Mapping and Analysis of **Privacy Laws in Africa**

November **2021**

CIPESA

Credits

This report was produced as part of a project that is researching privacy-related laws in Africa, which is supported by Meta and the Open Society Justice Initiative. The project is setting up a portal at www.privacytracker.africa, to track privacy-related laws in all African countries, notably those that enable surveillance, limit the use of encryption, govern biometric data collection, and require data localisation.

CIPESA appreciates the support rendered by several individuals to this research. They include Asha Abinallah, Alice Aparo, Ababacar Diop, Mohamed Farahat, Tusi Fokane, Yosr Jouini, Maxwell Kadiri, Jimmy Kainja, Ashnah Kalemera, Victor Kapiyo, Paul Kimumwe, Natasha Msonza, Richard Mulonga, Daniel Mwesigwa, Nashilongo Gervasius Nakale, Asenath Niva, Jean Paul Nkurunziza, Tope Ogundipe, Dunia Mekonnen Tegegn, Simone Toussi, Dércio Tsandzana, Wairagala Wakabi, and Edrine Wanyama.

Mapping and Analysis of Privacy Laws in Africa
Published by CIPESA
www.cipesa.org
November 2021

Table of Contents

1 Introduction

Privacy in the digital age has become a preeminent human rights issue, given its intricate connection with, and its being a foundation for realising other rights such as to human dignity and 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 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 or failed to take adequate measures to promote and protect the 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 limit the use of encryption. As a result, increased state surveillance across the continent is accelerating interference with various rights and freedoms. Moreover, surveillance is increasingly being used to entrench political control including through spying on activists, journalists, and dissidents.[1] 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 prohibitions on encryption services undermine citizens' right to communicate anonymously- 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.[2]

In addition, the advent of the COVID-19 pandemic has exacerbated the privacy concerns in several countries where 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.

It is therefore crucial to map and analyse the laws and policies that impact on privacy, notably those that regulate surveillance, limitations on encryption, data localisation, and biometric databases. This analysis can inform remedial and mitigatory steps to protect the right to privacy, which may include strategic litigation 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 *State of Internet Freedom in Africa 2019: Mapping Trends in Government Internet Controls, 1999-2019, https://cipesa.org/fifafrica/wp-content/uploads/2016/05/Collaboration-on-International-ICT-Policy-for-East-and-Southern-Africa-SIFA-19.pdf*

2 *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 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 and censorship on digital platforms. The study covers 19 countries - Cameroon, Chad, Egypt, Ethiopia, Ghana, Kenya, Malawi, Mali, Mozambique, Namibia, Nigeria, Rwanda, Senegal, South Africa, Tanzania, Tunisia, Uganda, Zambia, and Zimbabwe.

In assessing the various laws and policies, the study referenced the recently revised Declaration of Principles of Freedom of Expression and Access to Information in Africa[3] (the Declaration) of the African Commission on Human and Peoples' Rights (ACHPR). The Declaration sets common benchmarks by expounding on the obligations of Member States with respect to article 9 of the African Charter which African countries should comply with to protect and promote citizens' digital rights.

Using a recognised and standardised continental Declaration as the frame for the analysis makes the results 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, with principles 40 to 42 dealing with the right to privacy in particular.

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

2 Policy and Legal Framework

This section presents an analysis of laws and policies relevant to surveillance, data localisation, biometric databases, and limitations on encryption. It details the safeguards and retrogressive provisions of the different laws and policies, the relevant sanctions and penalties, oversight, and redress mechanisms.

International human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR) provide for the right to privacy in their articles 17 and 12 respectively. At the regional level, while the African Charter on Human and Peoples' Rights (African Charter) has no specific provision on the right to privacy, article 9 has been interpreted to encompass the right to privacy through the Declaration. In addition to expressly recognising the right to privacy, States are also required to adopt legislative, administrative and other measures to give effect to this right and to report to the ACHPR on their compliance with the Declaration as part of periodic reporting.

Further, the African Union Convention on Cybersecurity and Personal Data Protection, which is the continent's model instrument on privacy and data protection, provides safeguards for personal privacy and data protection. However, it is yet to come into force as the minimum threshold of 15 ratifications by states is yet to be attained, with only eight states having ratified the convention.[4]

Notably, the only regional treaty in force that deals with the right to privacy is the African Charter on the Rights and Welfare of the Child, which provides in article 10 that:

> ***"No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks."***

Also, only about half of African countries have adopted laws to protect personal data.[5] Even then, in many countries, the laws are yet to be fully operationalised through the adoption of implementing regulations.

4 *African Union Convention on Cybersecurity and Personal Data Protection, "Status List" as at 28th April, 2021,*

5 *https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf*
2020 is a crucial year to fight for data protection in Africa, https://privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa

2.1 Surveillance

While the increased use of digital technologies has made the right to privacy more critical, violations of the right by state and non-state actors are equally on the rise. In recent years, African countries, including those focused on in this research, have enacted laws and policies to regulate the right to privacy. Many of the laws enacted do not measure up to international human rights standards and fail to establish clear and appropriate oversight, redress and remedy mechanisms.

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, the Declaration requires states to ensure that any law authorising targeted communication surveillance provides adequate safeguards for the right to privacy, including 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 include 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.

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. They also embed several privacy and data protection provisions 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.

However, as the present research found, laws in various countries criminalise illegal surveillance and place various safeguards on the conduct of state surveillance. However, many of them contain retrogressive provisions that undermine citizens' enjoyment of the right to privacy, as they leave scope for intrusion, including enabling state surveillance with limited safeguards. Also, the laws provide for sanctions and penalties for illegal surveillance and include punitive sanctions against service providers that do not offer interception assistance to government agencies or where service providers fail to comply with court warrants and orders to assist governments in conducting surveillance.

Below, we explore the legal provisions on surveillance in various countries. It should be noted that in many countries, there is no evidence that the laws have been utilised in undermining the right to privacy though surveillance. Even where there is evidence of surveillance being conducted, or other breaches of digital rights, authorities do not always state the laws that inform their actions.

Cameroon

Section V, articles 49 to 51 of the Law N° 2010/012 of 21 December 2010 on Cybersecurity and Cybercrime[6] empowers criminal investigation officers to intercept, record, or transcribe any electronic communication. If the intermediaries have encoded or encrypted the data transmitted, they are required to decrypt the communications before disclosure to the police. Under article 25 of the law, intermediaries have an obligation to retain connection and traffic data for 10 years, and to install mechanisms for monitoring traffic data on their networks, which may be accessed in the course of judicial inquiries.

6 *Law n°2010/012 of 21 December 2010 on Cybersecurity and Cybercrime, https://bit.ly/3rARtEJ*

Article 42 obliges operators of electronic communications and information networks to ensure the confidentiality of information, including traffic data channelled through their systems, while article 43 holds operators liable for privacy infringement or invasion. Moreover, article 44 prohibits any person from listening, intercepting or storing communication and traffic data, or subjecting them to any means of interception or monitoring without the consent of the concerned users, save for where the interception is legally authorised.

This law was used by the Civil Cabinet of Cameroon's Presidency to instruct the National Agency for Information and Communication (ANTIC) to communicate all measures implemented to combat identity theft and the dissemination of fake news on social networks.[7] Citing articles 41, 42 and 78 of the law on cybercrimes, the Director of ANTIC announced that, of the 4,242 accounts which had been identified and reported (purportedly to Facebook) as fake, 3,372 accounts had been deleted as of 2020.[8] The Cameroon government also has a history of ordering internet shutdowns and the suspension of social media services such as Twitter to "protect the security of the nation".[9] Some individuals have also reported that they were under surveillance but there was no proof of this.[10] Nonetheless, in 2014 the Director of ANTIC affirmed that the institution uses "cutting-edge tools" to operate a permanent watch on social networks and possibly "block access to a website", in line with the provisions of articles 77 and 78 of the Cybersecurity and Cybercrime law.[11]

Article 92 of the 2007 Code of Criminal Procedure permits judicial police officers to intercept, record or transcribe any correspondence sent by telecommunication in the event of a crime punishable by imprisonment of at least two years.[12] According to article 244, the examining magistrate may order the interception, recording and transcription of correspondence transmitted using telecommunications. Per article 245(4), the interception warrant which is not subject to appeal, must be in writing, identify all the elements to intercept, state the offence that motivates the interception, and is valid for a maximum of four months.

The penalty for illegal surveillance is imprisonment for a period of one to two years and a fine of between one million and five million Central African (CFA) francs (USD 1,845-9,226). Article 74(1-2) of the 2010 cybersecurity law states that "anyone who, by any means whatsoever, invades the privacy of others by fixing, recording or transmitting, without the consent of their authors, electronic data of a private or confidential nature shall be punished with imprisonment of between one to two years and a fine of between one million to five million CFA francs." The same penalty applies to anyone who "intercepts personal data when it is transmitted from one information system to another."

Article 80 of Act N° 2010/013 of December 21, 2010 on Electronic Communications in Cameroon[13] punishes participation in an act that violates the secrecy of correspondence or disclosure, publication or use of the content without the authorisation of the sender or recipient. The penalty is imprisonment for a period of six months to two years, a fine of between one million and five million CFA francs (USD 1,845-9,226) or both.[14]

7 *Creation, Sharing of Fake News is a Crime Punishable by Law, https://bit.ly/3tniyN8*
8 *Cybersecurity: ANTIC claims it deleted 3,372 fake Facebook accounts out of 4,242 identified in 2020, https://bit.ly/3iizSQv*
9 *Cameroon Bans Mobile Version of Twitter, https://bit.ly/3yocYwv*
10 *Cameroon - May 20, 2014 - Interview with Woungly Massaga, Cameroonian politician and nationalist: "Cameroon is a real time bomb" (Fr.), https://bit.ly/3A4xX8e*
11 *Dr EBOT EBOT Enaw: "In Cameroon, there are no legal provisions authorizing the blocking of a website"; https://bit.ly/2Vp39Qv*
12 *Journal Officiel de la République du Cameroun; portant Code de Procédure Pénale N°2005/007 27 Juillet 2005, https://bit.ly/3r07gMG*
13 *Act N° 2010/013 of December 21, 2010 on Electronic Communications in Cameroon (in French); https://bit.ly/2PmdCZD*
14 *Law No. 2015/006 amending and supplementing certain provisions of the 2010 Act on Electronic Communications in Cameroon; https://bit.ly/3cabOMj*

Chad

In Chad, article 43 of the Law No. 009 of 2015 on Cybersecurity and Cybercrime forbids "any natural or legal person to listen to, intercept, store communications and related traffic data, or submit them to any other means of interception or surveillance, without consent of the affected users, except where that person is legally authorised to do so."[15] However, article 27 of the same law provides that judicial police officers and authorised agents of the National Agency for Computer Security and eCertification (ANSICE) may use appropriate technical means to collect or record in real time, data relating to the content of electronic communications. Article 31 of the law also permits the remote installation of software on a computer system to collect evidence.

Under article 61 of the same law, intermediaries have an obligation to retain connection and traffic data for 10 years, to install surveillance mechanisms for the data traffic of their networks and are responsible if the use of this data infringes the individual freedoms of users. Moreover, article 51 of the law requires communications service providers to retain data that enables the identification of any person who contributed to content creation in services they provide, for 10 years.

Egypt

Article 2 of Anti-Cyber and Information Technology Crimes Law No. 175/2018 requires internet service providers to retain customer usage data for 180 days, including data that enables user identification.[16] Article 6 of the same law authorises the investigation authority to issue a decision that allows surveillance and access to information.

Moreover, article 46 of the anti-terrorism law No. 94 of 2015 empowers the public prosecutor or "any investigation authority" in terrorist crimes, to order surveillance and recording of conversations and messages taking place in private places or through websites for a period of not more than 30 days. Sub-article 2 adds that the order of surveillance is renewable for one or more similar periods (30 days). In addition, article 3(2) of Emergency Law No. 162 of 1958 stipulates that the president has the power to order surveillance of all messages whatever their type. Finally, article 64(2) of communication regulation law No. 10 of 2003 requires service providers to collect accurate information and data about their users.

Egypt has conducted widespread internet surveillance since the days of the Hosni Mubarak regime, as it battled to close civic space and track members of dissident groups. The country has used COVID-19 contact tracking applications, arrested some individuals over circulating fake news about COVID-19 and detained some TikTok users under article 25 of the cybercrime law which criminalises the breach of the principles and values of Egyptian families. The arrests and detentions were an indication of surveillance of social media activity.

Ethiopia

Article 606 of the Criminal Code prohibits the unauthorised access to private communications including letters, telegrams, telecoms, which is punishable with up to six months of imprisonment or a fine. Article 399 of the Criminal Code criminalises breaches of professional secrecy, while article 422 criminalises abuse of the right of search or seizure, punishable with imprisonment not exceeding seven years.

Moreover, the Communications Service Proclamation in article 50 authorises the Ethiopian Communication Authority to approve information security, data privacy, and protection matters. Moreover, the Computer Crimes Proclamation No. 958/2016 permits search and seizure without warrants, and, under article 23, requires service providers to retain all computer data passing through their systems for at least one year, which they must disclose on the order of a court or a public prosecutor.

15 *Chad; Law No. 009/PR/2015 on Cybersecurity and Cybercrime, https://bit.ly/3lhYlXY*

16 *Anti-Cyber and Information Technology Crimes No. 175/2018, https://manshurat.org/node/31487*

However, article 25(1) of the Computer Crime Proclamation provides that warrants for interception are to be issued by court following an application by an investigatory organ. Nonetheless, article 25(3) provides that the Attorney General may permit the investigatory organ to conduct interception or surveillance without a court warrant "where there are reasonable grounds and urgent cases to believe that a computer crime that can damage critical infrastructure" is about to be committed.[17] In such circumstances, however, the Attorney General is required, under article 25(4), to present the reasons for interception or surveillance without a court warrant to the President of the Federal High Court within 48 hours, "and the president shall give [the] appropriate order immediately."

Under article 3 of the Computer Crime Proclamation, "Whosoever, without authorisation or in excess of authorisation, intentionally secures access to the whole or part of a computer system, computer data, or network shall be punishable with simple imprisonment not exceeding three years or fine from Ethiopian Birr (ETB) 30,000 to 50,000 (USD 675 to 1,125) or both." If the crime is committed against "a computer system, computer data or network that is exclusively destined for use by a legal person" it is punishable with imprisonment of between three to five years, a fine of ETB 30,000 to ETB 50,000 (USD 675 to 1,225) or both, and if on critical infrastructure, it is punishable with up to ten years' imprisonment, a fine of ETB 100,000 (USD 2,251), or both.

Kenya

Under section 51(c) of Kenya's Private Security Regulations Act, 2016 private security firms are prohibited from using and installing equipment that are capable of intercepting and interfering with other individuals' communication.[18] Further, the Computer Misuse and Cybercrimes Act, 2018,[19] the Prevention of Terrorism Act, 2015, and the National Intelligence Service Act, 2012,[20] require that a warrant for interception must be obtained from court prior to authorities undertaking surveillance. The National Intelligence Service Act, 2012 is specific that such warrants can only be obtained from the High Court, while under the other laws the warrant may also be obtained from lower courts such as Magistrates Courts.

Section 42 of the National Intelligence Service Act permits the Director General of the National Intelligence Service to apply in writing for a warrant ex parte before a judge of the High Court, for the purpose of investigating any threat to national security or to perform any of its functions.[21] Warrants can be issued for a period that does not exceed one month, and may be renewed for a similar period at a time provided the court is satisfied with the grounds adduced.

Likewise, section 36 of Kenya's Prevention of Terrorism Act, 2012 grants police officers above the rank of Chief Inspector of Police, with the consent of the Director of Public Prosecutions, to apply ex parte to a Chief Magistrate or the High Court for an interception of communication order.[22] Further, the Computer Misuse and Cybercrimes Act, 2018 permits a police officer to apply to a court to: enter any premises to access, search and similarly seize computer data (section 48); require a specific person to submit computer data that is in their control (section 50); require a service provider to submit subscriber information in its possession or control (section 50); expedite the preservation or partial disclosure of traffic data (section 51); permit the real-time collection of traffic data (section 52); and intercept content data through the application of technical means, including by compelling a service provider to collect the information or assist in its collection (section 53).

