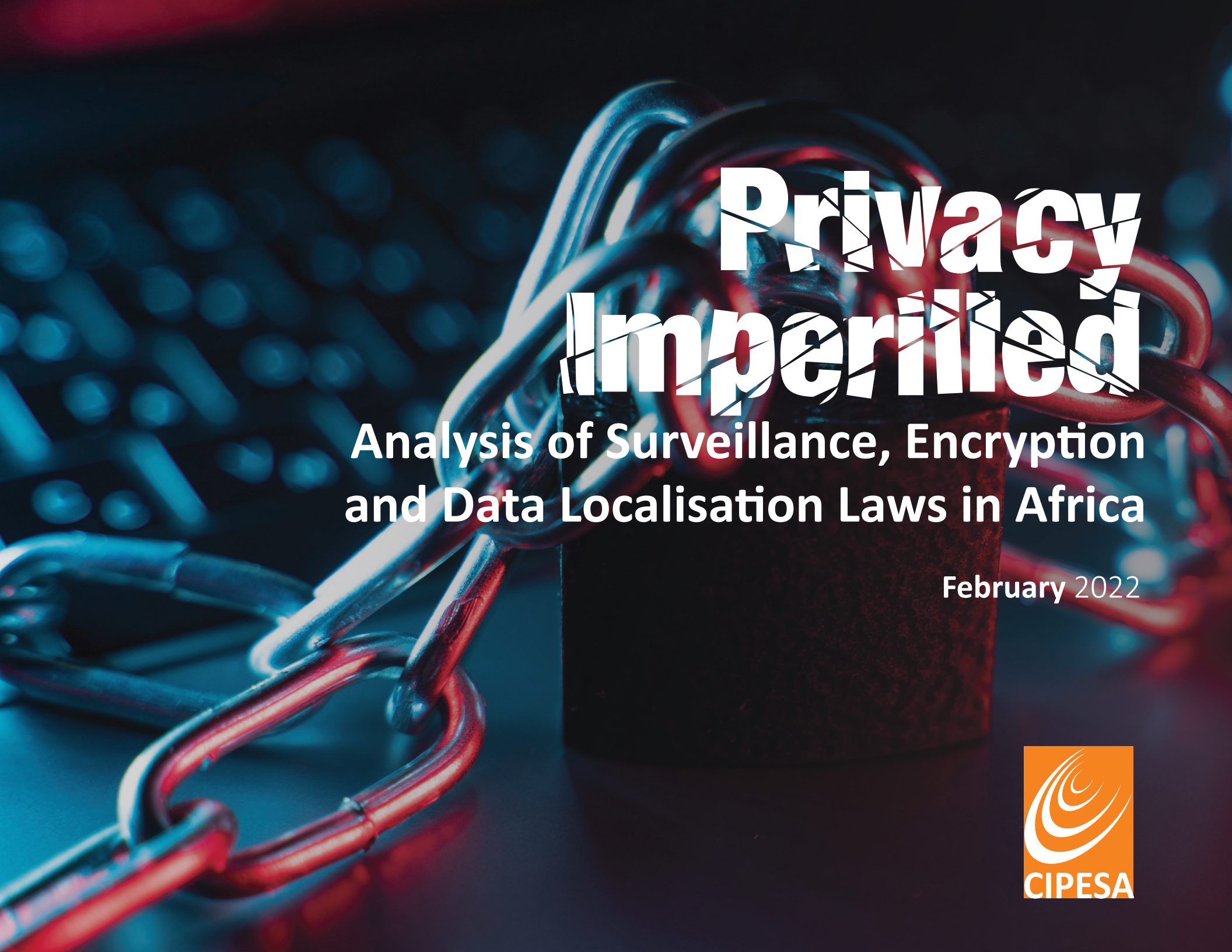


# Privacy Imperilled

## Analysis of Surveillance, Encryption and Data Localisation Laws in Africa

**February** 2022

CIPESA

This report was produced as part of a project that researched privacy-related laws in Africa, which was supported by Meta and the Open Society Justice Initiative. The project also set up the Africa Privacy Tracker portal at *www.privacytracker.africa*, which tracks laws related to surveillance, limitations on encryption, biometric data collection, and data localisation requirements in all African countries. The current study covers 23 countries. A similar study covering 19 other African countries is available at https://cipesa.org/?wpfb_dl=479.

