbabwe, the interception of communications law gives a maximum validity period of three months, but the minister can extend the validity for a period not exceeding three months. In Zambia, the validity of the interception order is three months and can be renewed by a judge for a period at their discretion. Uganda's validity period is also three months and may be renewed by a judge for a non-specified period (article 6). Cameroon offers a maximum validity of four months, per article 245(4) of the 2010 cybersecurity law.

Many of the laws and policies reviewed provide for sanctions and penalties for illegal surveillance and for failure by service providers to comply with court orders, or to facilitate state surveillance. Illegal surveillance is penalised in all countries and this includes service providers who are barred from engaging in random monitoring of subscribers' communications. The sanctions for unauthorised surveillance vary, ranging from fines, imprisonment or both.

Meanwhile, operators face stiff sanctions for failing to assist governments in conducting surveillance activities. In Nigeria, penalties for failure to render interception assistance to government agencies is punishable with a fine of USD 12,273 or licence revocation, Tunisia (USD 365-1,823), and Uganda (USD 667, up to five years imprisonment, or both).

2.2 **Limitations on Encryption**

Principle 40(3) of the Declaration obligates states not to adopt laws or other measures prohibiting or weakening encryption, including backdoors, key escrows, and data localisation requirements, unless such measures are justifiable and compatible with international human rights law and standards.

Anonymity and the use of encryption in digital communications engage both the right to freedom of expression and right to privacy very closely because without effective protection of the right to privacy, the right of individuals to communicate anonymously and without fear of their communications cannot be guaranteed.[7]

There were a few positive provisions noted in some countries that require the protection of personal data through technical security measures which include encryption. On the other hand, many countries under study have passed legislation that limit anonymity and the use of encryption through criminalisation of possession and use of cryptographic software or hardware, providing for fines and prison sentences. In other countries, there are penalties for offering cryptographic services without licensing, registration or authorisation.

Whether used to protect sensitive information or to verify identities, individuals and corporations alike benefit from cryptographic software in a world that is becoming increasingly networked.[8] Yet governments are increasingly restricting the use of these privacy tools because of fear that they will hamper their capacity to fight terrorism and crime.[9] These restrictions significantly and disproportionately violate the rights enshrined in Article 19 of the International Covenant on Civil and Political Rights (ICCPR) as well as national constitutional guarantees.[10]

In all countries studied there is mandatory SIM card registration, during which a horde of identifying data is collected. Telecom companies, regulators, and other government agencies (sometimes including those in charge of national identification, COVID-19 relief efforts and electoral processes) have access to this data. Moreover, several countries are increasingly collecting biometric data, creating various databases, and pegging access to public services to information in these databases, yet some countries lack data protection laws, or hardly implement the data protection legislation where it is in place. As has been argued,[11] SIM registration, in effect, eradicates the ability of mobile phone users to communicate anonymously and facilitates mass surveillance, making tracking and monitoring of all users easier for law enforcement and security agencies.

In Chad, Malawi, Senegal, Tanzania, Tunisia and Zambia, there are penalties for offering cryptographic services without licensing, registration or authorisation. Interception of communications provisions often require service providers to decrypt any encrypted information that they may intercept in the course of offering assistance to lawful interception. In countries such as Mali and Tanzania, the laws require the encryption services providers, upon registration with the authorities, to disclose the technologies they plan to use for encryption. In some countries, the requirements around encryption services providers are contained in laws governing the ICT sector, in e-transactions laws and cybersecurity laws.

.....

7 *Privacy International, Submission to the UN Special Rapporteur on freedom of expression – anonymity and encryption in digital communications, https://www.ohchr.org/Documents/Issues/Opinion/Communications/PrivacyInternational.pdf*

8 *Telecommunications Surveillance and Cryptography Regulatory Policy in Africa, https://apj.hkspublications.org/telecommunications-surveillance-and-cryptography-regulatory-policy-in-africa/*

9 *Human rights, encryption and anonymity in a digital age, https://www.ohchr.org/EN/NewsEvents/Pages/HRencryptionanonymityinadigitalage.aspx*

10 *How Undermining Encryption threatens Online User Security in Africa, https://www.opennetafrica.org/how-undermining-encryption-threatens-online-user-security-in-africa/*

11 *Amnesty ibid*

2.3 **Data Localisation**

The Declaration provides under Principle 40(3) that states shall not adopt laws or other measures prohibiting or weakening encryption, including backdoors, key escrows and data localisation requirements, unless such measures are justifiable and compatible with international human rights law. Moreover, Principle 42 (4) provides that "Every person shall have the right to exercise autonomy in relation to their personal information by law and to obtain and reuse their personal information, across multiple services, by moving, copying or transferring it."

A growing number of African countries have been legislating on data localisation, which has mostly taken the form of a requirement to store data locally and forbidding unauthorised cross-border data transfers. The countries have specified the conditions for authorising transfer, mostly where the data subject has offered consent and where an adequate level of protection is assured in the recipient country or international organisation.