Rule 15 of the Kenya Information and Communications (Consumer Protection Regulations), 2010 prohibits licensees of telecommunications services from monitoring, disclosing or allowing any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data.[23]

17 *Computer Crime Proclamation No. 958/2016 (2016), https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/103967/126636/F1922468791/ETH103967.pdf*
18 *Private Security Regulation Act, No. 13 of 2016, http://www.kara.or.ke/Private%20Security%20Regulation%20Act%2013%20of%202016.pdf*
19 *Computer Misuse and Cybercrimes Act, 2018 http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf*
20 *National Intelligence Service Act, 2012, https://www.nis.go.ke/downloads/THE%20NATIONAL%20INTELLIGENCE%20SERVICE%20ACT,%202012.pdf*
21 *National Intelligence Service Act, https://www.nis.go.ke/downloads/THE%20NATIONAL%20INTELLIGENCE%20SERVICE%20ACT,%202012.pdf*
22 *Prevention of Terrorism Act, 2012, https://www.probation.go.ke/resource-center/category/9-statutes.html?download=12:pota*
23 *Kenya Information and Communications (Consumer Protection Regulations), 2010, https://ca.go.ke/wp-content/uploads/2018/02/Consumer-Protection-Regulations-2010.pdf*

The Prevention of Terrorism Act and the Computer Misuse and Cybercrimes Act, 2018 grants power to police officers to intercept communications, and to conduct search and seizures of computer data and intercept content data, respectively. However, both laws as compared to the National Intelligence Service Act, 2012 provide fewer safeguards for privacy protection. These include lower thresholds that a court needs to be satisfied with, and fewer requirements for the police to provide, such as adequate reasons, clear purpose, specific time, scope, and the justifications sought for the use of surveillance. Also, section 36A of the Prevention of Terrorism Act grants National Security Organs general power to intercept communication for the purposes of detecting, deterring, and disrupting terrorism in accordance with procedures yet to be prescribed by the Cabinet Secretary.

In 2019, the government published a draft National Closed Circuit Television (CCTV) Policy to "guide installation, operation and management of all CCTV systems in public and private premises while promoting their use as a mechanism to deter, detect and prevent crime for a safe and secure nation."[24] The Policy requires all institutions, businesses, and facilities with public areas to ensure that those areas are covered by CCTV Systems, and provide reasonable access, connection, linkage and integration mechanisms to security agencies; and report all security related incidents captured by CCTV systems to the relevant security authorities. The Policy, which is yet to come into force, has been widely criticised for threatening the rights to privacy, freedom of expression and association.[25]

Kenya has stringent penalties for unauthorised surveillance and interception of communication. For example, section 36(6) of the Prevention of Terrorism Act provides that a police officer who intercepts communication other than as provided for under the Act shall on conviction be liable to imprisonment for a term of up to 10 years or to a fine of up to five million shillings (USD 46,315), or both. Also, under section 52(b) of the National Intelligence Service Act, a member of the service who conducts unauthorised search and seizure, is liable to a similar penalty. Moreover, by section 31 of the Kenya Information and Communications Act, 2009, telecommunication operators are prohibited from intercepting messages or disclosing to any person the contents of an intercepted message. Upon conviction, the offence attracts a fine not exceeding KShs three hundred thousand shillings (USD 2,808) or, to imprisonment for a term not exceeding three years, or to both.

Mali

Articles 74 to 78 of the Law No. 2019-056 of 5 December 2019 on the Suppression of Cybercrime permit the search of computers and the seizure of data by security operatives as part of criminal investigations. In addition, article 83 authorises judicial authorities to use appropriate technical means to collect or record, in real time, traffic data associated with specific communications, transmitted by means of an information system.

Further, articles 83 to 86 suggest real-time surveillance through interception of communications. Service providers are required to cooperate with the public prosecutor or the examining magistrate, including by ensuring that they have the necessary technical means to facilitate interception of communications. These broad powers double up as an addition to those given to authorities under article 4 of the Telecommunications Act. This article 4 states that: "When public security or the defence of the territory of Mali so requires, the Government may, for a limited period, requisition all the telecommunications networks established in the territory of Mali, as well as the equipment connected to it and / or prohibit the provision of telecommunications service."

Furthermore, communications service providers are required under article 25 of the cybercrime law to put in place mechanisms to monitor systems for potential illegal activity. The failure to inform "competent public authorities" of illegal activities is punishable by a prison sentence of between six months and two years, a fine of 500,000 to two million CFA francs (USD 830 to 3,318), or both.[26]

24 *Draft National CCTV Policy, https://www.interior.go.ke/wp-content/uploads/2019/07/CCTV-POLICY-DRAFT-TWO-14-02-2019.pdf*

25 *Kenya: Desist from indiscriminate and invasive mass surveillance, https://www.amnestykenya.org/kenya-desist-from-indiscriminate-and-invasive-mass-surveillance/; Unseen Eyes, Unheard Stories Surveillance, data protection, and freedom of expression in Kenya and Uganda during COVID-19, https://www.article19.org/wp-content/uploads/2021/04/EAF-Surveillance-Report_Final-min.pdf; A Commentary on Kenya's Draft National CCTV Policy https://cipit.strathmore.edu/a-commentary-on-kenyas-draft-national-cctv-policy/*

26 *New Mali Cybercrime Law Potentially Problematic to Digital Rights, https://cipesa.org/2020/02/new-mali-cybercrime-law-potentially-problematic-to-digital-rights/*

The Malian legal framework contains some progressive provisions that criminalise unlawful interception of communication of surveillance. For example, telecom service providers who, without the authorisation of the sender or recipient, disclose, publish or use subscribers' communications, face imprisonment of six months to three years or a fine of 25,000 to 300,000 CFA francs (USD 46-550), or both. A person who, without authorisation, invades another person's privacy by listening, recording or transmitting their communications faces similar penalties to telecom service providers above.[27] Further, article 50 of the Criminal Code punishes with life imprisonment those who, while participating in an insurrectional movement, break or attempt to break telephone lines, intercept or attempt to intercept communications between members of the security forces.

Article 8 of the Law n° 2019-056 of 05 December 2019 on the Suppression of Cybercrime[28] punishes "anyone who intercepts or attempts to fraudulently intercept computerised data during their non-public transmission to, from or within an information system, by imprisonment of three months to three years or a fine of 200,000 to 50,000,000 CFA francs (USD 362-90,432) or both penalties." Article 43 of the law punishes by imprisonment of between two and five years, a fine of two million to 30 million CFA francs (USD 3,618-54,262) or both penalties, "anyone who sets up a stolen access to data or an information system without the authorisation of the legitimate user." Further, under article 26, telecommunications service providers who fail to retain data allowing the identification of their subscribers can be imprisoned for between six months and two years, fined 500,000 to two million CFA francs (USD 362-3,618), or face both penalties. Meanwhile, the law on identification of users of telecom services provides for mandatory SIM card registration, and in article 6 requires cybercafé managers to maintain a register of users indicating their names, workstations used, the day, the hour and the duration of use.

Namibia

Article 73 of the Communications Act 8 of 2009[29] requires telecommunications service providers to obtain subscriber information that "must be sufficient to determine which telephone number or other identification has been issued to a specific customer in order to make it possible to intercept the telecommunications of that customer." The offence of unauthorised interception attracts a fine of Namibian dollars (N$) 20,000 (USD 1,343), imprisonment for a period of five years, or both.

Part 6 of the 2009 Communications Act provides for the interception of communications by establishing an interception centre for the purposes of combating crime and national security. Article 70(8) reads: "Where any law authorises any person or institution to intercept or monitor electronic communications or to perform similar activities, that person or institution may forward a request together with any warrant that may be required under the law in question to the head of an interception centre." The Act further empowers staff members of the interception centre to "do anything necessary in order to perform the interception or monitoring concerned (as well as any decoding or decryption necessary to make the information in question intelligible)."[30] Civil society and the media believe that the state, particularly the Central Intelligence Service, is highly engaged in arbitrary interception and surveillance of citizens, in disregard of their privacy rights.

Nigeria

Regulation 7 of the Lawful Interception of Communications Regulations 2019 made pursuant to the Nigerian Communications Act 2003 requires a warrant from a judge of the Federal High Court for the interception of communication.[31] Furthermore, Regulation 19 offers a system of accountability where authorised agencies must keep logbooks of all interceptions carried out and submit annual reports on concluded interception cases to the Attorney General in the first quarter of every year.

27 *Law n° 2001-79 of August 20, 2001 on the Penal Code; Amended by law n ° 2005-45 of August 18, 2005, law n ° 2016-39 of July 7, 2016; Article 125.*

28 *Law n°2019-056 of 05 December 2019 on the Suppression of Cybercrime, https://tinyurl.com/34fxc9zy*

29 *Communications Act 8 of 2009, https://laws.parliament.na/cms_documents/communications-86425fd24c.pdf*

30 *Digital Rights in Namibia, https://cipesa.org/?wpfb_dl=436*

31 *Lawful Interception of Communications Regulations 2019, https://www.ncc.gov.ng/accessible/documents/839-lawful-interception-of-comunications-regulations-1/file*

Meanwhile, section 39 of the Cybercrime Act (Prohibition, Prevention, etc) Act 2015 empowers a judge to order service providers or authorise a law enforcement officer to collect data or intercept communications "where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings."[32]

In enacting the various privacy-related laws, the government has appeared to pay less regard to the respect for human rights as it prioritises the fight against terrorism, preservation of national security and public order. Section 29 of the Terrorism (Prevention) Act, 2011 permits law enforcement agencies — with the approval of the Attorney General and the Coordinator of National Security — to apply to a judge for an "interception of communication order" for the purpose of preventing a terrorist act or prosecuting offenders under the Act. In addition, section 38 of the Cybercrime Act (Prohibition, Prevention, etc) Act 2015[33] empowers authorised law enforcement officials to request for the release of any information from service providers without warrants in respect of subsection (2)(b)[34] of the Act, and a service provider is bound to comply.

Moreover, regulation 4 of the Lawful Interception of Communications Regulations 2019[35] empowers government agencies such as the Office of the National Security Adviser or the Director of State Security Services[36] to intercept communications through communications licensees. Regulation 8 further provides conditions where interception of communications can be carried out without a warrant. Such interception shall be lawful where: one of the parties to the communication has consented to the interception, provided that an incontrovertible proof of such consent is available; it is done by a person who is a party to the communication, and has sufficient reason to believe that there is a threat to human life and safety; and in the ordinary course of business, it is required to record or monitor such communication.

Additionally, under the 2013 Nigerian Communications Commission (NCC) Guidelines for the Provision of Internet Services, Internet Service Providers are required to comply with and provide any service-related information requested by the Commission or other legal authority, including information regarding particular users and the content of their communications, subject to any other applicable laws of Nigeria.[37]

Additionally, the Lawful Interception of Communications Regulations 2019, state under regulation 16(1) that any person, licensee or its officers that fail to comply with the provisions of the law is liable to a fine of Nigerian Naira (₦) five million (USD 12,273). Where the offence continues, a daily default penalty of ₦ 500,000 (USD 1,228) is applied. Moreover, under regulation 16(2), the NCC may revoke the licence of the service provider for failure to comply with the regulations.

Rwanda

Law n° 60/2013 of 22/08/2013 regulating communications interception provides in article 3 that interception of communications shall be considered lawful where it is done in the interest of national security and in accordance with this law.[38] Article 7 requires communication service providers to ensure that their systems are technically capable of supporting interceptions at all times. This is reinforced in article 123 of the Law n° 24/2016 of 18/06/2016 governing information and communication technologies (ICT), which states that, notwithstanding the provisions of Rwanda's constitution, electronic communications network or service providers must equip their networks and services with technical equipment and features that allow and facilitate lawful interception and monitoring.[39]

32 *Cybercrime Act 2015, https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf*

33 *Cybercrime Act 2015, https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf*

34 *Section 38(2)(b) states that "a service provider shall, at the request of the relevant authority (for the time being, responsible for the regulation of communication services in Nigeria)*

35 *of this section or any law enforcement agency – (b) release any information required to be kept under subsection (1) of this section.*
Lawful Interception of Communications Regulations 2019, https://www.ncc.gov.ng/accessible/documents/839-lawful-interception-of-comunications-regulations-1/file

36 *Regulation 12(1) of the Lawful Interception of Communications Regulations, 2019,*

37 *Regulation 6(c) of the Guidelines, https://tinyurl.com/s87q5s8*

38 *Rwanda Government Gazette, https://gazettes.africa/gazettes/rw-government-gazette-dated-2013-10-14-no-41*

39 *See the Law governing ICT here: https://tinyurl.com/4dvks3xs*

According to article 127 of the law governing ICT, on the request of the Minister or the Regulatory Authority, "an electronic communications service provider shall, irrespective of professional secrecy, collect and provide to the Minister and the regulatory authority any information sought for the guidance and supervision of activity relating to the ICT."

Uncommon to other countries' interceptions laws, article 127 of Rwanda's law governing ICT provides that "the licensed electronic communications service provider has the right to request for reasons behind the information so required." Rwanda also has an extensive list of crimes listed under "the interest of national security" for which an interception warrant may be issued. They include murder, armed robbery, drug trafficking, human trafficking, corruption and other related offences, treason or espionage, terrorism, genocide ideology and other related offenses, tax evasion, and "other felonies".

A head of a security organ is required to apply in writing for a warrant from the National Prosecutor. Per the Prime Minister's order n° 90/03 of 11/09/2014 determining modalities for the enforcement of the law regulating interception of communication, an interception warrant is valid for three months and is renewable only once (article 7) but the period of renewal is not stated.[40] Further, according to article 9 of the 2013 interceptions law, where there are urgent public security interests, the National Prosecutor may grant a verbal interception request valid for up to 24 hours.

Moreover, article 10 of the same law provides that an authorised person can request an interception warrant without recourse to a communication service provider where the equipment used for interception does not need recourse to a communication service provider. Such equipment is governed by the law relating to arms, and the Rwandan president determines the organ in charge of managing such equipment. Article 14 of the Prime Minister's order states that the head of this organ shall determine the format to be filled by the head of the authorised security organ before carrying out interception.

Article 12 of the 2013 law provides that the president "shall appoint inspectors in charge of monitoring authorised persons to ensure that they intercept communication in accordance with the Law." In the Prime Minister's Order of 2014, the Inspectors "shall verify that interception requests, their interception warrant and any other document related to the interception of communication comply with the Law" (article 11). Under article 12, the Inspectors shall submit a report on their work to the Rwandan president "once a year and whenever considered necessary".

Senegal

The law n° 2016-33 of December 14 2016 relating to Intelligence Services provides in article 10 that in the interest of national security, intelligence authorities can "use technical, intrusive, surveillance or location procedures to collect information useful for neutralising a threat''. Article 11 requires service providers to cooperate with and assist unspecified "relevant private bodies" with intelligence activities. Further, Act No. 2016-30 amending Act No. 65-61 of 1965 on the Code of Criminal Procedure[41] requires in article 90-11 the cooperation of intermediaries with investigative authorities in collecting or recording "in real time" relevant electronic data and communications. Article 90-14 provides that a public prosecutor must issue to telecommunications operators and service providers a formal request for cooperation. Recording and interception of communications under the criminal code are subject to the written authorisation by a judge.

Meanwhile, article 90-17 empowers judges to order intermediaries to decrypt data or provide information on the operation of encrypted systems. Orders are not subject to appeal and their validity is restricted to between two and four months and are renewable on a case-by-case basis. The lack of provisions in the laws enabling individuals subject to surveillance to challenge court orders is against the provisions of the Budapest Convention - which Senegal is Party to - and the Africa Declaration, which aims to ensure an appropriate balance between the interests of law enforcement and respect for fundamental human rights.

40 See the order here: https://tinyurl.com/4ffb9vwp

41 Act No. 2016-30 amending Act No. 65-61 of 1965 on the Code of Criminal Procedure, http://www.jo.gouv.sn/spip.php?article11002

Article 20 of the eCommunications Code re-emphasises the requirement for service providers to cooperate with government authorities in accordance with the provisions of Article 90-11 of the Code of Criminal Procedure, including through disclosing relevant information and offering technical assistance when asked. Under article 36 of Senegal's Electronic Communications Act, service providers are obliged to identify users at the time of subscribing to their services and to retain data that would allow their identification.