CIPESA appreciates the support rendered by several individuals to this research. They include Ariik Robert Ajack, Alice Aparo, Karel Osiris Coffi Dogue, Afi Edoh, Khattab Hamad, Wremongar Joe, Yosr Jouini, Maxwell Kadiri, Ashnah Kalemera, Abdulai Kallon, Victor Kapiyo, Paul Kimumwe, Lillian Nalwoga, Juliet Nanfuka, Asenath Niva, Jean Paul Nkurunziza, Amreesh Phokeer, Mamothokoane Tlali, Arsene Tungali, Tope Ogundipe, Fabienne Rafidiharinirina, Simone Toussi, Dércio Tsandzana, Wairagala Wakabi, and Edrine Wanyama.

# Table of contents

# 1.0 Introduction

The right to privacy has come under increased attack in many African countries, with the proliferation of digital technologies being matched by state measures that negate this right. In the past few years, many countries across the continent have enacted various laws that permit surveillance, mandate telecommunication intermediaries to facilitate the interception of communication, stipulate the mandatory collection of biometric data, limit the use of encryption, require the localisation of personal data, and grant law enforcement agents broad search and seizure powers.[1]

Such measures have been adopted despite these African countries being signatories to international human rights instruments such as the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights, which provide for the right to privacy in their articles 17 and 12 respectively. At the regional level, the African Charter on Human and Peoples' Rights has no specific provision on the right to privacy, but provides for the respect for a person's dignity.[2] Moreover, the recently revised Declaration of Principles of Freedom of Expression and Access to Information in Africa (the Declaration) of the African Commission on Human and Peoples' Rights (ACHPR)[3] has expressly recognised the right to privacy, most notably in Principle 40, and requires states to adopt legislative, administrative and other measures to give effect to this right. States are also required to report to the African Commission on Human and Peoples' Rights on their compliance with the Declaration in their periodic reviews. Worryingly, while the African Union Convention on Cybersecurity and Personal Data Protection, the continent's model instrument on privacy and data protection, provides safeguards for personal privacy and data protection, it is yet to come into force as most states are yet to sign or ratify it.[4]

Surveillance undermines the privacy of communications and the right to anonymity, and consequently leads to self-censorship and the withdrawal of some individuals and groups from the online public sphere.[5] Yet the right to 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. Many African countries have also passed legislation that limits anonymity and the use of encryption, purportedly to aid governments' efforts to combat terrorism and crime. Other governments limit the use of encryption to enable them to monitor the communications of critical journalists, human rights defenders, and opposition politicians.[6] Similarly, state surveillance is increasingly being used to entrench political control including through spying on activists, journalists, and dissidents.[7]

A related concern is that in several African countries, government agencies are collecting and processing personal data (which increasingly includes biometric data) without adequate data protection laws, amidst limited oversight mechanisms and inadequate remedies.[8] Data localisation requirements and biometric data collection could, in the absence of robust legal and practical safeguards, further facilitate efforts by state and non-state actors to undermine privacy-related rights.

1 *CIPESA, State of Internet Freedom in Africa 2021, https://cipesa.org/?wpfb_dl=467*
2 *African Charter on Human and Peoples' Rights, https://www.achpr.org/legalinstruments/detail?id=49*
3 *Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019,*
4 *African Union Convention on Cybersecurity and Personal Data Protection, "Status List" as at 28th April, 2021,*
5 *CIPESA ibid.*
6 *How African Governments Undermine the Use of Encryption, https://cipesa.org/?wpfb_dl=477*
7 *State of Internet Freedom in Africa 2019: Mapping Trends in Government Internet Controls, 1999-2019*
8 *CIPESA, Mapping and Analysis of Privacy Laws and Policies in Africa Summary Report, https://cipesa.org/?wpfb_dl=454*

This report therefore maps and analyses the laws and policies that impact on privacy, notably those that regulate surveillance, limitations on encryption, data localisation, and biometric databases. This analysis could 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.