However, there are divergent views on data localisation across the world, creating tension between its proponents and opponents. Its proponents often cite the need to protect national security, promote the local digital economy, and safeguard users' privacy. Moreover, it has been suggested that an increasing number of African countries have been enacting data localisation laws because of unfounded fears that sending their citizens' data abroad could increase citizens' vulnerability to serious security and privacy threats from foreign actors.[12]

Opponents contend that strengthening state control over users' data "does little to address genuine grievances surrounding cybersecurity, disinformation, or the online targeting of marginalised communities by state and non-state actors."[13] Data localisation requirements have also been identified as potentially some of the most restrictive and disruptive barriers to international trade, as they often require foreign businesses to duplicate infrastructure such as data centres and computing facilities.[14] Hence, opponents view data localisation laws as posing "a significant barrier to new investment, even when these laws are driven by desires to promote local economic development."[15]

In light of the above, African countries are adopting differing approaches towards data localisation. Several countries use financial services (Nigeria, Ethiopia and Rwanda), cybersecurity and cybercrimes (Rwanda, Zambia and Zimbabwe), telecommunications (Cameroon, Rwanda and Nigeria) and data protection (Kenya, South Africa, Tunisia and Uganda) laws to place restrictions on cross-border transfer of data, with the data transfer permitted where certain conditions are met, or where authorisation is granted by the relevant government bodies.

Some countries have specified the data that cannot be exported without authorisation. Kenya specifies all public data; Nigeria mentions all government data and all subscriber and consumer data; while Zimbabwe, Malawi and Tunisia cite personal information. Zambia specifies "critical information" in the cybersecurity law with section 70(2) providing that although the minister may prescribe categories of personal data that may be stored outside the country, "sensitive personal data" is exempted and must be processed and stored in a server or data centre located in Zambia.

.....

12 *Ibid*

13 *Freedom House, User Privacy or Cyber Sovereignty? https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty*

14 *GSMA, Cross-Border Data Flows The impact of data localisation on IoT January 2021, https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf*

15 *Data Localization Laws are Making African Trade Less Free, https://weetracker.com/2019/09/20/data-localization-laws-are-making-african-trade-less-free/*

However, there is scant information on enforcement mechanisms, including whether the respective countries are indeed authorising any or all cross-border transfers of the relevant data. In the same vein, there is scanty information on regulatory sanctions against entities that breach data localisation regulations. A notable exception here is Rwanda, which in 2017 fined telecom operator MTN Rwanda for failing to locally host its data. Equally, evidence is thin on the data security practices for locally hosted data in countries with local data residency regulations, and the impact it has had on enhancing citizens' privacy rights. Notably, the growing appetite for state surveillance could be a key driver towards the adoption of data localisation laws. This is because hosting data locally could grant state surveillance apparatus in some countries easier access to data for surveillance purposes, as they would not need to go through foreign countries' or intermediaries' data management protocols to access this data.

2.4 **Establishment of Biometric Databases**

Principle 40 of the Declaration provides that "Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information." Further, Principle 42 of the Declaration requires states to adopt laws for the protection of personal information of individuals in accordance with international human rights law and standards. Further, these laws should include privacy principles,[16] provide effective remedies, and adequate oversight for the protection of personal information.

Several countries have incorporated privacy rights protection in their constitutions and most of them have enacted data protection laws that provide for the rights to privacy and the protection of personal data. The laws embed several privacy and data protection principles such as data minimisation, consent, objection to data processing by data subjects, data retention period limits, security, the notification of data subjects of the processing of their data, and provisions for remedies.

In several countries, government agencies are collecting and processing personal data without adequate data protection laws, amidst limited oversight mechanisms and inadequate remedies. While many have recently passed data protection laws and policies, implementation is not effective, and the safeguards are not water-tight as required under international human rights law.

Some laws in countries such as Chad, Kenya, Tunisia, Uganda, South Africa, and Zimbabwe, prohibit the collection of certain categories of data, including specific types of biometric data generally, or where certain conditions are not complied with.

In other countries, the laws require the mandatory collection of biometric information for the registration of telecommunications subscribers, for digital identity programmes and during voters' registration. Several laws and policies on biometric data collection contain provisions on sanctions and penalties for breach.

.....

16 *These principles in data processing should be: by the consent of the individual concerned; done in a lawful and fair manner; in accordance with the purpose for which it was collected, and adequate, relevant and not excessive; accurate and updated, and where incomplete, erased or rectified; transparent and disclose the personal information held; and confidential and kept secure at all times.*

2.5 **Weak Oversight, Transparency and Accountability Mechanisms**

The Declaration states that the independence of the oversight mechanism shall be guaranteed in law, which shall stipulate a transparent and participatory appointment process, a clear and specific term of office, adequate remuneration and resourcing, and ultimate accountability to the legislature. The study found that countries have adopted different approaches to oversight, including specifying courts, data protection authorities, sector regulators and administrative bodies as key oversight bodies.

Some of these bodies are located within the executive, and therefore may lack the proper legal, financial, and institutional independence to stem violations within government, and especially by state security agencies. The laws in most countries require judicial authorities to issue a warrant for interception or monitoring of communications. However, in some countries interception orders can be issued by non-judicial officials, such as ministers.