Senegal's Data Protection Bill of 2019 under clause 121 introduces the regulation of video surveillance, with a requirement for a visible notification of the presence of the surveillance system, a receipt reference issued by the Authority, and contact details of the person or service responsible for the "rights of access, opposition and deletion" of content from the video system. Other than for purposes of safety of property and people, the installation of video surveillance for "systematic, deliberate and permanent monitoring" at places of work as defined in the Labour Code is outlawed under clause 120.[42]

South Africa

In South Africa, section 16(5) of the Regulation of Interception of Communications and Provision of Communications-related Information Act (RICA) of 2002 provides that "interception directions" should be authorised by a designated judge to prevent the commission of a serious offence, gather information related to the public health or safety or national security of the country, assist in cross-border crime prevention as a result of a bilateral agreement or international obligations. An interception direction is limited to three months and must be in writing.[43]

In February 2021, the Constitutional Court declared various provisions of the RICA unconstitutional.[44] Specifically, the court stated that RICA failed to: provide for safeguards to ensure that the designated judge[45] is independent; provide for notification of the subject of surveillance of the fact of their surveillance as soon as the notification could be given without jeopardising the purpose of surveillance after surveillance has been terminated; and adequately provide safeguards to address the fact that interception directions are sought and obtained ex parte. Further, the court found that the RICA failed to adequately prescribe procedures to ensure that data obtained pursuant to the interception of communications was managed lawfully and not used or interfered with unlawfully, including prescribing procedures to be followed for examining, copying, sharing, sorting through, using or destroying the data; and failed to provide adequate safeguards where the subject of surveillance is a practicing lawyer or journalist.

However, the court suspended the application of its declaration on the law's unconstitutionality for 36 months to enable Parliament enact legislation to address the gaps in RICA. Also, during the period of suspension, the court ordered that RICA be deemed to include a new section, 23A, which requires the disclosure to courts of warrants relating to journalists or practicing lawyers; and a new section, 25A, which requires the notification of a person who was the subject of surveillance within 90 days of the expiry of the warrant. Further, the Court held that bulk surveillance activities and foreign signals interception undertaken by the National Communications Centre were unlawful and invalid as there was no law that authorised them.

While RICA is the primary legislation governing telecommunications surveillance, the Criminal Procedure Act, 1977 (CPA) is also relevant. In May 2017, an investigation by the Daily Maverick revealed that law enforcement agents frequently used section 205 of the CPA to access call data records in several cases, pursuant to section 15 of RICA.[46] According to section 205, law enforcement officials can apply to a high court, regional court, or magistrates court for an order to obtain the records.[47]

42 *Senegal to Review Data Protection Law, https://cipesa.org/2020/01/senegal-to-review-data-protection-law/*

43 *Regulation of Interception of Communications and Provision of Communications-related information Act No 70 of 2002, https://www.gov.za/sites/default/files/gcis_document/201409/a70-02.pdf*

44 *amaBhungane Centre for Investigative Journalism and Another v the Minister of Justice and Others 2021 ZACC 3, http://www.saflii.org/za/cases/ZACC/2021/3.html*

45 *Means any Judge of a High Court discharged from active service under section 3(2) of the Judges' Remuneration and Conditions of Employment Act [47 of 2001], or any retired Judge, who is designated by the Minister to perform the functions of a designated Judge for purposes of RICA*

46 *Privacy International, State of privacy in South Africa, https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa*

47 *Criminal Procedure Act, 1977, https://www.justice.gov.za/legislation/acts/1977-051.pdf*

Ordinarily, the Protection of Personal Information Act 4 of 2013 (POPIA) – South Africa's comprehensive data protection framework – does not apply to the processing of personal information by or on behalf of a public body which involves national security, to the extent that adequate safeguards have been established in legislation to protect such personal information. However, for the purposes of surveillance in respect of the COVID-19 pandemic, the regulations published in terms of the Disaster Management Act 57 of 2002 are relevant.[48]

Furthermore, guideline 5.1 of the Guidance Note on the Processing of Personal Information in the Management and Containment of COVID-19 Pandemic, published by the Information Regulator in terms of POPIA,[49] allows for contemplating the permissibility of electronic communication service providers to provide the government with mobile location-based data of individuals. Guideline 5.2 of the guidance note provides that electronic communication service providers "can provide the government with location-based data of data subjects and the government can use such personal information for the purpose of conducting mass surveillance of data subjects if the personal information is anonymised or de-identified in a way that prevents its reconstruction in an intelligible form." The Guidance Note makes clear that the provisions of POPIA must be complied with in respect of these activities.

The RICA provides for various penalties for natural and juristic persons convicted of offences under the Act. For natural persons, the penalty is a fine not exceeding South Africa Rand (ZAR) two million (USD 139,188) or imprisonment for a period of up to 10 years. For juristic persons, the penalty is a fine not exceeding ZAR five million (USD 344,657).[50] Telecommunications service providers that fail to comply with RICA may also have their licenses revoked.[51]

Tanzania

Tanzania's Cybercrimes Act, 2015 criminalises unlawful access to computer systems (section 4) and illegal interception of communication (section 6). Further, the Electronic and Postal Communications Act of 2010, in section 121(1) prohibits the disclosure of authorised intercepted communications to third parties. Meanwhile, sections 31(3)(b)(i) and (ii) of the Prevention of Terrorism Act, 2002 provides certain degrees of responsibility to courts in determining the reasonableness of the application for interception orders. The Tanzania Intelligence and Security Services Act, 1984 establishes the Tanzania Intelligence and Security Services (TISS), which under section 5(2) can intercept personal communications for national security reasons.

The Cybercrimes Act, 2015 specifically sections 39, 40, 41, 42, 43, 44 and 45, states that operators and service providers are not required to monitor communications and services they render or disclose to third parties. Additionally, operators and service providers are not liable for any illegal activities by third parties over which they have no control.

Section 31 of the Act empowers a police officer in charge of a station to search and seize or authorise the search and seizure of communication devices or data for investigatory purposes. This may be done where the officer is satisfied that there are reasonable grounds to suspect or believe that a computer system may be used as evidence in proving an offence or is acquired by any person as a result of an offence. In such an instance, the officer may authorise a law enforcement officer to: enter into any premise and search or seize a device or computer system; secure the computer data accessed; or extend the search or similar accessing to another system where a law enforcement officer conducting a search has grounds to believe that the data sought is stored in another computer system or part of it.

48 *COVID-19 Regulations, http://www.saflii.org/content/covid-saflii-0*

49 *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*

50 *Section 51 of the RICA, 2002*

51 *Section 56*

In addition, Regulation 13(1)(d) of Electronic and Postal Communications (Online Content) Regulations, 2020 (commonly known as EPOCA) obligates internet café service providers to install surveillance cameras inside their cafés to monitor users' activities. The same provision requires registration of all users of internet cafés, who are required to produce an ID. Rule 120 of EPOCA penalises unlawful interception and disclosure of intercepted communications, with a fine of Tanzania Shillings (TZS) five million (USD 2,156), or one year in jail, or both.

Tunisia

Tunisia first introduced a data protection law in 2000 that created a data protection office. Yet, despite being a pioneer in adopting such a law in the region, the legislation was introduced under the Ben Ali regime that placed political opponents under physical and electronic surveillance. The Organic Act No. 26 of 2015 Relating to the Fight Against Terrorism and the Suppression of Money Laundering[52] grants an Investigative Judge or the Prosecutor of the Republic the power to issue interception orders. Section 54(5) of the Act requires the authority responsible for carrying out the interception to apply for a warrant from the public prosecutor or the investigating judge. The maximum period of the order is four months, and it is renewable only once for the same duration.

Data can be collected by the Technical Telecommunication Agency (ATT) from the servers of telecom operators and Internet Service Providers (ISPs). The law requires investigators to always keep a written record of surveillance operations and under section 56(2) all data not leading to a criminal prosecution is protected by the data protection law. Meanwhile, ISPs are bound to keep customers' personal data confidential (article 14).

However, the current laws fail to put in place adequate mechanisms to ensure that any interference with citizens' communications upholds international standards and does not infringe on their rights, including the right to proper redress and remedy when privacy violations occur. Contrary to the provisions of the Declaration on Principles of Freedom of Expression and Access to Information in Africa, they do not provide effective monitoring and regular review of lawful surveillance and exempts public institutions from some of the provisions.

Article 11(3-4) of the 2014 decree that sets out the modalities for the operations of ISPs requires them to render assistance to the relevant authorities as necessary for the performance of their duties, and specifically obliges them to respect instructions of judicial, military, and national security authorities.[53]

Decree No. 2013-4506, relating to the creation of the ATT does not put in place transparency mechanisms over the Agency's activities. While article 5 requires the submission of annual reports by the agency's Director-General to the ICT ministry, there are no requirements that these reports should be made public. Meanwhile, article 16 exempts contracts linked to ATT's purchases from being subject to general transparency obligations placed on other public institutions.[54] Also, the directors of the ATT are appointed by the ICT minister, under whose control the Agency falls.

Tunisian law does not provide for a subject of surveillance to be given notification prior, during or after surveillance. This undermines an individual's ability to oppose or challenge the interception, monitoring, recording, or storing of their communications. Unauthorised interception attracts a punishment of between one and five years in prison and a fine ranging from 1,000 to 5,000 Tunisian Dinar (DT) (USD 365-1823), per article 64 of the 2014 decree.

52 *Organic Act No. 26 of 2015, https://www.bct.gov.tn/bct/siteprod/documents/Loi_2015_26_fr.pdf*

53 *Decree No. 4773 of 2014 Fixing the Conditions and Procedures to Grant the Authorization for the Activity of Supplying Internet Services, http://www.intt.tn/upload/txts/fr/d%C3%A9cret2014_4773.pdf*

54 *http://www.intt.tn/upload/txts/fr/d%C3%A9cret2013_4506fr.pdf*

Uganda

Under section 4(3) of the RICA an application for a warrant must detail all facts and circumstances including the allegations against the subject of interception. Under section 5, a warrant is valid for three months but may be renewed for an unspecified time. Under section 6(b) of RICA, the warrant must specify the name and address of the interception subject and the manner of interception; order the service provider to strictly comply with such technical requirements as may be specified by a designated judge to facilitate the interception; specify the apparatus and other means that are to be used for identifying the communication that is to be intercepted; and contain any other necessary details relating to the interception subject.[55]

The Anti-Terrorism Act, 2002 Part VII (sections 18 to 22) provides for and permits the interception of communications and surveillance on grounds such as the public interest, national economy and security, prevention of crime and protection of human rights and freedoms.[56] Section 18 only designates the Minister responsible for internal affairs to authorise a security officer to carry out interception - whereas the 2010 interception regulations permit the heads of the police, defence forces, external security and internal security agencies to apply for interception warrants. The Act provides for the collection and storage of data with the aim of tracking terrorist activities and perpetrators of terrorism. Section 19(6)(a) of the Act empowers an authorised officer to detain a suspected individual and make copies of any intercepted matter.[57]

Part VII of the anti-terrorism law has been reinforced by section 2 of the RICA that provides for control of interception. Section 9(2) of RICA obligates telecommunication service providers to ensure that existing subscribers register their SIM cards. In addition, section 11 of the Act obligates service providers to always technically assist the government to intercept communications by installing hardware and software to enable the interception of communications. Further, section 28 of the Computer Misuse Act provides for searches and seizures, which potentially facilitates surveillance on the activities of individuals and groups.

Section 8(1)(2) of RICA penalises service providers who fail to assist and facilitate the interception of communications. Upon conviction, they are liable to a fine of up to Uganda Shillings (UGX) 2,400,000 (USD 667), or imprisonment for a period not exceeding five years, or both. The same penalties apply for illegal interception of communications (section 2(3)) and disclosure of communication or information obtained as a result of interception (section 15).

Zambia

The Cyber Security and Cyber Crimes Act, 2021 prohibits unlawful interception of communications under section 26(1).[58] Section 28 requires law enforcement officers seeking to intercept communications in relation to ongoing criminal investigations to apply to a judge for an interception of communications order, after making a written application to the Attorney General for written consent and such consent has been obtained. The interception order is valid for an initial period of three months, renewable by a judge for an unspecified period.[59]

In addition, section 29 permits law enforcement officers to intercept any communication without first seeking an interception order and to orally request a service provider to intercept communications where there are "reasonable grounds to prevent possible or inflicted bodily harm, loss of life or threats to kill oneself, or damage to property or actual or possible cause of financial loss." Similarly, section 30 permits oral requests for the interception of communication for purposes of determining location of an individual where a law enforcement officer has reasonable grounds to believe that an emergency exists.

55 *Regulation of Interception of Communications Act, 2010, http://www.ulrc.go.ug/system/files_force/ulrc_resources/regulation-interception-communications-act-2010.pdf?download=1*

56 *Anti-Terrorism Act, 2002, http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf*

57 *Under sections 2 and 18, an authorised person means one designated in writing by the minister responsible for internal affairs.*

58 *Cyber Security and Cyber Crimes Act, 2021, https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%202%20of%202021The%20Cyber%20Security%20and%20Cyber%20Crimes.pdf*

59 *Implications of Zambia's Cyber Security and Cyber Crimes Act 2021 on Digital Rights copy, https://cipesa.org/?wpfb_dl=447*

A law enforcement officer who intercepts communication under section 29 and 30 is required to immediately after the interception, submit to a judge a copy of the written confirmation of the interception request made to a service provider; an affidavit setting out the results and information obtained from that interception; and a recording of the communication that has been obtained through that interception, a full or partial transcript of the recording of the communication and any notes made by the law enforcement officer.

Also, section 34(1) of the law bars service providers from random monitoring of customers' communications except for mechanical or service quality control checks. Under section 37(1), persons who are neither law enforcement nor service providers are prohibited from using interception devices or systems, software or hardware. In section 82(1), the law provides that a service provider bears no obligation to monitor traffic data or to actively seek facts or circumstances indicating an unlawful activity over their platforms.

Under section 31(3), anyone that discloses contents of intercepted communications is liable to a fine of up to 300,000 Kwacha (USD 16,520) or imprisonment of up to 10 years, or both. Furthermore, under section 34(2), a service provider in Zambia who engages in random monitoring of customers' communications is liable for a fine not exceeding 150,000 Kwacha (USD 8,259), imprisonment of up to five years, or both. Moreover, section 35(4) of the law provides that a service provider who fails to disclose records or details of intercepted communication to a law enforcement officer is liable on conviction to a fine not exceeding 150,000 Kwacha (USD 8,259) or imprisonment of up to five years, or both. Also, under section 37, a person who is neither law enforcement nor service provider who uses a prohibited interception device or system software or hardware is liable to a fine not exceeding 900,000 Kwacha (USD 49,559) or imprisonment for 25 years, or both.

Zimbabwe

The Interception of Communications Act (2007) criminalises illegal interception, which is defined as interception of communication without consent or authorisation by a warrant.[60] Section 16(3) restricts disclosure of interception information to unauthorised parties, which is punishable with a fine not exceeding Zimbabwe Dollars (ZWL) 1,600,000 (USD 4,420), imprisonment for up to five years, or both. However, it also provides a legal basis for state authorities to conduct communications surveillance without safeguards such as the prior authorisation of an independent and impartial judicial authority; due process; specific limitation on time, notification of the surveillance and effective monitoring and regular review by an independent oversight mechanism, which are stipulated by the Declaration.[61]

Section 18 of the Interceptions Act states that individuals aggrieved by the warrant of interception issued by Postal and Telecommunications Authority may appeal to the Administrative court, which has the final decision. The law appears to suggest that the subject of monitoring would be informed of the decision authorising surveillance against them. Section 19 provides 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."

In 2020, the Access to Information and Protection of Privacy Act (AIPPA) was repealed and replaced by the Freedom of Information Act (2020).[62] The country currently has no designated privacy and data protection law.[63]

60 *Interception of Communications Act (Chapter 11:20), http://www.vertic.org/media/National%20Legislation/Zimbabwe/ZW_Interception_of_Communications_Act.pdf*

61 *Principle 41(3) of the ACHPR Declaration.*

62 *Freedom of Information Act No. 1 of 2020, http://www.veritaszim.net/sites/veritas_d/files/Freedom%20of%20Information%2C%20Act%20No.%201%20of%202020.pdf*

63 *Zimbabwe AfDec Covid-19 Report: Assessing compliance with the African Declaration on Internet Rights and Freedoms in Zimbabwe by Kuda Hove (Unpublished)*

According to a 2017 report by Privacy International,[64] communication surveillance by state security agencies in Kenya continues without oversight and outside of legal procedures. Through direct access to the country's telecommunications networks, the National Intelligence Services purportedly intercepts both communications data and content and shares the intelligence gathered with law enforcement authorities, paramilitary groups and anti-terrorism units. The gathered intelligence is the basis upon which counter-terrorism operations such as surveilling, profiling, locating, tracking and arresting targets are carried out, with well documented cases of abuse, torture, abduction and extrajudicial killings.