## 1.1 Methodology

The research employed a qualitative approach, including legal and policy analysis, literature review and key informant interviews to identify the laws 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 23 countries - Algeria, Angola, Benin, Burkina Faso, Burundi, Cape Verde, the Central African Republic (CAR), Congo Brazzaville, the Democratic Republic of Congo (DRC), Gabon, Guinea Conakry, Ivory Coast, Lesotho, Liberia, Madagascar, Mauritius, Morocco, Niger, Sao Tome & Principe, Sierra Leone, South Sudan, Sudan, and Togo.

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 (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 to 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 specifically.

# 2.0 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 provide for the right to privacy in their articles 17 and 12 respectively. At the regional level, the African Charter on Human and Peoples' Rights has no specific provision on the right to privacy, but provides for the respect for a person's dignity.[9] However, it is significant that the Declaration has expressly recognised the right to privacy, most notably in Principle 40 and requires states to adopt legislative, administrative and other measures to give effect to this right. States are also required to report to the African Commission on Human and Peoples' Rights on their compliance with the Declaration in their periodic reviews.

Further, while the African Union Convention on Cybersecurity and Personal Data Protection, the continent's model instrument on privacy and data protection, provides safeguards for personal privacy and data protection, it is yet to come into force as most states are yet to sign or ratify it.[10] 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."

The right to privacy in various African countries is undermined by laws and regulations that enable state surveillance, including the interception of digital communications, collection of personal data including biometric data, video surveillance and the use of facial recognition technology, as well as physical search and seizure. The broad powers given to the state and its agencies to conduct surveillance, the abuse of the surveillance powers, the limited oversight and transparency over surveillance activity, the strenuous and sometimes unclear demands on intermediaries, including to facilitate interception of communication or hand over communication data of their subscribers to state security agencies, are primary concerns.[11]

Many African countries have passed legislation that limits anonymity and the use of encryption, purportedly to aid governments' efforts to combat terrorism and crime. Other governments limit the use of encryption to enable them to monitor the communications of critical journalists, human rights defenders, and opposition politicians.[12]

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

10 *African Union Convention on Cybersecurity and Personal Data Protection, "Status List" as at 28th April, 2021, https://tinyurl.com/2p9c43ru*

11 *CIPESA ibid.*

12 *How African Governments Undermine the Use of Encryption, https://cipesa.org/?wpfb_dl=477*

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,[13] provide effective remedies, and adequate oversight for the protection of personal information. A concern is that in several African countries, government agencies are collecting and processing personal data without adequate data protection laws, amidst limited oversight mechanisms and inadequate remedies; and 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.[14]

Another growing trend has been data localisation, which refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction.[15] It entails various policy measures that restrict data flows by limiting the physical storage and processing of data within a given jurisdiction's boundaries.[16] 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.[17] On the other hand, 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."[18]

Some critics argue that "data localisation policies are causing more harm than good" as "they are ineffective at improving security, do little to simplify the regulatory landscape, and are causing economic harms to the markets where they are imposed."[19] Further, it has been argued that data localisation requirements undermine social, economic and civil rights by eroding the ability of consumers and businesses to benefit from access to both knowledge and international markets and by giving governments greater control over local information.[20]

Indeed, the issue of data localisation is mentioned by the Declaration under Principle 40(3). It 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. Moreover, Principle 42(4) provides that "Every person shall have the right to exercise autonomy in relation to their personal information by law and to obtain and reuse their personal information, across multiple services, by moving, copying or transferring it."