The Declaration recommends that notification of surveillance should be done "within a reasonable time of the conclusion of such surveillance." However, in some countries, such as Cameroon and Uganda, the interception order is not appealable, yet in Zimbabwe Section 18 of the interceptions law states that individuals aggrieved by the warrant of interception may appeal to the administrative court. The Zimbabwean law appears to suggest that the subject of monitoring would be informed of the decision authorising surveillance against them.

Most interception orders are granted ex parte to law enforcement agencies on condition that the intermediaries facilitating them keep the orders confidential. Consequently, where the laws are silent on notification or the appeal processes, renders such appellate processes meaningless, as notices are never issued to subjects of interception and thereby weakening the due process safeguard. In this regard, ordinary citizens can only rely on judicial officers to independently exercise their power to affirm and protect their rights when presented with surveillance requests. However, this is not always the case, as national security considerations when pleaded, could easily override the rights of the interception subject.

Equally worrying is that in some countries interception can be conducted without a warrant. In Nigeria section 8 of the Regulations provides grounds under which lawful interception of communication can take place without a warrant, with law enforcement officials given powers to access data from service providers without obtaining a warrant. Uganda and Rwanda, among others, provide for an oral application to a judge for an interception order, although this has to be followed within 48 hours by a written application. Meanwhile, under Ghana's electronic transactions law and Tanzania's Cybercrimes Act, law enforcement officers can seize computers and electronic equipment.

The shortage of accountability and transparency is among the weakest links in the various countries' surveillance laws. Yet there are some good examples, such as in Nigeria, where section 19 of the interceptions regulation requires agencies which order interceptions to keep a logbook of all interceptions and to submit reports to the Attorney General in the first quarter of every year. Tunisian law addresses this too, requiring investigators to keep a written record of their surveillance operations at all times. Zimbabwe's interceptions law also specifies accountability mechanisms, stating in section 19 that the Prosecutor-General shall receive an annual summary from the Minister detailing "the particulars of every warrant which, during that calendar year, was issued by him or her but not renewed." Rwanda's law requires the president to appoint inspectors to "verify that interception requests, their interception warrant and any other document related to the interception of communication comply with the Law", and the inspectors are required to submit to the Rwandan president "once a year and whenever considered necessary" a report on their work.

A similar level of accountability requirement such as is in Nigeria, Tunisia, Rwanda, Zimbabwe is lacking in most other countries' laws. Such a requirement, especially when coupled with a disclosure mechanism such as in a publicly accessible record, can be important in guarding against security agencies misusing their powers to conduct unauthorised surveillance. Moreover, while these oversight and accountability provisions are commendable, it is not known whether they are applied. No entity in any of the countries reviewed permits public access to such records, or publishes any data related to interception warrants issued and if at all they do record such data, they are categorised as classified information under state secrets laws. Thus, the public and oversight institutions such as judiciaries and parliaments remain in the dark about the extent and legality of the conduct of surveillance in the respective countries.

.

3.0 Recommendations

It is recommended that governments should:

1. Review existing laws, policies and practices on surveillance, including COVID-19 surveillance, biometric data collection, encryption and data localisation to ensure they comply with the principles in the Declaration and international human rights standards.
2. Enact standalone data protection laws in line with international human rights standards.
3. Establish and put in place administrative, legislative, budgetary, and practical measures to guarantee the full independence of data protection authorities.
4. Adopt multi-stakeholder approaches to ensure meaningful participation of all stakeholders in the development of policies and laws that affect the right to privacy and data protection.
5. Ensure any measures or programmes limiting the right to privacy are based on accessible, transparent, clear, comprehensive and non-discriminatory laws that are proportionate, fair, comply with international human rights standards, and are subject to the rule of law and impartial and independent judicial oversight.
6. Report to the African Commission on Human and Peoples' Rights on the measures taken to facilitate compliance with the provisions of the Declaration.

It is recommended that civil society actors should:

1. Advocate for the promotion and protection of the right to privacy and data protection.
2. Use strategic public interest litigation as an avenue to challenge laws that violate privacy rights and push for policies and practices reforms that uphold privacy.
3. Monitor and document privacy rights violations through evidence-based research, and report on state compliance with their obligations to human rights monitoring bodies.
4. Sensitise the general public on their rights to privacy and the need for personal data protection including through use of encryption, circumvention and anonymisation tools.
5. Create awareness on the right to privacy, highlighting ongoing violations and continuously place privacy concerns on the public agenda.
6. Investigate and expose breaches of privacy.

It is recommended that companies should:

1. Comply with the United Nations Business and Human Rights principles.
2. Implement privacy and data protection policies and best practices in their handling of customer data.
3. Engage courts and work together with policy makers and civil society stakeholders to promote privacy respecting laws and to challenge those that unjustifiably restrict privacy rights or place undue intermediary liability obligations.
4. Publish privacy policies and transparency reports and inform users about the collection, use, handling, sharing and retention of their data that may affect their right to privacy.
5. Develop technologies and solutions that embed and integrate privacy principles by design and default.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Tel: +256 414 289 502
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org