There are reports that like its counterpart in Kenya, Namibia's Central Intelligence Service conducts state-sanctioned interception of communications and surveillance against citizens under the guise of "countering violent extremism", "radicalisation" and terrorism.[65] [66]

Similar surveillance reports in Nigeria, Rwanda and Zimbabwe have come to the fore, with notable cases targeting journalists and critics. In 2020, Nigerian police were reported to have used telecom surveillance to lure and arrest journalist Samuel Ogundipe for questioning, after they used his friend Azeezat Adedigba's call data records obtained from telecom providers.[67]

In April 2014, private WhatsApp and Skype messages that popular Rwandan musician Kizito Mihigo purportedly exchanged with government opponents living in exile were used as evidence to convict him of conspiracy to overthrow the government.[68] He was sentenced in February 2015 to 10 years in prison, although three years later he was pardoned by the president. Communication interception was also used to gather evidence in the case of Diane Rwigara, a Rwandan government critic, but the prosecution lost the case in 2018 on grounds of insufficient evidence.[69] The trial of army officers Colonel Tom Byabagamba and retired Brigadier Frank Rusagara, who were convicted in 2016, also heard evidence from private communications.[70]

It is not clear if this evidence was intercepted, as Rwandan law provides that evidence of a crime collected after the message reached the receiver, and "evidence based on communication recorded by the sender or the receiver or other recording person without using a monitoring device for interception of communication" is not considered as interception of communication (article 15 of Prime Minister's order).

In Zimbabwe, there are reports that widespread use of technology by civil society and political activists for mobilisation and organising is matched by state surveillance of private communications which is facilitated by the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), where government control ensures compliance with its orders.

Meanwhile, surveillance through CCTV is also a growing concern. Unlike in Senegal where CCTV especially at workplaces is a contentious issue[71] and efforts are underway to regulate use of CCTV in public and private places, in other countries, deployments are increasingly widespread, without safeguards in place. For instance, whereas Zambia has a largely positive human rights record, the country has embarked on a Safe City Project that mounted 24-hour surveillance cameras in public places and on the main road networks without adequate judicial oversight and monitoring to guard against possible abuse by law enforcement agencies. [72] The Safe City Project is particularly worrying given that a 2020 report by Citizen Lab, a global digital rights watchdog, identified Zambia as a possible customer of cyber espionage software.[73] This was the second time that Zambia, alongside other African governments, was featured in the report that unmasks clients of surveillance software.

64 *Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf*

65 *Action Access to Internet, 'The rise of the Namibian surveillance state (Part I)', https://action-namibia.org/risenamibian-surveillance-state/*

66 *5 The Namibian, 'The rise of the Namibian surveillance state: Part 3', https://www.namibian.com.na/175475/archive-read/The-rise-of-the-Namibian-surveillance-sta*

67 *How Nigeria's police used telecom surveillance to lure and arrest journalists, https://cpj.org/2020/02/nigeria-police-telecom-surveillance-lure-arrest-journalists/*

68 *Kizito Mihigo pleads guilty as co-accused deny treason, https://www.theeastafrican.co.ke/tea/news/east-africa/kizito-mihigo-pleads-guilty-as-co-accused-deny-treason-1329746*

69 *Kigali court orders Diane Rwigara and mother detained, https://www.theeastafrican.co.ke/tea/news/east-africa/kigali-court-orders-diane-rwigara-and-mother-detained-1376018*

70 *Byabagamba, Rusagara get lengthy jail terms, https://www.newtimes.co.rw/section/read/198556*

71 *Vidéosurveillance dans les lieux de travail: la CDP avocat des salariés, https://www.socialnetlink.org/2019/12/12/videosurveillance-dans-les-lieux-de-travail-la-cdp-avocat-des-salaries/*

72 *Huawei to plant 24 Hour cameras across Lusaka, https://bit.ly/368Nesm*

73 *Citizen Lab, Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles, https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/*

2.2 Limitations on Encryption

Principle 40(3) of the Declaration provides 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 and standards." Anonymity and the use of encryption in digital communications engage both the right to freedom of expression and the 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.[74] Many countries under study have passed legislation that limit anonymity and the use of encryption.

There were a few positive provisions noted in some countries that required the protection of personal data through technical security measures, which include encryption. On the other hand, several countries have adopted laws which criminalise the unauthorised possession and use of cryptographic software or hardware, providing for fines or prison sentences. In Chad, Malawi, Senegal, Tanzania and Zambia, there are penalties for offering cryptographic services without licensing, registration or authorisation. Below, we explore the legal provisions on encryption in various countries. It should be noted that in virtually all countries, there is no evidence that the provisions of the laws relating to restrictions on the use of encryption have been employed to undermine the right to privacy or other digital rights.

Cameroon

Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercrime prohibits, under section 86(1), the importation, transfer or sale of computer programmes, passwords or access codes designed or adapted to facilitate access to all or part of an electronic communication or information system. Under section 7, the National Agency for Information and Communication Technologies (ANTIC) is empowered to examine applications for the certification of cryptographic means and issue certificates. Under section 55(2) of the same law, Cameroonian courts can order for decryption of encrypted content. Further, section 58(1) requires natural persons or corporate bodies providing cryptographic services to disclose to criminal investigation officers or authorised officials of the ANTIC, upon request, their encoding systems.

Moreover, under section 60, ANTIC may prohibit the circulation of a means of cryptography where a Certification Authority is non-compliant.[75] In such an instance, the provider is under an obligation to withdraw the means of cryptography from circulation. Under section 88(1), a person who uses a secret decoding convention or cryptographic means to prepare, facilitate or commit a crime, or refuses to hand it over to judicial authorities, or refuses to use it on request by such authorities, shall be punished with imprisonment for between one and five years or a fine of between one million and five million CFA francs (USD 1,845-9,226), or both. Where the disclosure to authorities could have helped to prevent the commission of a crime or limited its effects, the penalties may be increased to imprisonment for three to five years and a fine of between one million and five million CFA francs (USD 1,845-9,226).

Chad

Article 14 of Law No. 007/PR/2015 on the protection of personal data provides for confidentiality, especially when the processing involves data transmission over a network. Further, under article 19 and 36 of the Law No. 009/PR/2015 on Cybersecurity and Cybercrime, judicial authorities may require decryption when a means of cryptography has been used. Further, under article 22, cryptography service providers are required to provide court or police "with agreements allowing the decryption of transformed data." Providing cryptology services without prior approval attracts imprisonment of between one and five years, a fine ranging between one million and 10 million CFA Francs (USD 1,837-18,304), or both.

74 *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*

75 *A Certification authority is a "trusted authority responsible for creating and assigning public and private keys as well as electronic certificates". Section 4 (11) of the Cameroonian Cybersecurity and Cybercrime Act.*

Ethiopia

In Ethiopia, the manufacture, assembly and import of any telecommunications equipment that also includes encryption technology requires a license from the government. Article 3(1) of the Proclamation on Telecom Fraud Offences (No. 761/2012) criminalises the manufacture, assembly or import of any telecommunications equipment without a permit, which is punishable by "rigorous imprisonment" for between 10 and 15 years and a fine of between Birr 100,000 and 150,000 (USD 2,251-3,376).[76] In addition, article 3(2) states that a person who uses or holds any telecom equipment without a permit is upon conviction liable to imprisonment of between one and four years and a fine of between Birr 10,000 to 40,000 (USD 225-900).

Kenya

The country has a few positive provisions that require the protection of personal data through technical security measures, including encryption. Section 41 of the Data Protection Act, 2019[77] requires all data controllers or processors to implement appropriate technical measures to ensure privacy by design or default, which include pseudonymisation and encryption of personal data. Additionally, the draft Data Protection (Civil Registration) Regulations, 2020 under regulation 35(2) requires that the transfer of personal data through a public network be conducted through commonly used encryption methods.

However, section 53 of the Computer Misuse and Cybercrimes Act, 2018 permits the police to seek court orders to compel a service provider to collect or record content data through the application of technical means. Service providers may also be ordered to cooperate and assist the competent authorities in the collection or recording of content data, in real-time, of specified communications within the jurisdiction transmitted by means of a computer system. The unauthorised disclosure of passwords and access codes to data in a computer system attracts a fine of up to five million shillings (USD 46,430) or imprisonment of up to three years under section 19 of the Act.

Malawi

Section 52(4) of the Electronic Transaction and Cyber Security Act, 2016 permits the lawful use of encryption programmes or products provided that they have lawfully come into possession of a person. Section 74 of the Act requires data controllers to implement "technical and organisational measures" to protect personal data against accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

In addition, providers of cryptographic services or products are required to register with the Malawi Communications Regulatory Authority (MACRA) under section 52 of the Electronic Transaction and Cyber Security Act, 2016.[78] The registration requirements might make it easy for the regulator and other government agencies to have access to information held by encryption services providers, including decryption keys and encrypted data. Also, section 67(1) requires a person who provides encryption services to declare to MACRA "the technical characteristics of the encryption means as well as the source code of the software used". However, the Minister and MACRA are yet to develop the regulations required under section 52(3) of the Electronic Transaction and Cyber Security Act, 2016 to regulate or restrict the use, importation and exportation of encryption programmes and encryption products.

Under section 54(1) of the Electronic Transaction and Cyber Security Act, 2016, the use of cryptography without registration is an offence which attracts a penalty of five million Kwacha (USD 6,307) and imprisonment of seven years. Section 68 of the same law provides that where a supplier of encryption does not comply with its obligation under the Act, MACRA may prohibit the distribution of the concerned encryption.

76 *World Map of Encryption, https://www.gp-digital.org/world-map-of-encryption/*

77 *Data Protection Act, 2019, http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf*

78 *Malawi Government Act, No. 33 of 2016, November 4, 2016, https://malawilii.org/mw/legislation/act/2016/33*

Mali

Many provisions under the Cybercrime Act are likely to weaken the use of cryptographic services. The law requires any cryptology services provider must communicate to the Authority in charge of the regulation of cryptology,[79] the description of the technical characteristics of the means of cryptology and the source code of the software used (article 37). Similarly, any supply, import or export of cryptology services not exclusively providing authentication or integrity control functions must first obtain authorisation from the Authority in charge of cryptology regulation (articles 38, 39 and 40).[80]

Article 75 provides that data may be copied and stored where seizure of the medium seems inappropriate. Article 77 requires the public prosecutor or the examining magistrate to requisition any qualified natural or legal person to conduct technical operations to enable access to encrypted data during an investigation, or to demand the secret convention of decryption of the cryptogram, when a means of cryptography has been used. In addition, cryptography services providers are required to decrypt data at judicial authorities' request, or provide the latter with the codes allowing the decryption of data they have encrypted (article 78).

The failure by a cryptology services provider to inform the Authority in charge of the regulation of cryptology of the description of the technical characteristics of the means of cryptology and the source code of the software used, as provided for under article 37, is punishable with imprisonment for from six months to five years, a fine of 400,000 to 20 million CFA francs (USD 735-36,769), or both. The same penalties apply to a service provider who supplies, imports or exports cryptology services not exclusively providing authentication or integrity control functions without authorisation from the Authority (articles 38, 39 and 40).

Namibia

Article 76 of Namibia's Communications Act criminalises the possession, import, export, distribution or sale of any equipment or software that "may be used to prevent lawful interception or monitoring or rendering it less effective". Article 76 punishes the possession, import, export, distribution or sale of any equipment or software that "may be used to prevent lawful interception or monitoring or rendering it less effective" with a fine of N$20,000 (USD 1,343), imprisonment for five years, or both.

Nigeria

Of concern, rule 11 of the Lawful Interception of Communication Regulations provides that no licensee shall provide any communications services that cannot be monitored and intercepted.[81] Furthermore, rule 9(1) of the regulations states that where the communication intercepted is encrypted or protected communication within the possession of the licensee, they will be required to provide it, upon request, to the authorised agency. Penalties for non-compliance are hefty as prescribed by rule 16 of the regulations, of Nigerian Naira (₦) five million (USD 12,273) and where the offence continues, a daily default penalty of ₦ 500,000 (USD 1,228).

79 *Here, the Malian Regulatory Authority for Telecommunications, Information and Communication Technology and Posts (AMRTP); Article 2 of Decree No. 2019-0248 P-RM of March 27, 2019 setting the conditions for issuing the Approval to Cryptology Service Providers as well as their Obligations.*

80 *Mali; Law n°2019-056 of 05 December 2019 on the Suppression of Cybercrime*

81 *Lawful Interception of Communications Regulations, 2019, https://www.ncc.gov.ng/accessible/documents/839-lawful-interception-of-comunications-regulations-1/file*

Senegal

Article 12 of the Law on Cryptography of 2008 (Law No. 2008-41) provides that the use of encryption services and means is free, unless the encryption provides confidentiality (as opposed to simply integrity or authenticity) functions.[82] Further, the supply, import and export of cryptology means exclusively ensuring authentication or integrity control functions are also free. Under Article 13 of Decree No. 2010-1209 on Cryptology, the use of encryption is free only if the key length is less than or equal to 128 bits.[83] Article 14 and 15 of the Law on Cryptography of 2008 states that the supply, import or export of means of cryptology that do not exclusively provide authentication or integrity control functions is subject to prior authorisation by the National Cryptology Commission. Under article 16, bodies offering cryptology services must be licenced by the Commission.

Under article 19 of the same law, the National Cryptology Commission may impose sanctions on providers of cryptology services for failing to comply with their obligations under the law, such as prohibition of the means of cryptology, temporary withdrawal of the authorisation granted for up to three months, or total withdrawal of the authorisation, or fines. Chapter VII provides for additional sanctions including imprisonment of between six months and two years, a fine of between 400,000 and two million CFA francs (USD 735-3,673), or both, for failing to provide the technical characteristics of the cryptology means. In addition, the provision of cryptology services without the prior approval of the Commission attracts imprisonment of between one and five years, a fine of one million to 20 million CFA francs (USD 1,837-36,731), or both. The same penalties apply for the use of a banned means of cryptology.

South Africa

There are different provisions that deal with decryption in South Africa. Section 21 of RICA provides that an officer of the Police, or an authorised law enforcement officer, may apply to a designated judge who may issue a decryption direction if the judge is satisfied with the facts alleged in the application. The direction must be in writing and is for a renewable period of three months. A decryption key holder addressed in a decryption direction may only disclose the decryption key or provide the decryption assistance but may not disclose any other information which is not specified in the direction.

Furthermore, Chapter V of the Electronic Communications and Transactions Act, 2002[84] (ECTA) deals with cryptography providers. Section 29 provides that the Director-General must establish and maintain a register of cryptography providers; and section 30 provides that no person may provide cryptography services or products in South Africa until the particulars referred to in section 29 have been recorded in the register. Section 31 provides that the information contained in the register must not be disclosed to any person other than to employees of the Department of Communication who are responsible for keeping the register, or subject to certain exceptions. Section 32 provides that the provisions of Chapter V do not apply to the National Intelligence Agency.

82 *Law on Cryptography (Law No. 2008-41), http://www.jo.gouv.sn/spip.php?article7197*

83 *Decree No. 2010-1209, http://www.jo.gouv.sn/spip.php?article8667*

84 *Electronic Communications and Transactions Act, 2002, https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf*

Tanzania

In 2016, Tanzania passed the Electronic Transactions (Cryptographic and Certification Services Providers) Regulations, 2016 to provide the framework for licensing cryptographic and certification providers.[85] Despite requiring registration of service providers, rule 29(1) of these regulations obligates cryptographic and certification service providers and their agents to keep subscribers' information confidential, and only disclose it when authorised by the subscribers. However, section 35(2)(d) of the Electronic Transactions Act, 2015 requires applicants for a license to disclose a description of the technology to be applied in their services. Further, section 33 of the Act requires the minister to designate a government institution to regulate cryptographic and certification services.

Providing cryptographic or certification services without a license contravenes section 36(1) of the Electronic Transactions Act, 2015 and attracts a fine of not less than 10 million shillings (USD 4,312), imprisonment for a term not less than five years, or both.

Tunisia

Tunisian Internet Service Providers may only transmit encrypted information subject to the authorisation of the communications minister. According to Decree No. 2008-2639 regulating the importation and commercialisation of encryption systems for telecom networks, the National Agency of Digital Certification and the Centre for Studies and Researches of Telecommunications (which comprises members appointed by the communications minister) approve the import and sale of encryption systems.[86] This decree does not apply to encryption used by the ministries of National Defence, the Interior, or Foreign Affairs, or by diplomatic and consular missions in Tunisia.