Below, we explore the legal provisions on surveillance, data localisation requirements, biometric data collection, and limitations on the use of encryption. It should be noted that in many countries, there is no evidence of how the provisions of the laws have actually been employed to undermine the right to privacy or other digital rights.

13 *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.*

14 *Mapping and Analysis of Privacy Laws and Policies in Africa Summary Report, https://cipesa.org/?wpfb_dl=454*

15 *Svantesson, D., Data localisation trends and challenges, http://dx.doi.org/10.1787/7fbaed62-en*

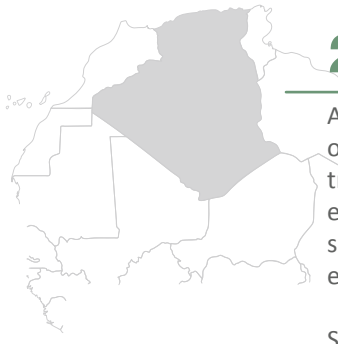
16 *How Would Data Localization Benefit India? https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-8429*

17 *How Surveillance, Collection of Biometric Data and Limitation of Encryption are Undermining Privacy Rights in Africa, https://tinyurl.com/4ptmxy43*

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

19 *Emily Wu, Sovereignty and Data Localization, https://www.belfercenter.org/publication/sovereignty-and-data-localization*

20 *Breaking the Web: Data Localization vs. the Global Internet, https://ssrn.com/abstract=2407858*



# 2.1 Algeria

Article 65(5) of Law No. 06-22 of December 20, 2006[21] on the code of criminal procedure and article 3 of Law No. 09-04 of August 5, 2009[22] on the fight against ICT-related offenses provide for authorised surveillance. The surveillance is conducted in investigations related to drug trafficking, organised crimes, breach of automated data processing systems, money laundering, terrorism, offenses relating to foreign exchange legislation, and corruption. Law No. 09-04 of August 5, 2009 prescribes additional conditions allowing surveillance operations, such as a potential attack on a computer system, posing a threat to public order, national defense, state institutions or the national economy, and for purposes of investigations when it is difficult to obtain relevant information without conducting electronic surveillance.

Surveillance must be carried out under the authorisation and direct supervision of the public prosecutor or in case of an open judicial investigation, the magistrate under article 65(5) of Law No. 06-22. According to article 65(8) of this law, the public prosecutor or the judicial police officer authorised by the prosecutor, the investigating judge or the judicial police officer appointed by the judge, may request any qualified agent of a service, of a unit or a public or private body responsible for telecommunications, to assist with the communication monitoring or interception. Written authorisation is required and should include all the elements making it possible to identify the connections to be intercepted, the targeted places, and the offense which justifies the recourse to these measures as well as the duration of the interception. Article 65(7) limits the maximum duration of surveillance to four months, renewable according to the needs of the investigation. Law No. 09-04 provides that, in investigating terrorist or subversive acts and offenses against state security, the authorisation is issued to the judicial police officers by the Attorney General at the Court of Algiers, for a renewable period of six months, on the basis of a report indicating the nature of the technical process used and the objectives it aims to achieve.

Article 41 of Law No. 18-04 of 10 May 2018[23] establishing the general rules relating to postal and electronic communications, requires all equipment and installations that are intended to be connected to a public communications network, offered for sale or distributed for free, to be approved by the Regulatory Authority of Post and Electronic Communications (ARPCE). Also, Executive Decree No. 09-410 of December 10, 2009 setting the safety rules applicable to sensitive equipment,[24] lists encryption software among the sensitive goods. Its articles 17 and 20 provide that the acquisition and use of encryption software by natural or legal persons are subject to prior authorisation by the ARPCE and approval from the Ministry of Defence and the Ministry of the Interior.