Tunisia prohibits the importation or distribution of cryptographic software or hardware without authorisation. Article 87 of the 2001 Telecommunications Code provides for imprisonment for between six months and five years, a fine of one thousand to five thousand dinars (USD 365-1,823), or both for whoever uses, manufactures, imports, exports, holds for sale or free distribution the means or cryptology services without authorisation.[87] Section 88 of the Electronic Signatures Act grants police conducting a search under section 86 and 87 of the Act unlimited access to computerised data, including passwords, encryption or decryption codes, and any other means required to enable the comprehension of computerised data.[88]

Zambia

Section 85 of the Electronic Communications and Transactions Act, 2021[89] permits the use of encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used, in the manner provided for under the law. Further, section 86 of the Act provides that the Act should not be construed as requiring the use of any form of encryption that "limits or affects the ability of the person to use encryption without a key escrow function, or limits or affects the ability of the person who uses encryption with a key escrow function not to use a key holder." Section 89 punishes the use of encryption to obstruct or impede a law enforcement officer or interfere with their performance of any functions under the Act, with a fine of up to 60,000 Kwacha (USD 2,672), imprisonment for a term not exceeding two years, or both. Under section 34(3) of the law, a person who provides a cryptography service without registration is liable for a fine of 150,000 Kwacha (USD 8,260) or imprisonment of up to five years.

84 *Electronic Transactions (Cryptographic and Certification Services Providers) Regulations, 2016, https://www.parliament.go.tz/uploads/documents/1476207950-GN%20228-ELECTRONIC%20TRANSACTIONS%20(CRYPTOGRAPHIC%20AND%20CERTIFICATION%20SERVICES%20PROVIDERS)%20REGULATIONS,%202016.pdf*

85 *Decree N° 2008-2639, http://www.certification.tn/sites/default/files/reglementations/Decret2639-2008Fr.pdf*

86 *This includes the use, manufacture, import, export, holding for sale or distribution as free or expensive or offers for sale or sells the means or cryptology services without authorisation.*

89 *Section 86 provides for search by warrant issued by a Magistrate while Section 87 provides for search and seizure without warrant to a police officer not below the rank of Inspector Electronic Communications and Transactions Act, 2021, https://zambialii.org/zm/legislation/act/2021/no4-2021/act-no-4-2021-electronic-communications-and-transactions0.pdf*

However, section 34(1) requires a person who intends to provide cryptography services to apply for registration to the National Root Certification Authority and to pay the prescribed fee. The registration requirements might make it easy for the regulator and other government agencies to access information held by encryption services providers, including decryption keys and encrypted data. Moreover, per section 83(2), the Minister may, by statutory instrument, prescribe procedures for service providers to inform the competent public authorities of alleged illegal activities or information provided by recipients of their service and communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

On a positive note, under section 2(a) of the Electronic Communications and Transactions Act, 2021, a person that gains unauthorised access to encryption or decryption keys is liable to imprisonment for between 10 and 25 years without the option of a fine. Section 87 penalises the release of decryption keys or the decryption of any data without authorisation, with a term of imprisonment of between 10 to 25 years without the option of a fine. Also, section 88 of the Act punishes the disclosure of a record or any other personal information relating to an owner of a key held or managed by the key holder with a similar penalty.

Zimbabwe

Under section 11(1) of the Interception of Communications Act, security and law enforcement agencies may impose "disclosure requirements" to persons in respect of encrypted information where they believe that a key to encrypted information is in the possession of that person, and the disclosure is necessary, in the interests of national security, to prevent or detect a serious criminal offence, or in the interests of the country's economic well-being. Further, section 11(1)(d) provides that if an authorised person believes that it is not reasonably practicable for them to obtain possession of the protected information in an intelligible form without giving the required notice, the authorised person may by notice to the person whom he or she believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

Moreover, once the disclosure requirement is issued, section 11(4) requires the person to use any key in their possession to provide access to the information to an authorised officer in an intelligible form. Where the person no longer possesses the key but has information that will facilitate obtaining or discovery of the key, section 11(6) requires that they disclose that information to the law enforcement agency. Under section 11(8) of the Act, failure to comply with a disclosure requirement is an offence, punishable with up to five years' imprisonment, a fine not exceeding ZWL 120,000 (USD 373), or both.

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. Furthermore, Principle 42 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."

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. Also, 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.[90]

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."[91] 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.[92] Hence, critics 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."[93]

In light of the above, African countries are adopting differing approaches towards data localisation. In several countries, there are restrictions to the cross-border transfer of data, and the transfer is permitted where certain conditions are met, or where the relevant government bodies grant authorisation. Some countries use financial services (Nigeria, Ethiopia, Rwanda and Uganda), 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. However, there is limited evidence of how various countries have implemented their legal provisions on data localisation.

Cameroon

Cameroon does not have a clear legal framework for data localisation. However, data encryption can be waived in certain conditions regarding international judicial cooperation and assistance. While section 90 of the Cybersecurity and Cybercrime Act provides that Cameroonian certification authorities[94] may establish agreements with foreign certification authorities, there is no clear specification as to the agreements' types or conditions. Moreover, under section 57(1), foreign jurisdictions can receive warrants from Cameroonian judicial authorities to investigate cybercrime offences when they are partially committed in Cameroon or where one of the perpetrators is in Cameroon. Section 20(1) specifies that an electronic certificate[95] issued outside the national territory produces the same legal effects as a qualified certificate issued in Cameroon, provided that there is an act of recognition from the issuing authority signed by the minister in charge of telecommunications.

90 *Ibid*

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

92 *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*

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

94 *A certification authority is defined as a trusted authority responsible for creating and assigning keys used for asymmetric encryption mechanisms belonging to secret entities, or which can be freely distributed; Article 4 (11) (17) (18) (19) of the Cybersecurity and Cybercrime Act.*

95 *Defined as an electronic document secured by the electronic signature of the person who issued it and who certifies the authenticity of its content; Section 4 (13) of Cybersecurity and Cybercrime Act.*

Chad

Article 29 of Law No. 007/PR/2015 on the protection of personal data[96] prohibits the transfer of personal data to a country that is not a member of the Economic and Monetary Community of Central Africa (CEMAC) or the Economic Community of Central African States (ECCAS), unless this state ensures a sufficient level of protection of the privacy, freedoms and fundamental rights of individuals. Under article 84, a prison term of between three months and one year, or a fine of one to ten million CFA Francs (USD 1,837-18,304) applies to any person who transfers data to a country outside ECCAS or CEMAC, or to a country that does not have sufficient data protection safeguards.

Egypt

Under article 35 of the personal data protection law, a data subject has a right to compensation in case of breach of the law. Article 36 of the law adds that a processor, controller and possessor or those who collects, processes, discloses, and circulates any personal data which is electronically processed in non-permissioned cases or without consent of data subject shall be punished with a fine of not less 100,000 Egyptian Pounds (LE) (USD 6,382) and not more two million LE (USD 127,636).

Further, if the purpose was to get material or moral benefit or to expose the data subject to harm and risk, the punishment is imprisonment for not less than six months, a fine not less 200,000 LE (USD 12,764) and not more two million LE (USD 127,636), or both. Article 41 of the same law stipulates that a processor, controller and a possessor who collects, processes, discloses, circulates, stores and maintains any sensitive personal data in non-permissioned cases or without consent of data subject shall be punished with imprisonment for no less than three months, a fine of not less 500,000 LE (USD 31,908) and not more five million LE (USD 319,089) or both.

Ethiopia

According to the Licensing and Authorisation of Payment System Operators Directive No. ONPS/02/2020, the transfer of domestic payment information outside of Ethiopia for the purposes of authorisation, clearing and settlement by Point of Sale (POS) machine operators is outlawed. Consequently, only payment data made through the international card scheme to the financial institution or national switch can be sent. Similarly, Automated Teller Machine (ATM) operators are prohibited from sending any transaction data outside Ethiopia for processing, authorisation and switching.

Kenya

Kenya's Data Protection Act 2019 in sections 48 and 49 prohibits cross-border transfer of personal data to a country that lacks appropriate safeguards to the security of the data. However, the Data Commissioner may authorise cross-border transfer where the necessity of the transfer is justified. Further, the Cabinet is empowered to develop regulations requiring that specific processing be carried out through servers or data centres located in Kenya.

Also, the draft Data Protection (General) Regulations 2021 are very explicit on localisation and seek to impose, under Part VII, further conditions regulating the transfer of personal data outside Kenya.[97] Article 38 stipulates the requirements prior to transfer, while article 39 requires the transferring entity to enter a written agreement with the recipient of the personal data that shall contain provisions on (a) the unlimited access by the transferring entity to ascertain the existence of a robust information technology system of the recipient for storing the personal data; and (b) the countries and territories to which the personal data may be transferred under the contract. Meanwhile, article 41 provides that for the purpose of confirming the existence of appropriate data protection safeguards in the recipient country, any country or a territory is taken to have such safeguards if has ratified the African Union Convention on Cyber Security and Personal Data Protection; or has a reciprocal data protection agreement with Kenya; or has an adequate data protection law as shall be determined by the Data Commissioner.

96 *Chad; Law No. 007 / PR / 2015 on the protection of personal data: https://bit.ly/32CSuSr*

97 *Data Protection (General) Regulations 2021, https://www.odpc.go.ke/regulations/data-protection-general-regulations-2021/*

Likewise, rule 38 of the draft Data Protection (Civil Registration) Regulations, 2020 proposes to prohibit civil registration entities from transferring personal data collected for civil registration purposes out of Kenya, except with the written approval of the National Security Council.[98]

Under section 58 of the Act, the Data Commissioner is empowered to issue enforcement notices to any person who has failed to comply with any provision of the Act. The Commissioner may impose administrative fines of up to five million shillings (USD 46,315), for the infringement of any provision of the Act. In the case of a legal entity, the fine may be up to one percent of its annual turnover of the preceding financial year, whichever is lower.

Clause 44 of the Huduma Bill, 2019 proposes that any processing of data under the National Integrated Identity Management System (NIIMS) be done through a server or a data centre located in Kenya.[99]

Malawi

Clause 36 of Malawi's Data Protection Bill, 2021[100] proposes that cross-border transfer of personal data should only happen on condition that the data subject has given consent to such transfer after being informed of possible risks of such transfers; the processing is necessary for the performance of a contract to which the data subject is party; and where the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject to that transfer.

While some countries do not provide a specific penalty for unauthorised cross-border data transfer, such penal consequences may be inferred from other provisions relating to non-compliance. In Malawi, Section 42 of the Data Protection Bill, 2021 penalises non-compliant data controllers and processors with a fine of five million Malawi Kwacha (USD 6,375).

Nigeria

The 2019 Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) issued by the National Information Technology Development Agency (NITDA) require telecommunication and networking services companies to host all subscriber and consumer data within the country.[101] Also, guideline 13 requires all government ministries, departments and agencies to host all sovereign data locally on servers within Nigeria, and only host the data outside the country with NITDA's express approval.

The grounds for an approval to host data outside Nigeria include: compliance with the Nigeria Data Protection Regulation, where personal data is in consideration; implications of the Nigeria Cloud Policy; a guarantee that the Nigerian government has unfettered right to access and retrieve its data wherever it is located; and an undertaking of non-disclosure of the Nigerian government's data to any third party without the express consent of the government. Other considerations include a guarantee of adequate and appropriate data security processes; a choice by the Nigerian government of the jurisdiction where its data will be hosted; and an undertaking for periodic submission of third-party audit reports for review by NITDA.

Meanwhile, Guideline 4.4.8 of the Central Bank of Nigeria's 2011 Guidelines on Point of Sale (POS) Card Acceptance Services requires entities engaging in POS services to use a local network switch (which connects devices and processes information to and from connected devices) for all domestic transactions. Domestic transactions cannot be routed outside Nigeria for switching between Nigerian issuers and acquirers. [102]

98 *The Data Protection (Civil Registration) Regulations, 2020, https://ict.go.ke/wp-content/uploads/2020/02/THE-DATA-PROTECTION-CIVIL-REGISTRATION-REGULATIONS-2020.pdf*

99 *Huduma Bill https://www.ict.go.ke/wp-content/uploads/2019/07/12-07-2019-The-Huduma-Bill-2019-2.pdf*

100 *Invitation to Comment on the Draft Data Protection Bill, 2021, http://www.pppc.mw/assets/upload/downloads/Notice_-_Data_Protection_Draft_Legislation_Ver_4__2_Feb.pdf*

101 *Guideline No. 11.1(4) and 12.1(4) of the Guidelines for Nigerian Content Development in Information and Communication Technology (ICT), https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf*

102 *Data localisation laws: Nigeria, https://www.uubo.org/media/1795/data-localization-laws-nigeria-w-022-1015.pdf*

Neither the Central Bank of Nigeria's 2011 Guidelines on Point-of-Sale Card Acceptance Services nor NITDA's Guidelines for Nigerian Content Development in ICT specify penalties for violations. Nonetheless, the National Data Protection Regulation stipulates penalties for privacy breaches, some of which might be applicable to unauthorised cross-border data transfer and storage. For example, per section 2.10(a), breaches by a data controller dealing with more than 10,000 data subjects draw a fine of 2% of annual gross revenue of the preceding year or payment of the sum of 10 million Naira (USD 26,281), whichever is greater. Data controllers with less than 10,000 data subjects pay a fine of 1% of their annual gross revenue or two million Naira, whichever is greater.

Rwanda

Article 3 of the Regulation No. 02/2018 of 24/01/2018 on cyber security provides that any bank licensed by the Central Bank must maintain its primary data within the territory of Rwanda.[103] Article 27 of the 2010 law governing the credit information system in Rwanda provides that the Central Bank shall have the authority to approve the sharing of customer information beyond the borders of Rwanda. Similarly, the Regulation n° 03/2018 of 24/01/2018 on Outsourcing provides that banks "shall not outsource their primary data outside Rwanda as provided in the regulation on cyber security".[104]

Further, the Ministerial Instructions N° 001/MINICT/2012 OF 12/03/2012 Related to the Procurement of ICT Goods and Services by Rwanda Public Institutions, provides in article 17 that all government systems and applications which process, store and provide critical government data and information shall be hosted in the National Data Centre.[105] Those listed are website hosting, email hosting, shared applications such as document management and e-archiving, and government enterprise applications.

Article 54 and 55 of the law on data protection and privacy of 2021 regulates cross-border data transfer.[106] Authorisation is granted by the Authority in charge of data protection after providing proof of appropriate safeguards with respect to the protection of the personal data. Under article 55, controllers and processors shall host and store personal data in Rwanda except with the Authority's authorisation.

Under article 15 of the Cybersecurity Regulation of 2020, which replaced the regulations of 2016,[107] all networks, systems and applications of a licensee shall not be managed, hosted, accessed or located outside Rwanda unless explicitly authorised by the regulator.[108] Article 32 lays down sanctions for non-compliance with regulator directives, which include an administrative fine of between one million and five million Rwandan Francs (FRw) or USD 997-USD 4,987.

Rwanda is renowned for intercepting communications and conducting surveillance against government critics and opponents.[109] Having data locally hosted makes that effort easier. Indeed, according to its preamble, the Cybersecurity Regulations were made pursuant to the 2013 law regulating the interception of communications especially article 5,[110] and to the Prime Minister's Order n° 90/03 of 11/09/2014 determining modalities for the enforcement of the law regulating interception of communication, specifically under articles 8 and 9.[111]

103 *Regulation No. 02/2018 of 24/01/2018 on cyber security, https://tinyurl.com/yk8t8zr5*

104 *Regulation n° 03/2018 of 24/01/2018, https://gazettes.africa/archive/rw/2018/rw-government-gazette-dated-2018-08-06-no-32.pdf*

105 *Instructions on Procurement of ICT Goods and Services by Public Institutions, https://tinyurl.com/36hxdrxd*

106 *https://www.minijust.gov.rw/fileadmin/user_upload/Minijust/Publications/Official_Gazette/2021_Official_Gazettes/October/OG_Special_of_15.10.2021_Amakuru_bwite.pdf*

107 *Regulations Governing Telecom Network Security in Rwanda (2016) metamorphosed into the Cybersecurity Regulation of 2020*

108 *RURA, Cybersecurity Regulation of 2020, https://rura.rw/fileadmin/Documents/ICT/Laws/Cybersecurity_Regulation_in_Rwanda.pdf*

109 *Rwanda – the country where a private conversation can cost you your freedom, https://www.telegraph.co.uk/global-health/terror-and-security/rwanda-country-private-conversation-can-cost-freedom/*

110 *Article 5 states that the interception of any communication in the course of the transmission by means of a public or private communication system or a public or private postal service when it is done without authorisation from the competent authority shall be unlawful. See https://gazettes.africa/archive/rw/2013/rw-government-gazette-dated-2013-10-14-no-41.pdf*

111 *Article 8, on Protection of the intercepted information, provides that the organ that intercepted communication, in order to protect the intercepted information, prepares i) the level of classification of the intercepted information in accordance to the classification of information; and ii) persons to whom the intercepted information can be shared with and the manner for sharing the information. Article 9 provides that each security organ authorised to intercept communication shall establish regulations governing the management of intercepted information. See: Order n° 90/03 of 11/09/2014, https://tinyurl.com/9u3fm9hk*

Senegal

Article 49 of the law on the protection of personal data of 2008 prohibits the transfer of personal data across borders if the principle of reciprocity relating to the protection of privacy and fundamental rights and freedoms is not ensured. It stipulates that a data controller may only transfer personal data to a third country if that country ensures an adequate level of protection of the privacy, fundamental rights and freedoms of individuals with regard to the processing of which such data are or may be the subject. Per article 49(3) of this law, the Data Protection Commission has to be informed and to authorise cross-border data transfers. Article 4 of the law on the protection of personal data enshrines the obligation to appoint a representative based in Senegal when data processing is to be carried out by a processor located outside Senegalese territory.