The ARPCE published requirements for issuing operating licences to encryption software and equipment, in Decision No. 17/SP/PC/ARPT of June 11, 2012.[25] Applicants must submit the type and nature of the equipment that will be used, list of cryptography algorithms, the size of the encryption keys, the type of Virtual Private Network (VPN) used, the authentication methods, the Public IP address and any other information required by the ARPCE.[26]

In 2017, the ARPCE ordered operators to disallow private internet access in particular to embassies and multinational companies using VPNs.[27] It specified that, for VPN authorisation, the following information must be provided: the type of VPN used (IPsec, SSL / TLS or others), the authentication method used (pre-shared key, certificate, Challenge/ Response, etc.), the cryptographic algorithms used in the key exchange phase (Key exchange protocol, encryption algorithm and hash function), used to ensure integrity, and public IP (internet protocol) addresses. In October 2019, the ARPCE specified that any operation of a VPN outside the regulatory framework constituted a violation of the laws and regulations in force, and that the operator was required to declare it and comply with the system put in place.[28]

21 *Law No. 06-22 of December 20, 2006, https://www.joradp.dz/TRV/FPPenal.pdf*
22 *Law No. 09-04 of August 5, 2009, https://www.arpce.dz/fr/file/p3m2q0*
23 *Law No. 18-04 of 10 May 2018, https://www.arpce.dz/fr/file/q0e1b5*
24 *Algeria, Executive Decree No. 09-410 of 23 Dhou El Hidja 1430 / December 10, 2009 setting the safety rules applicable to sensitive equipment, https://bit.ly/3DdK8l7*
25 *Algeria, Decision No. 17/SP/PC/ARPT of June 11, 2012 on the validity period of the operating authorization for encryption equipment and software, https://www.arpce.dz/fr/file/b0o8z9*
26 *ARPCE, Encryption Equipment and Software, Procedure, https://www.arpce.dz/fr/service/crypt*
27 *For law's violation, the ARPCE blocks the VPN of VFS Global, https://bit.ly/3H1WjDH*
28 *ARCPE, Press Release, https://www.arpce.dz/fr/pub/v2x8l8*

Law No. 18-07 of June 10, 2018 related to data protection[29] restricts cross-border transfer of personal data. Article 44 prohibits any transfer of personal data to a foreign state when it is likely to harm public security or the vital interests of Algeria. However, articles 44 and 45 allow cross-border transfer of personal data under specific conditions. If the destination country provides a sufficient level of security and protection of privacy, fundamental rights and freedoms of individuals with regard to processing of personal data, the controller is permitted to transfer the data after obtaining authorisation from the National Authority for the Protection of Personal Data (NAPP) - a body that is yet to be formally established.

The sufficiency of the level of protection provided by a country is assessed by the NAPP, in particular, depending on the legal provisions in force in that state, the applicable security measures, and the specific characteristics of the processing such as its purposes. If the NAPP has assessed the level of protection in the destination country as insufficient, cross-border transfer is only allowed with authorisation of the national authority, or the consent of the concerned person, or in the application of a bilateral or multilateral agreement to which Algeria is a party, or if the transfer is necessary. Article 45 further details the conditions of necessity to include the preservation of the public interest and the execution of an international legal assistance measure. Under article 67, transferring personal data to a foreign state in violation of the provisions of article 44 is sanctioned by one to five years of imprisonment and a fine of between 500,000 - 1,000,000 Algerian Dinar (DA) (USD 3,654-7,308). In the event of a repeat offence, the penalties are doubled, according to article 74.

Separately, the ARPCE issued decision No. 48/SP/PC/ARPT/17 dated 29 November 2017[30] defining the conditions and modalities for establishing and operating of hosting and storage services for computerised content for user benefit in the context of cloud computing services. According to article 10 of the decision, the service provider is required to establish its infrastructure on the national territory by means of equipment incorporating the most recent and proven technologies to guarantee that customer data is hosted and stored on Algerian territory. Further, Law No. 18-05 of May 10, 2018 relating to electronic commerce[31] requires local e-commerce operators wishing to sell online to host their website in Algeria and be registered in the commerce register. Similarly, Executive Decree No. 20-332 of November 22, 2020 laying down the procedures for online content publications, requires such operators to host their sites in Algeria, with a".dz" domain name (article 6).[32]

The 2018 law on protection of personal data does not define biometric data. However, it defines sensitive data as “personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of the data subject or which relate to his health including his genetic data”. According to article 18 of this law, the processing of sensitive data is only allowed for reasons of public interest essential to guarantee the exercise of the legal or statutory functions of the controller or when the data subject has given their express consent, in the event of a legal provision which enshrines it, or with the authorisation of the national authority. Any processing of sensitive data outside of these exceptions is an offense punished by imprisonment of between two and five years and a fine of between 200,000-500,000 DA (USD 1,465-3,654).

29 *Algeria, Law No. 18-07 of June 10, 2018 related to data protection, https://bit.ly/30bVlEx*
30 *Algeria, Decision No. 48/SP/PC/ARPT/17 dated 29 November 2017, https://bit.ly/3F9rKKH*
31 *Algeria, Law No. 18-05 of May 10, 2018 relating to electronic commerce, https://bit.ly/3D1DUEC*
32 *Decree No. 20-332 of November 22, 2020, https://www.webservices.dz/journal-officiel*

In 2012, the directorate of titles and secured documents was created under the Ministry of the Interior and Local communities, through executive Decree No. 11377 of November 21, 2011[33] among whose objectives is the personalisation of biometric documents and the development of e-government services. The country has an electronic biometric national passport issued under Decree of December 26, 2011[34] whose issuance started in early 2012.[35] Algeria also has a National biometric electronic identity card (CNIBE) whose procedures were stipulated by Presidential Decree No. 17-143 of 18 April 2017,[36] with the single National Identification Number (NIN) which is generated for the ePassport also used for the national identity card. The national identity card is issued to all Algerian citizens regardless of age (Article 3). However, minors under the age of 12 are exempt from collecting fingerprints, according to article 13 of the decree. It is issued together with a secret code to be used by the applicant to access online services.

The National Driving License Office made public, on January 4, 2020, a new directive sent to all driving schools that it is compulsory to have a biometric identity card in order to take driving licence exams. In June 2019, the Algerian interior ministry started converting driving licences to a biometric format.[37] They are equipped with an encrypted electronic chip that contains personal and biometric data of the driver; as well as other applications including one that is devoted to the point-based licence device.[38]

Moreover, SIM card registration is mandatory in Algeria, per Law No. 18-04 of May 10, 2018 setting the general rules relating to post and electronic communications which requires the operator to identify the subscriber before activating services to them.[39] The ARPCE decision No. 53/SP/ PC/ARPCE/2021 of October 18, 2021 amending decision No. 71/SP/PC/ARPT/2015 of October 28, 2015[40] setting the conditions and procedures for identifying customers who subscribe to or hold prepaid SIM / USIM cards, states in its third article that it is the responsibility of the operator to take the appropriate measures to ensure the protection and confidentiality of the personal information that it holds, that it processes or that it registers on the identification module of subscribers or of its customers who hold a prepaid or postpaid SIM or USIM. Any customer requesting a prepaid or postpaid SIM or USIM card must present a copy of an official identity document such as the national ID or the passport.[41] The operator is required to establish and maintain a digital database containing the following information for all its subscribers: first name(s) and surname, date and place of birth, the national identification number and date of subscription.

33 *Decree No. 11377 of November 21, 2011, http://www.joradp.dz/FTP/jo-francais/2011/F2011063.pdf*

34 *Decree of December 26, 2011, https://bit.ly/3znVEcw*

35 *Modernisation du Service Public en Algérie, https://www.id4africa.com/2019_event/presentations/InF3/4-Abderrazak-Henni-MOI-Algeria.pdf*

36 *Presidential decree No. 17-143 of 18 April 2017, https://www.interieur.gov.dz/images/Doc3.pdf*