South Africa

The POPIA prohibits cross-border data transfers unless one of the exceptions applies, including having consent to the transfer or in circumstances where the foreign country provides for adequate safeguards.[112] Moreover, the Draft National Policy on Data and Cloud[113] contains several provisions on data localisation. Clause 10.4.1 proposes that all data classified as Critical Information Infrastructure should be processed and stored within South Africa. Clause 10.4.2 provides that any cross-border transfer of data should be governed by POPIA but clause 10.4.3 adds that even where data is transferred beyond national borders, a copy of such data must be stored in South Africa for purposes of law enforcement. The draft policy has, however, been met with some criticism, including its proposals on cross-border data transfers.[114]

Tunisia

The Organic Act No. 2004-63 of 27 July 2004 on the Protection of Personal Data prohibits the transfer of personal data to a foreign state if it does not provide an adequate level of protection.[115] Additionally, article 50 prohibits the transfer of personal data to a foreign state if it may endanger public security or Tunisia's vital interests. On September 5, 2018, the National Authority for the Protection of Personal Data (INPDP) issued a list of 49 countries it said provided an adequate level of data protection, the African ones being only Algeria, Mauritania, Mauritius, Morocco, and Senegal.[116]

However, the INPDP lacks the resources to operate efficiently and proactively. Moreover, its members are appointed by the government and there are no measures to ensure their independence. Nonetheless, in its 2009-2017 report,[117] the INPDP reported receiving complaints against public authorities like the interior ministry but was not able to further consider them because public authorities are exempt from oversight provisions of this law.

Meanwhile, in November 2017, the INPDP informed the public prosecutor of infractions committed by OVH Tunisie, a subsidiary of the French cloud computing company OVH.[118] The lawsuit was based on three infractions, two of which were related to data localisation. The INPDP said the company did not disclose to its Tunisian customers where their data was stored nor got their consent. The other offence was related to the transfer of data from Tunisian customers abroad without requesting authorisation from the INPDP in violation of article 52 of the data protection law.

Article 90 of the 2004 data protection law prohibits the transfer of personal data to a foreign state without the INPDP's authorisation and the data subject's consent. The penalty for this offence is imprisonment for one year and a fine of TND 5,000 (USD 1,823). Article 87 stipulates a two-year imprisonment and a fine of TND 10,000 (USD 3,646) for violating the provisions on processing sensitive data.

112 *South African Data Protection Law and Third Party Processors, https://www.dlapiper.com/en/belgium/insights/publications/2019/04/africa-connected-issue-2/south-african-data-protection-law-and-third-party-processors/*

113 *Draft National Policy on Data and Cloud, https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf*

114 *Several flaws in SA's draft data and cloud policy, say experts, https://www.itweb.co.za/content/xA9PO7NZ46Z7o4J8*

115 *Organic Act No. 2004-63 of 27 July 2004 on the Protection of Personal Data, http://www.inpdp.nat.tn/ressources/loi_2004.pdf*

116 *INPDP, http://www.inpdp.nat.tn/3_protection_adequate.pdf*

117 *INPDP Report, http://www.inpdp.nat.tn/Rapport_2009-2017.pdf*

118 *INPDP Report, https://thd.tn/linpdp-apporte-des-precisions-sur-laffaire-dovh-tunisie/*

Uganda

Article 68 of Uganda's National Payment Systems Act 2020 states that an electronic money issuer, shall establish and maintain its primary data centre in relation to payment system services in Uganda. Meanwhile, section 19 of the Privacy and Data Protect Act, 2019 provides that where a data processor or controller based in Uganda processes or stores personal data outside Uganda, they shall ensure that the country in which the data is processed or stored has adequate measures in place for the protection of personal data at least equivalent to the protection provided for by the Act. Section 35 of the Data Protection and Privacy Act penalises any person who unlawfully obtains, discloses, or procures the disclosure to another person of personal data held by a data controller or processor with a fine not exceeding UGX 4.8 million (USD 1,327) or imprisonment for 10 years, or both.

Zambia

Section 18(1) of the Cyber Security and Cyber Crimes Act, 2021 obligates a data controller to store all critical information[119] on a server or data centre located within Zambia unless authorised by the Minister. Under Section 18(2), the Minister may authorise a controller of critical information to externalise the critical information outside the country. Moreover, the cybersecurity law specifies "critical information"[120] and section 70(2) provides that although the minister may prescribe categories of personal data that may be stored outside the country, "sensitive personal data"[121] is exempted and must be processed and stored in a server or data centre located in Zambia.

In the same vein, the Data Protection Act, 2021, under Section 70, requires data controllers to process and store personal data on a server or data centre located in Zambia.

Zimbabwe

Clause 28(1) of the Cyber Security and Data Protection Bill,[122] proposes that a data controller may not transfer personal information about a data subject to a third party who is in a foreign country unless an adequate level of protection is ensured in the recipient country or international organisation and the data is transferred solely to allow tasks covered by the competence of the controller to be carried out.[123]

119 *Section 2 of the Act defines "critical information" as information that is declared by the Minister to be critical for the purposes of national security or the economic and social wellbeing of the Republic*

120 *Section 17(1) provides that the Minister may by statutory instrument declare information which is of importance to the protection of national security, economic or social well-being of the Republic, to be critical information*

121 *"Sensitive personal data" means personal data which by its nature may be used to suppress the data subject's fundamental rights and freedoms and includes (a) the race, marital status, ethnic origin or sex of a data subject; (b) genetic data and biometric data; (c) child abuse data; (d) a data subject's political opinions; (e) a data subject's religious beliefs or other beliefs of a similar nature; (f) whether a data subject is a member of a trade union; or (g) a data subject's physical or mental health, or physical or mental condition*

122 *Cyber Security and Data Protection Bill (2019), https://www.cbn.gov.ng/cashless/POS_GUIDELINES_August2011_FINAL_FINAL%20(2).pdf*

123 *The Cyber Security and Data Protection Bill, https://www.veritaszim.net/sites/veritas_d/files/Cyber%20Security%20and%20Data%20Protection%20Bill.pdf*

Rwanda has been positioning itself to become a regional ICT hub and to engender ICT-driven socio-economic development. Data localisation is then seen as contributing to this vision of creating local capacity, infrastructure, and jobs.

In a directive issued in May 2017, the industry regulator, Rwanda Utilities Regulatory Authority (RURA), faulted MTN Rwanda for failing to shift its data centre from neighbouring Uganda. At the time, moving the data centre to Rwanda was deemed by some as a complex, expensive and disruptive matter that would undermine the MTN Group's efficient deployment of resources.

RURA fined MTN Rwanda FRw 7.03 billion (USD 8.2 million) for breach of the Regulations Governing Telecom Network Security in Rwanda (2016) whose article 16 provided that subscribers' information such as voice, SMS, data including call data records and billing information shall not be transferred, stored or processed outside of Rwanda, and the 2016 law governing ICT. The regulator cited article 269 of the law governing ICT, which provides for sanctions against a licensee that fails to comply with a regulatory directive. The sanctions specified in the article include an administrative fine of between FRw 500,000 and 15 million (USD 499-14,960) for each day of non-compliance; imposition of additional conditions on the operator's license; suspension of a license for a specified period; and, revocation of a license.

In November 2017, Tunisia's data protection authority instituted proceedings against OVH Tunisie, a subsidiary of the French cloud computing company OVH on allegations of infractions related to data location.[124] In a lawsuit before the public prosecutor, the National Authority for the Protection of Personal Data (INPDP) said the company did not disclose to its Tunisian customers where their data was stored nor got their consent. Furthermore, that OVH transferred data from Tunisian customers abroad without requesting authorisation from the INPDP in violation of article 52 of the data protection law.[125]

123 *INPDP Report https://thd.tn/linpdp-apporte-des-precisions-sur-laffaire-dovh-tunisie/*

124 *State of Surveillance Tunisia, https://privacyinternational.org/state-privacy/1012/state-surveillance-tunisia*

2.4 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 to protect the personal information of individuals in accordance with international human rights law and standards. Further, these laws should include privacy principles,[126] provide effective remedies, and adequate oversight for the protection of personal information.

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 in the recent past 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.

Despite some positive provisions, there are several negative sections within many countries' legal frameworks. In several 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.

Cameroon

Article 2 of Decree No. 2016/375 of 04 August 2016 on the National Identity Card[127] establishes a computerised, biometric and personal National Identity Card (NIC), which contains an electronic chip. The personal data collected includes names, birth date and place, gender, height, picture, signature, fingerprints, special signs like scars or beauty spots on the holder's body, address, and parents' names.[128] The biometric NIC is valid for ten years and contains a permanent Unique ID Number. Article 84 of the Law No. 2012/001 of April 19, 2012 on the Electoral Code establishes a "permanent biometric personal Voter's Card" which carries the names, date, place of birth, parentage, photo, fingerprints, profession and address of the holder.[129]

Article 17 of Decree No. 2015/3759 on the identification of subscribers[130] requires that "operators of telecommunications networks and ISPs take appropriate measures to ensure the protection, integrity and confidentiality of the identification data they hold or process, as well as the information they hold on the location of customers subscribed to their networks.[131] The law also requires the telecoms regulatory agency to ensure the confidentiality of subscribers' identification data that it accesses. Article 6 of the Decree requires subscribers to provide their original national identity card, their exact address including location map, and the international mobile equipment identity number (IMEI) of their device. This is in line with article 55 of the eCommunications Act. SIM card registration has been in force in Cameroon since 2016. In 2019, the telecoms regulator ART sanctioned mobile operators (Orange, MTN and Nexttel) with fines totalling CFA 3.5 billion (USD 5.9 million) for failure to comply with SIM card registration rules.

Laws on SIM card registration hold companies and their agents liable if customers' information is misused. Cameroonian law prescribes penalties for violations of personal data and the privacy of individuals: six months to five years imprisonment or fines ranging from one million to 50,000,000 CFA francs (USD 1,854-92,714), or both. The specified violations include processing of personal data.

126 *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.*

127 *Cameroon, Decree No. 2016/375 of 04 August 2016 on Characteristics and Methods of Establishing and Issuing the National Identity Card, https://bit.ly/3yz9IyF*

128 *Id., Article 3 (a) (b).*

129 *Cameroon, Law No. 2012/001 of April 19, 2012 on the Electoral Code, https://bit.ly/3ikeDOf*

130 *Decree No. 2015/3759 on the identification of subscribers and terminal equipment of eCommunications networks, https://bit.ly/3tXSkkb*

131 *Decree No. 2015-0265 / P-RM on procedures for identifying subscribers to telecommunications / ICT services open to the public, https://tinyurl.com/42dk29j2*

Ethiopia

Ethiopia has required mandatory SIM card registration for several years. According to the SIM Card Registration Directive No. 799/ 2021, all SIM card subscribers must be registered, and the telecoms regulator is required to establish and maintain a database of all registered subscribers' information referred to as the National Subscriber Registry.[132] Article 8(1) provides that the minimum information and documents be required for SIM card registration are the full name as it appears on a residence identification card, a driver license, or passport; nationality; date of birth; gender; physical address; postal address (where applicable); recent photograph; and "any biometric data, if available." Telecom operators or their agents require subscribers to provide a residence identification card, driver's license; or passport to verify their identities.

Article 14 states that telecommunications operator shall grant the Authority access to their systems, premises, facilities, files, records, and other data to enable the regulator to undertake regulatory audit and ensure the effective compliance with the regulation at any given time.

Moreover, the Licensing and Authorisation of Payment Instrument Issuers Directive requires payment instrument issuers to report to the NBE any cyber security breach or data loss. The consent of the data subject is required in order to process certain personal data, unless it is legally permitted to do otherwise. For example, under article 5.4.7 of the Financial Consumer Directive, a financial service provider should only use and disclose financial consumer's and security provider's data consistently with the original purpose of collection or with the explicit and informed consent of the financial consumer or otherwise required or permitted by the Financial Consumer Protection Directive or other laws.

Kenya

Section 44 of the Data Protection Act, 2019 prohibits the processing of sensitive personal data such as biometric information. It only permits it where the principles of data protection under section 25 are complied with, and the conditions imposed under section 45 such as legitimacy and necessity are observed.[133] Also, rule 16 of the Kenya Information and Communication (Registration of SIM card) Regulations, 2015 requires telecommunications operators to take all reasonable steps to ensure the security and confidentiality of subscribers' registration particulars.[134]

The Kenya Information and Communications Act (Registration of SIM cards) Regulations, 2015 under rule 4 requires all mobile network providers to register all SIM card subscribers.[135] The failure to provide the information is an offence punishable under the regulations, by a fine of KES 300,000 (USD 3,000) or to imprisonment for a term not exceeding six months, or both.[136]

The Elections Act allows for the biometric registration of voters to capture a voter's fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures in the integrated electronic electoral system that enables biometric voter registration, electronic voter identification and electronic transmission of results.[137]

132 *SIM Card Registration Directive No. 799/ 2021, https://eca.et/wp-content/uploads/2021/07/SIM-Card-Registration-Directive-No.-799-2021English.pdf*

133 *Data Protection Act, 2019, http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf*

134 *Kenya Information and Communication (Registration of SIM-card) Regulations, 2015 https://ca.go.ke/wp-content/uploads/2018/02/Registration-of-SIM-%E2%80%93Cards-Regulations-2015-1.pdf*

135 *Regulations https://ca.go.ke/wp-content/uploads/2018/02/Registration-of-SIM-%E2%80%93Cards-Regulations-2015-1.pdf*

136 *Regulations https://ca.go.ke/wp-content/uploads/2018/02/Registration-of-SIM-%E2%80%93Cards-Regulations-2015-1.pdf*

137 *Elections Act, https://www.iebc.or.ke/uploads/resources/kqI5cmgeyB.pdf*

Kenya's Statute Law (Miscellaneous Amendments) Act, 2018[138] amending the Registration of Persons Act, created the National Integrated Identity Management System (NIIMS) that was intended to be a single source of personal information, including biometric data of all Kenyans as well as foreign residents in Kenya. Dubbed the "Huduma Namba," the Digital ID programme was challenged in court and the government barred from making registration mandatory, tying access to government services on Huduma Namba enrolment, collecting DNA and GPS information, and sharing data between agencies and third parties in the absence of an appropriate legal framework.[139] Notably, the two draft regulations proposed by the government to implement NIIMS have also been criticised for failing to provide explicit safeguards for the collection, processing, use, and transfer of personal information in line with the Data Protection Act, 2019 and international human rights laws and standards.[140]

Following public interest litigation, the government was ordered to proceed with implementing the Huduma Namba[141] biometric project on condition that an "appropriate and comprehensive regulatory framework" on the implementation is enacted.[142] The government has since published the Huduma Bill, 2019,[143] the draft Registration of Persons (National Integrated Identity Management System) Regulations, 2020,[144] and the draft Data Protection (Civil Registration) Regulations, 2020[145] for public engagement in its bid to comply with the court orders as the Huduma Namba cards are rolled out. The draft regulations describe the NIIMS structure and propose safeguards to entrench the rights of data subjects, the obligations of data collection entities, the principles to be upheld, and the standards to be observed to ensure the security of personal data. However, in October 2021, the High Court quashed the decision by the state to roll out Huduma Namba cards, holding that the rollout of the cards was illegal owing to the states failure to conduct a data protection impact assessment prior to rolling out the cards.[146]

Malawi

Malawi is yet to enact the Data Protection Bill, which underwent public consultations in February 2021.[147] Section 44 of the National Registration Act, 2010 provides for confidentiality and prohibits the disclosure of information recorded in the register except in accordance with and for specific purposes of the Act, or during any judicial proceedings. Under section 44(2), the Minister may furnish any information concerning any person whose name or particulars are registered under the Act to any Ministry, local authority, or body for any purpose of that Ministry, local authority, or body.