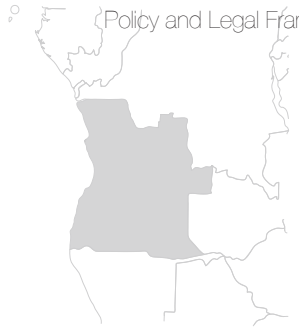
37 *See Launch of issuance of electronic biometric point-based driving licenses, https://bit.ly/3sRLaAC*

38 *The officially launched biometric permit: what will change, https://www.tsa-algerie.com/le-permis-biometrique-officiellement-lance-ce-qui-va-changer/*

39 *Law No. 18-04 of May 10, 2018, https://www.arpce.dz/fr/pub/w0k9a2*

40 *Decision No. 53/SP/ PC/ARPCE/2021 of October 18, 2021, https://www.arpce.dz/fr/file/i7l3i1*

41 *Décret exécutif n° 20-64 du 20 Rajab 1441, https://www.arpce.dz/fr/file/w7q6b7*



## 2.2 Angola

In Angola, the law on video surveillance No. 2 of 22 January 2020[42] provides for the installation of video surveillance systems by state security forces to maintain public safety. Article 29 obliges all persons with CCTV systems to provide recordings when requested by the Data Protection Agency (DPA), and mandates the Agency to impose sanctions and penalties, including for infractions related to operation of CCTV systems.

As for the law on Mobile Identification or Location and Electronic Surveillance No. 11/20 of 23 April 2020,[43] per article 3, its aims include prevention and prosecution of crime; location of a cellular signal of a device owned or presumed to be owned by a missing person who is a victim or a perpetrator of crime; and obtaining relevant data or information for criminal investigation of perpetrators of crime through their surveillance. Article 8 provides that interception, monitoring or surveillance through the deployment of surveillance technology, including spyware and telecommunications interception, can be carried out by the National Police, and is authorised by the Public Prosecutor's Office or judges through a written surveillance order (article 20).

The law does not stipulate the duration of the surveillance order. However, the law requires that investigators report to judicial authorities the results of the surveillance once it is over. Also, the law prohibits surveillance on political grounds or based on discriminatory motivation, which terms are not defined. Further, surveillance must be done in coordination with the DPA which must submit an annual report on its overall activities to the National Assembly. However, this has not happened since the Authority's establishment in 2016. Under article 12, cellular identification or tracking and electronic surveillance may be carried out by the following means: software for locating and accessing telephone and telematics registration and signals, computer applications and platforms for monitoring cellular signals; video surveillance cameras and audio surveillance equipment, installed in fixed locations; equipment for locating and intercepting telephone communication; and radio listening equipment. Under article 31, every citizen is obliged to cooperate with justice entities when they request for information.

There are concerns that, given insufficient safeguards against misuse of surveillance powers by state agents, the law will expand state surveillance activity,[44] even as offline and online surveillance are integrated through the Integrated Public Security Centre (CISP). The CISP in the capital Luanda is reportedly connected to over 719 cameras in the city, whose capabilities include vehicle tracking, facial recognition, and infrastructure monitoring.[45]

Meanwhile, article 31 of the Law on the Protection of Information Networks and Systems – 07/2017 of 16 February 2017[46] provides that only telecommunications providers are free to import and use encryption. The law does not provide instances of sale or use for commercial purposes. Service providers are required to register with the regulator – Instituto Angolano das Comunicações (INACOM). Further, article 32 provides that operators of publicly available electronic communications networks must retain data where communications are not initiated or terminated on national territory. Under article 8, it is the responsibility of the operator of the electronic communications network to guarantee the technical and security conditions under which electronic communications are carried out for the purpose of transmission of traffic and location data relating to natural and legal persons. The law is silent on limits to the use of encryption.