Section 92 of the Communications Act, 2016 provides for mandatory registration of generic numbers and SIM cards. The information required for registration includes full name, identity card number, residential and business or registered physical address. Further, licensees or distributors shall, before filling in particulars of the potential subscriber, verify the subscriber's information; and retain, either hard copy or electronically, all certified copies of the documents obtained.

138 *Statute Law (Miscellaneous Amendments) Act, 2018, http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2018/StatuteLawMischellaneousNo18of2018.pdf*

139 *Kenya's National Integrated Identity Management System, https://www.justiceinitiative.org/uploads/8f3b665c-93b9-4118-ad68-25ef390170c3/briefing-kenya-nims-20190923.pdf*

140 *Kenya: Digital identity regulations must satisfy constitutional requirements, https://www.article19.org/resources/kenya-digital-identity-regulations-must-satisfy-constitutional-requirements/*

141 *Huduma Namba https://www.hudumanamba.go.ke/*

142 *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR, http://kenyalaw.org/caselaw/cases/view/189189/*

143 *Huduma Bill https://www.ict.go.ke/wp-content/uploads/2019/07/12-07-2019-The-Huduma-Bill-2019-2.pdf*

144 *Registration of Persons (National Integrated Identity Management System) Regulations https://ict.go.ke/wp-content/uploads/2020/02/THE-REGISTRATION-OF-PERSONS-NATIONAL-INTEGRATED-IDENTITY-MANAGEMENT-SYSTEM-REGULATIONS-2020.pdf*

145 *Data Protection (Civil Registration) Regulations, 2020, https://ict.go.ke/wp-content/uploads/2020/02/THE-DATA-PROTECTION-CIVIL-REGISTRATION-REGULATIONS-2020.pdf*

146 *Huduma Namba: Court declares rollout illegal, https://www.the-star.co.ke/news/2021-10-14-huduma-namba-court-declares-rollout-illegal/; Roll out of Huduma card is unlawful, judge rules, https://www.standardmedia.co.ke/national/article/2001426231/roll-out-of-huduma-card-is-unlawful-judge-rules*

147 *Invitation to Comment on the Draft Data Protection Bill, 2021: http://www.pppc.mw/assets/upload/downloads/Notice_-_Data_Protection_Draft_Legislation_Ver_4__2_Feb.pdf*

The National Registration and Identification System (NRIS), which is being used for biometric data collection and its processing, has been centralised in Malawi since 2017. The NRIS is linked to voter registration, revenue collection, immigration, SIM card registration, and banking, as well as financial inclusion programmes. This has made it even more crucial to have strong regulations to protect personal data privacy.[148] Starting March 2021, the system has been used to support the Covid-19 vaccine rollout. The NRIS has been described as having been rolled out at "breakneck speed", without due regard for human rights.

Mali

In Mali, Decree No. 014 of 09/01/88 establishing and regulating the issuance of the Identity Card and the Consular Card article 61 of Law N. 2018-014 of 23 April 2018[149] institutes a personal and non-transferable biometric voter card, the falsification of which is prohibited. This card is then used with the photo, fingerprint and / or National Identification Number (NINA) of its holder for registration on the electoral roll.[150] Following alignment with the ECOWAS biometric national identity card system,[151] Mali has instituted biometric data collection including fingerprints, picture, height and complete address, to establish the national ID card.[152]

Article 8 of the Decree No. 2015-0265/ P-RM of April 10, 2015 on the procedures for identifying subscribers of telecommunications/ICT services requires that operators of telecommunications networks and ISPs take appropriate measures to ensure the protection, integrity and confidentiality of the identification data they hold or process, as well as the information they hold on the location of customers subscribed to their networks.[153] All communications operators are required to register all SIM cards under article 3 of the decree.

Article 43 of the Law n° 2019-056 of 05 December 2019 on the Suppression of Cybercrime punishes by imprisonment of between two and five years, a fine of two million to 30 million CFA francs (USD 3,618-54,262) or both, "anyone who sets up a stolen access to data or an information system without the authorisation of the legitimate user." Further, under article 26, eCommunications service providers who fail to retain data allowing the identification of their clients can be imprisoned for between six months and two years, fined between 500,000 and two million CFA francs (USD 362-3,618), or both. Meanwhile, the law on the identification of users of telecom services provides for mandatory SIM card registration, and in article 6 requires cybercafé managers to keep a register indicating the names of all clients, the workstations used, the day, the hour and the duration of the connections used.

Nigeria

Some legislation in the country contains provisions to protect biometric data, including the rights of data subjects. For example, section 14 and 15 of the National Identity Management Commission (NIMC) Act of 2007[154] requires that details of persons in the database shall be identified using unique and unambiguous features such as fingerprints and other biometric information. The NIMC is also required to ''ensure the preservation, protection, sanctity, and security (including cybersecurity) of any information or data collected, obtained, maintained or stored in respect of the National Identity Database.''

148 *Data Protection Law on the Horizon in Malawi, https://cipesa.org/2021/06/data-protection-law-on-the-horizon-in-malawi/*

149 *Law No. 2016-048 of October 2016 on the Electoral Act, amended with Law No. 2018-014 of 23 April 2018; https://bit.ly/2TVLL5t*

150 *Id.; Article 35.*

151 *ECOWAS biometric identity card program to launch in 2016, https://tinyurl.com/eu2fzb2j*

152 *https://demarchesadministratives.gouv.ml/demarches/afficher/Carte-Nationale-d-Identite-demande*

153 *Decree No. 2015-0265 / P-RM on procedures for identifying subscribers to telecommunications / ICT services open to the public, https://tinyurl.com/42dk29j2*

154 *National Identity Management Commission Act 2007, https://www.nimc.gov.ng/docs/reports/nimc_act.pdf*

Nigeria also conducts mandatory SIM card registration and biometric data collection related to identification. Section 27 of the NIMC Act makes digital identity registration mandatory before citizens can access several public services, yet Nigeria does not have a substantive data protection law. In November 2011, the Nigeria Communications Commission (NCC) issued the Communications Commission (Registration of Telephone Subscribers) Regulations (2011), which require mobile phone subscribers to allow their fingerprints and a biometric map of their faces to be collected and registered to their SIM card, which are then stored in a central government database.[155] In 2013, the NCC issued a directive to all cyber cafe owners and operators to register and maintain a database of users of their services. Cybercafé operators were to register users' full names, physical addresses, telephone numbers, and to take their passport photos and telephone numbers.[156]

Section 28 of the NIMC Act provides penalties for unauthorised access of the national database and a refusal to give information to the NIMC. Section 29 fines individuals and corporate bodies who carry out transactions without a national identification number . The offences attract a ₦100,000 (USD 263) fine or six months imprisonment, or both.

Senegal

Article 20 paragraph 5 of the law on data protection provides for the "processing of personal data including biometric data" after authorisation from the Personal Data Commission. Under clause 122 of the Personal Data Protection Bill of 2019 which is expected to replace the current data protection law of 2008, establishes the principle of the legitimate installation of biometric devices, while clause 123 lays down the principle of proportionality in the collection of biometric data. Clause 128 of the bill prohibits the collection of biometric data.

Senegal requires mandatory SIM card registration[157] which is overseen by the Regulatory Authority for Telecommunications and Posts (ARTP), and the data is linked to the national identity database. However, there have been numerous reports of non-compliance with the data protection law and the Commission of Personal Data (CDP) regulations.[158] Moreover, Senegal is known to be among the countries that controversially seek users' data from intermediaries.[159]

South Africa

Under the 2002 Regulation of Interception of Communication Act (RICA), all SIM cards, whether used in a mobile phone voice or for data, must be registered with the state via the service provider. According to section 41 of RICA, prior to SIM card activation, a South African citizen must provide his or her name, address and identity number. For non-citizens, a name, address and passport number are required.[160]

Section 33 of POPIA deals with, among others, authorisation concerning a data subject's biometric information. Because of its provisions, section 16(5) of the Electoral Laws Amendment Bill was amended to require the redaction of personal information from the voters' roll to ensure only the voter's date of birth, citizenship and only some digits of the ID number appear.

155 *NCC Registration of Telephone Subscribers Regulations 2011, https://tinyurl.com/wwjoh99*

156 *Cyber Cafes in Nigeria Asked to Register Users to Help Fight Cyber Crime, https://tinyurl.com/vsuo6da*

157 *L'artp Donne Un Ultimatum De 6 Mois Aux Operateurs, http://mobile.sudonline.sn/l-artp-donne-un-ultimatum-de-6-mois-aux-operateurs_m_29793.htm*

158 *Avis Trimestriel N° 01-2021 De La Commission De Protection Des Donnees Personnelles Du Senegal (Cdp) https://www.cdp.sn/content/avis-trimestriel-n%C2%B0-01-2021-de-la-commission-de-protection-des-donnees-personnelles-du-0*

159 *SENEGAL: UPR Session 31 Digital Rights Advocacy Briefing Document, https://cipesa.org/?wpfb_dl=291*

160 *State of Privacy South Africa, https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa*

Tanzania

The Electronic and Postal Communications (SIM Card Registration) Regulations, 2020 requires mandatory SIM card registration. Section 19 of the Registration and Identification of Persons Act imposes a duty on the Registrar, Registration and Immigration Officers not to disclose photographs and fingerprints collected, except with the written permission of the Minister. It is not possible to register a SIM card unless the biometric information collected is verified against the National Identification Authority (NIDA) database. In turn, "public institutions have moved to make the National ID or NINs (as the NIDA ID is commonly referred to) as primary or mandatory requirement for identification for service provision, including institutions like the Higher Education Loans Board, the Tax Revenue Authority, Business Registration, Licensing Authority and the Government Recruitment Agency."[161]

Regulation 20 of the SIM card regulations prohibits the misuse of information of a customer collected during the registration of SIM cards by the licensee, stating that, "Any licensee, dealer or agent who misuses information of a customer for SIM card registration commits an offence and upon conviction shall be liable to a fine of not less than five million TZS or imprisonment for a term not less than 12 months or both. Further, the SIM card registration law holds companies and their agents liable if customers' information is misused.

Uganda

Section 9 of the Regulation of Interception of Communications Act (RICA), 2010 requires telecommunication service providers prior to entering into contract with any person, to obtain their biometric information and any other information that service provider deems relevant.[162] In turn, section 9(2) of RICA requires telecommunication service providers to ensure that subscribers register their SIM cards. The registration of SIM cards was made mandatory in Uganda in 2012 following a campaign by the communications regulator, arguing that the exercise was necessary to curb crime by enabling the tracking of criminals and identification of SIM card owners.

The Data Protection and Privacy Act, 2019 lists several offences such as obtaining or disclosing personal data in an unlawful manner (section 35) that is punishable by a fine of UGX 4.8 million (USD 1,327) or imprisonment for 10 years or both. Additionally, the Registration of Persons Act, 2015[163] provides additional sanctions for breach of personal data. For example, under section 81, a registration officer or any other officer of the National Identification and Registration Authority (NIRA) who without authority discloses, submits, or transfers data from the register to any other person, commits an offence and is liable on conviction to a fine not exceeding UGX 1.44 million (USD 408) or imprisonment not exceeding five years or both.

Under the Registration of Persons Act, the National Identification and Registration Authority (NIRA) which is established by section 4, is charged with, among others, creating, managing, maintaining and operating the National Identification Register under section 5. This function extends to registering citizens and non-citizens who are lawfully resident in the country, registration of births (sections 28—40) and deaths (sections 41—48), assigning a unique national identification number to every person registered in the register and issuing national identification cards and aliens identification cards. This information includes names, places of birth, gender, age, residential address, religious beliefs, profession and places of employment.

161 *Tanzania: NIDA IDs for civic services, or not? https://www.africaportal.org/features/tanzania-nida-ids-civic-services-or-not/*

162 *Regulation of Interception of Communications Act, 2010, http://www.ulrc.go.ug/system/files_force/ulrc_resources/regulation-interception-communications-act-2010.pdf?download=1*

163 *Registration of Persons Act, 2015, https://www.ict.go.ug/wp-content/uploads/2018/06/Registration-of-Person-Act-2015.pdf*

Zimbabwe

In May 2021, Zimbabwe government announced that the cabinet had approved the engagement of a private partner in implementing a National Biometric Database for the production of e-passports, national IDs and birth certificates.[164] The country introduced a biometric voter registration (BVR) ahead of the 2018 elections.

The Postal and Telecommunications Regulations Statutory (POTRAZ) Instrument 95 of 2014 (Subscriber Registration) of Zimbabwe requires all telecommunications companies to create a centralised subscriber database of all their users.[165] Section 4 of the regulations requires telecommunications companies, at their own cost, to implement a system to obtain, record and store where the customer is a natural person: their full name; permanent residential address; nationality; gender; subscriber identity number; national identification number; or passport number. Where the customer is a legal person, to record or store: a copy of certificate of registration or incorporation or business licence; the full names, surname, national identification number and an address of the authorised representative of the legal person; the name and address of the juristic person and, where applicable, the registration number of the legal person; and subscriber identity number.

The database is managed by POTRAZ who claim to use it, among other things, to assist law enforcement agencies for safeguarding national security, as well as authorising access for the purposes of research in the sector. In June 2016, the government through POTRAZ issued threats to the public, highlighting the fact that perpetrators of "abusive and subversive materials" would be identified, disconnected and arrested.

Section 14 of the Cyber Security and Data Protection Bill prohibits the processing of genetic, biometric and health data without an individual's consent, which can be withdrawn by the data subject at any time without providing any reasons.

164 *Zimbabwe's Big Brother technology is a threat to digital rights https://www.africaportal.org/features/zimbabwes-big-brother-technology-threat-digital-rights/*

165 *Statutory Instrument 142 of 2013 "Postal and Telecommunications (Subscriber Registration) Regulations, 2013".*

3 Oversight Mechanisms

The Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019 provides for oversight mechanisms in the context of access to information and privacy and data protection. Firstly, principle 34 provides 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." Secondly, principle 41(3) requires states to among others, ensure that any law authorising targeted communication surveillance provides adequate safeguards for the right to privacy including effective monitoring and regular review by an independent oversight mechanism. Similarly, principle 42 requires states to adopt laws for the protection of personal information of individuals in accordance with international human rights law and standards by among others, providing for independent oversight mechanisms for the protection of communication and personal information.

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 the executive arm of government, and especially by state security agencies. Also, the laws in most countries require judicial authorities to issue warrants for the interception of communications. However, in some countries interception orders can be issued by non-judicial officials, such as ministers. Yet in others there is significant oversight power invested in the judiciary.

Cameroon

Judicial authorities in Cameroon have various powers with respect to privacy and data protection. For example, they are empowered to request for and access communication data from providers, the conversion of encrypted text, and facilitate and enforce foreign judicial assistance requests. Article 7(2) of the 2010 law on cybersecurity places surveillance oversight under the National Agency of ICT (ANTIC) and empowers it to "ensure surveillance, detection and information on computer and cybercrime related risks." The ANTIC is under the technical supervision of the Ministry of Posts and Telecommunications and the financial supervision of the Ministry of Finance, and as such is not entirely independent.

Moreover, the mandate of ANTIC to regulate "the use of ICT, respect for ethics, as well as the protection of intellectual property, consumers, good manners and privacy"[166] conflicts with the role of the Telecommunications Regulatory Agency (ART) which is in charge of regulation, control and monitoring of the activities of operators and electronic communications services providers;[167] "guaranteeing consumer protection";[168] and the identification system for subscribers of electronic communications terminals."[169]

166 *Decree No. 2012/180 on the organisation and functioning of ANTIC, in accordance with article 90 paragraph 2 of the law governing electronic communications in Cameroon, Article 5, https://tinyurl.com/y7kss2sx*

167 *Law n ° 2010/013 of December 21, 2010 on electronic communications in Cameroon as amended by Law 2015-06 of April 20, 2015; section 36, Paragraph 1.*

168 *Id. Paragraph 2.*

169 *Decree No. 2015 / 3759 on procedures for identifying subscribers and terminal equipment of electronic communications networks; op. cit.*

Chad

Section 4 of Cybersecurity and Cybercrime Act establishes the National Agency for Computer Security and Electronic Certification (ANSICE) as an independent national authority responsible for ensuring the application of the law on Cybersecurity and Cybercrime. The ANSICE is responsible for ensuring the implementation of the Personal Data Protection Act.[170]

Ethiopia

The draft Data Protection Proclamation 2021 provides for a regulatory entity called the Data Protection Commission.[171] The Communications Service Proclamation grants power to the Ethiopian Communication Authority to approve information security, data privacy, and protection. As a result, it is permitted to introduce directives in order to ensure that the benefits of consumers of communication services are protected as per article 50(1) of the Communications Service Proclamation.

Article 9 of the Authentication and Registration of Documents Proclamation imposes a duty of secrecy and prohibits notaries from providing information to third parties except in compliance with a court order or upon request by other bodies authorised by law.[172] However, the notary has the duty to report to the appropriate organ if it accesses information connected to the commission of a crime.

Kenya

Under section 50 of the National Intelligence Service Act, a person aggrieved by the issuance or extension of an interception warrant may appeal to the High Court within 14 days of the issuance or extension of the warrant. Similarly, section 55 of the Computer Misuse and Cybercrimes Act permits a person aggrieved by any decision or order made by a court to appeal to the High Court or the Court of Appeal within 30 days of the decision. The Prevention of Terrorism Act does not provide a similar right of appeal. Further, there is no obligation in any of these laws, to notify a subject of a warrant of such orders.

Moreover, the Data Protection Act grants a data subject aggrieved by a decision of any person under the Act to lodge a complaint with the Data Protection Commissioner, either orally or in writing. Such complaints may be investigated within 90 days, and if the complainant suffered damages, the data subject is entitled to compensation from the data controller or data processor, as specified under section 65 of the Act.

Malawi

Persons aggrieved by the decision of MACRA may apply to the High Court within thirty days of the decision for judicial review. Clause 8 of draft Data Protection Bill, 2021 proposes to establish a Data Protection Office as a unit under MACRA responsible for the activities of the Authority in relation to data protection under the Act. Further, clause 39 of the draft Bill provides that a data subject who is aggrieved by the decision, action or inaction of a data controller or data processor may lodge a complaint with MACRA. In addition, section 69 of the Electronic Transaction and Cyber Security Act empowers MACRA to appoint Cyber Inspectors "to monitor and inspect any website database with critical data or activity on an information system in the public domain and report any unlawful activity to the authority.

170 *Law n° 06/PR/2015 on the creation of ANSICE; Article 7.*

171 *First structured personal data protection proclamation in the making https://www.capitalethiopia.com/featured/first-structured-personal-data-protection-proclamation-in-the-making/?utm_source=rss&utm_medium=rss&utm_campaign=first-structured-personal-data-protection-proclamation-in-the-making*

172 *Authentication and Registration of Documents Proclamation http://extwprlegs1.fao.org/docs/pdf/eth135124.pdf*

Mozambique

In Mozambique, article 11-12 of the Electronic Transactions Act, 2017, grants the mandate to implement the law to the National Institute of Information and Communication Technologies (INTIC).

Nigeria

Regulation 20 of the Nigeria Lawful Interception of Communications Regulations 2019,[173] provides that any person or Licensee who is aggrieved by any interception activity shall in writing notify the Nigeria Communications Commission (NCC) and may make a formal application to the Federal High Court for judicial review. The provision also states that "Every decision or direction on interception of Communications shall subsist and remain in force until it is set aside by a Court of competent jurisdiction in a final decision of the court."

In addition, clause 21 of the Data Protection Bill 2020[174] makes the right to judicial remedy by data subjects possible. Moreover, clause 29 allows the compensation of data subjects for the failure of data controllers to comply with the Bill, while clause 57 lays out the procedure for lodging lawsuits against the Commission.

South Africa

In South Africa, the Information Regulator, established under section 39 of the Protection of Personal Information Act (POPIA), administers both the privacy and access to information legislations. The regulator has a wide range of powers and functions regarding the right to privacy, including developing regulations and guidelines. However, POPIA does not ordinarily apply to processing for national security purposes, provided that such laws contain adequate safeguards for data protection. In terms of surveillance, the Inspector General of Intelligence and the Joint Standing Committee on Intelligence are in charge of implementing surveillance activity subject to application to and authorisation by a judge.

Tanzania

The Tanzania Communication Regulatory Authority (TCRA) is responsible for licensing and regulating the ICT sector. In addition to licensing, TCRA monitors licensees and is mandated to receive complaints arising from ICT service providers. Persons aggrieved by decision of Authority may appeal to the Fair Competition Tribunal.

Tunisia

In Tunisia, article 15 of the data protection law requires the processing of personal data to be subject to the authorisation of the National Authority for Protection of Personal Data, with the exception of data related to health.[175] According to the law regulating the importation and commercialisation of encryption systems for telecommunications networks, the National Agency of Digital Certification is responsible for approval of the importation and sale of such systems.[176]

Uganda

In Uganda, the only oversight measures on surveillance stipulated are the requirement for a judge to issue an interception warrant, and they do not require submission of annual reports to any oversight authority. The Registration of Persons Act under section 83(2) provides that a person who is dissatisfied with a decision of the committee established under section 83(1)(a) may appeal to the High Court. The data protection law establishes a personal data protection office headed by the national personal data protection director, under the National Information Technology Authority - Uganda (NITA-U).

173 *Lawful Interception of Communications Regulations 2019, https://www.ncc.gov.ng/accessible/documents/839-lawful-interception-of-comunications-regulations-1/file*

174 *Data Protection Bill 2020, https://nimc.gov.ng/docs/Draft_Data_Protection_Bill_2020.pdf*

175 *Organic Act n°2004-63 of July 27th 2004 on the protection of personal data, https://media2.mofo.com/documents/The+Organic+Act+2004-63.pdf*

176 *Decree N° 2008-2639, http://www.certification.tn/sites/default/files/reglementations/Decret2639-2008Fr.pdf*

Zambia

In Zambia, complaints relating to privacy breaches may be made to the Zambia Human Rights Commission, the High Court or the Constitutional Court, Zambia ICT Authority (ZICTA), the Ministry of Transport and Communication, and the National Cybersecurity Advisory Coordinating Council. Appeals from the decisions of ZICTA fall to the ICT Minister, and subsequently the High Court.

Zimbabwe

Zimbabwe's Interception of Communications Act (2007) provides for oversight of the warrants by the Prosecutor-General. Section 19 states 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." Further requests for additional information can be made, and recommendations made by the Prosecutor General. However, there is no provision for the publishing of the report, neither are there any other additional mechanisms for transparency and accountability. At present, both the Minister and the Prosecutor General in Zimbabwe are presidential appointees.

4 Discussion and Recommendations

4.1 Discussion

A review of various African laws related to the right to privacy, shows notable progress and at the same time, key policy gaps that will require attention if citizens are to enjoy their rights and freedoms online, as outlined in the Declaration. Many of the laws and policies reviewed fail to uphold international human rights standards, and to establish clear and appropriate mechanisms for oversight, redress and remedy.

4.1.1 Growing Surveillance

Principle 41(3) of the Declaration provides that countries "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..." States are also required to ensure that laws authorising targeted communication surveillance provide adequate safeguards for the right to privacy, including the prior authorisation of 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.

Indeed, "national security" considerations have been employed in laws in various countries to broadly 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.[177] Notably, Rwanda references its interception of communications law in the preamble of the Cybersecurity Regulation of 2020 that requires local data hosting. What is of great concern is that in many African countries, security agencies are known to abuse 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, and 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. In Ethiopia, the Attorney General can give a 48-hour interception order.

Kenya published a draft National CCTV Policy in 2019, while Zambia is reportedly in the process of developing CCTV regulations. However, some countries such as Uganda, which have implemented wide-scale video surveillance (CCTV) programmes while also planning to introduce mandatory vehicle surveillance, lack such regulations or policies and are yet to indicate any plans to develop them. Senegal's 2019 Data Protection Bill introduces the principle of the legitimate installation of biometric devices, while also laying down the principle of proportionality in the collection of

177 *Elias Biryabarema, "MTN Uganda says government security personnel raided its data center," Reuters, July 6, 2018, https://www.reuters.com/article/us-uganda-mtn-group-idUSKBN1JW1Q5*

biometric data. These two areas (video surveillance regulations and policies around installation of biometric devices) are indicative of gaps in the existing legislation that countries will need to be addressed in the coming years.

Many 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. One of the areas of concern is the period of validity of warrants. Notably, Tanzania's cybercrime 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 notes 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 increase the validity for a period of three months. In Zambia, the validity of the interception order is three months and can be renewed by a judge for a period of their discretion. Uganda's validity period is also three months and may be renewed by a judge for a non-specified period. Cameroon offers a maximum validity period of four months, per article 245(4) of the 2010 cybersecurity law.

4.1.2 **Limitation 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 encryption protect privacy, and without effective protection of the right to privacy, the right of individuals to communicate anonymously and without fear of their communications being unlawfully detected cannot be guaranteed.[178] 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.[179] Yet governments are increasingly restricting the use of these privacy tools because they fear these will hamper their capacity to fight terrorism and crime.[180] This continues despite laws, practices and policies that ban, restrict, or otherwise undermine encryption and anonymity significantly and disproportionately violate the rights enshrined in of the African Charter and article 19 of the International Covenant on Civil and Political Rights (ICCPR) as well as national constitutional guarantees.[181]

In all countries studied there is mandatory SIM card registration, during which a horde of identifying data, including biometric information, are collected. Telecom companies, regulators, and other government agencies (sometimes including those in charge of national identification and electoral processes) are increasingly collecting biometric data, creating various databases. Of recent, many government entities have been pegging service delivery 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,[182] SIM registration, in effect, eradicates the ability of mobile phone users to communicate anonymously and in the absence of proper oversight, facilitates mass surveillance, making tracking and monitoring of all users easier for law enforcement and security agencies.

The research shows that many countries studied require the registration of encryption services providers. In Chad, Malawi, Senegal, Tanzania, Tunisia and Zambia, there are penalties for offering cryptographic services without licensing, registration or authorisation. Further, the interception of communications provisions often require service providers to decrypt any encrypted information that they may intercept in the course of offering assistance to law enforcement. In countries such as Mali and Tanzania, the laws require the encryption services providers, upon

178 *Amnesty International, 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*

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

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

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

182 *Supra note 185*

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.

4.1.3 **Data Localisation**

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 ensured in the recipient country or international organisation.

Some countries have specified the data that cannot be exported without authorisation. Kenya specifies all public data; Nigeria specifies 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.

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 host its data locally. 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 or curtailing citizens' privacy rights. Notably, the growing appetite for state surveillance could be a key driver towards the adoption of data localisation laws. Hosting data locally could grant state surveillance apparatus in some countries in the region 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. Likewise, hosting data locally may enable local innovation and spur investments in local ICT and hosting infrastructure if the right incentives for investment, the requisite skills, and enabling provisions on access to data and data use and reuse, are in place.

4.1.4 **Common Gaps in the Privacy**

4.1.4.1 Weak Oversight Provisions

The Declaration requires that notification of surveillance should be done "within a reasonable time of the conclusion of such surveillance." However, in many 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. In South Africa, the Constitutional Court found in February 2021 the regulation of interceptions law was unconstitutional for failing to among others, provide for notification of the subject of surveillance of the fact of their surveillance as soon as the notification could be given without jeopardising the purpose of surveillance after surveillance has been terminated; and for not adequately providing safeguards to address the fact that interception directions are sought and obtained ex parte.

In addition, most interception orders in Africa are granted to law enforcement agencies ex parte, with a requirement that the intermediaries facilitating them keep the orders confidential. Consequently, where the laws are silent on notification or the appeal processes, such appellate processes are rendered meaningless as notices are never issued to subjects of interception, which weakens the due process safeguards. 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. Also, 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. Under Nigeria's cybercrime law, a law enforcement official has the power to access data from service providers without obtaining a warrant. In Zambia, interception orders can also be made orally without warrants. Meanwhile, under Ghana's Electronic Transactions law and Tanzania's Cybercrimes Act, law enforcement officers can seize computers and electronic equipment. These interception methods weaken oversight mechanisms provided and could provide an easy path or justification for law enforcement agencies to by-pass the stringent requirements required for seeking and obtaining court warrants.

4.1.4.2 Poor Accountability and Transparency Provisions

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 such as is in Nigeria, Tunisia, Rwanda, and Zimbabwe is lacking in most other countries' laws. Such accountability requirements, especially where 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. However, while these oversight and accountability provisions are commendable, there is no proof that these provisions are implemented in practice. 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, the reports are categorised as classified information under state secrecy laws. Thus, the public and oversight institutions in some of the countries such as data protection authorities and parliaments remain in the dark about the extent and legality of the conduct of surveillance in the respective countries.

4.1.4.3 Severe Criminal Sanctions for Breach

Many of the laws and policies reviewed provide for sanctions and penalties for illegal surveillance, the failure by service providers to comply with court orders, or to facilitate state surveillance. Illegal surveillance is penalised in all countries, and this includes prohibiting service providers from engaging in random monitoring of customers' communications. The sanction for unauthorised surveillance varies and includes in Uganda (USD 667 fine, five years imprisonment, or both), Tunisia (USD 365-1,823), Zimbabwe (USD 4,420, five years maximum, or both), Cameroon (USD 1,845-9,226, or between one and two years), Zambia (five years or a fine), Chad (USD 1,830 to 18,306), and Mali (USD 366 to 91,529).

Meanwhile, operators face stiff sanctions for failing to assist governments in conducting surveillance activities. In Nigeria, penalties for failing to render interception assistance to government agencies can be 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).

4.2 Recommendations

The report reveals a range of gaps in the protection and enforcement of the right to privacy. Various recommendations accrue to the various stakeholders especially the government, civil society and the private sector.

Governments

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 article 9 of the African Charter and with the principles in the African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019.
2. Enact standalone and comprehensive data protection laws which comply with regional and international human rights standards on data protection and privacy through multi-stakeholder involvement and participation in the development processes.
3. Proactively establish independent data protection authorities and independent entities in charge of providing oversight over surveillance and encryption and put in place sufficient administrative, judicial, legislative, budgetary, and practical measures to guarantee their independent operations.
4. Periodically report to the different international human rights treaty body monitoring mechanisms such as the Universal Periodic Review, the Committee on Civil and Political Rights and the African Commission on Human and Peoples' Rights on the status of implementation of national, regional and international laws and the measures taken to guarantee the right to privacy and data protection.

African Commission on Human and Peoples Rights (ACHPR)

1. Require states to report on compliance with the Declaration in their state reports and interrogate the government compliance as part of the state reporting process during the ACHPR Ordinary Sessions.
2. Provide normative guidelines and other best practice tools to guide states in implementing the requirements of article 9 of the African Charter as supplemented by the Declaration, on each of these aspects - surveillance, encryption, data localisation, and biometric data collection.
3. Establish a working group on privacy to support the work of the ACHPR and in particular its Special Rapporteur on freedom of expression and access to information.

Civil Society

1. Advocate for the promotion and protection of the right to privacy and data protection through various advocacy engagements such as media campaigns and building the capacity of civil society players to demand for the right to privacy from governments.
2. Engage in strategic public interest litigation especially through collaborative efforts to challenge laws and measures that violate privacy rights and push for reforms of laws, policies and practices to uphold privacy.
3. Continuously monitor and document privacy rights violations through evidence-based research, and report to the African Commission on Human and Peoples Rights and other human rights monitoring bodies on states' compliance with their obligations.
4. Sensitise the general public on their right to privacy and data protection using information, education and communication materials and the need for personal data protection including through use of encryption, circumvention and anonymisation tools.
5. Investigate and report breaches of privacy to the ACHPR and other treaty body mechanisms such as the Universal Peer Review of the UN Human Rights Council, and UN Special Rapporteurs with mandates over privacy, free expression and related rights.
6. Relentlessly engage in action-oriented advocacy to push States into complying with recommendations and obligations emerging from international instruments and human rights enforcement mechanisms.

Companies

1. Comply with the United Nations Business and Human Rights Principles by conducting human rights impact assessments to ensure that measures undertaken do not harm individual rights to privacy and data protection.
2. Develop, publish and strictly implement internal privacy and data protection policies and best practices in handling customer data so as to guarantee customers' data protection and privacy.
3. Support actors that challenge laws and policies that weaken privacy and data protection and stipulate undue intermediary liability obligations.
4. Develop technologies and solutions and use privacy-enhancing technologies that embed and integrate privacy principles by design and default.

CIPESA

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

+256 414 289 502

programmes@cipesa.org

@cipesaug

facebook.com/cipesaug

www.cipesa.org