42 *Law on video surveillance – no. 2 of 22 January 2020, https://www.paced-paloptl.com/uploads/publicacoes_ficheiros/lei-videovigilancia.pdf*

43 *Mobile Identification or Location and Electronic Surveillance No. 11/20 of 23 April 2020, https://apd.ao/fotos/frontend_1/editor2/200420_lei_11-20_de_23_abril-identificacao_celular_vigilancia_electronica.pdf*

44 *Video Surveillance Law is already in Diário da República, https://www.jornaldeangola.ao/ao/noticias/detalhes.php?id=443586*

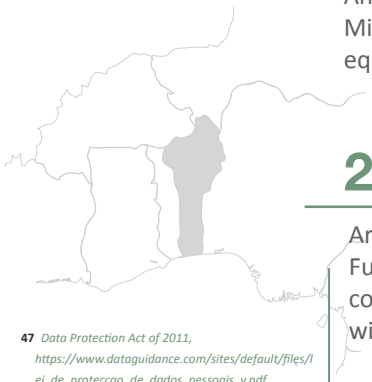
45 *CISP revolutionizes the security system in Angola, https://angola.shafaqna.com/PT/AL/268307*

46 *Law on the Protection of Information Networks and Systems – 07/2017 of 16 February, https://animalexdominis.files.wordpress.com/2018/03/proteccc3a7c3a3o-das-redesesistemas-informc3a1ticos-2017.pdf*

On data localisation, article 34 of the Data Protection Act of 2011[47] states that the international transfer of data to another country should only be carried out if there is adequate data protection in the third country and must be authorised by the DPA. Such authorisation can only be granted if certain conditions are met, such as the consent of the data subject and if the transfer is the result of the application of international treaties or agreements between Angola and other countries. Article 24 of the same Act states that the interconnection of data may only be carried out with the authorisation of the DPA, unless otherwise provided by law. The DPA only authorises such interconnection if it is appropriate for the pursuit of the lawful purposes of data processing.

The DPA is empowered to issue administrative fines ranging from USD 75,000 to USD 150,000 where a controller or processor fails to notify the DPA in the event of data breach or violation of other provisions of the data protection law.[48] Some violations of the data protection law can also render controllers or processors liable to between three and 18 months' imprisonment.[49] Since its creation in 2019, the DPA has received over 100 requests and invasion of privacy complaints including on personal data processing without consent and sites without privacy notices.[50]

SIM card registration is mandatory and is regulated by the Law 11/20 of 23 April 2020 - Identification or Cellular Location and Surveillance. The mandatory SIM card registration is overseen by the Angolan National Regulatory Institute for Communications (INACOM), the ICT regulator. The process requires an identity card or driving licence and tax card for citizens, or a passport with a valid visa for foreigners. Ahead of the August 2022 elections, Angola is planning to launch a biometric passport.[51] According to Gil Famoso, the director of Angola's Migration and Foreigners Service, the new passport "will contain three levels of visual security, verifiable through electronic and security equipment and through specific conformation techniques and forensic techniques."[52]



## 2.3 Benin

Article 12(2) of Law No. 2017-20 of 20 April 2018 on the Digital Code in Benin prohibits the conduct of surveillance without a warrant. Further, article 52 of the Benin Code of Criminal Procedure prohibits any person other than the sender or recipient of an electronic communication to listen, intercept, store communications and data or to subject them to any other means of interception or surveillance, without the prior consent of the users concerned.

The 2012 Code of Criminal Procedure relating to the interception of correspondence or article 595 of the Digital Code provides for authorisation of designated administrative authorities to conduct surveillance, which is supervised by an investigating judge. However, the implementing regulations designating the authorised authorities are yet to be adopted by the Minister. Under article 596, the justification for surveillance is based on grounds such as the maintenance of national independence, territorial integrity or national defence, the preservation of major foreign policy interests, the safeguarding of major economic, industrial and scientific interests, and the prevention of terrorism, collective violence likely to seriously undermine public peace, or organised crime. [53]

47 *Data Protection Act of 2011, https://www.dataguidance.com/sites/default/files/lei_de_proteccao_de_dados_pessoais_v.pdf*

48 *Decree 214/2016, art. 46 and Law 22/11, art. 14.*

49 *Law 22/11, art.51, 55, 56, 58, 60 and 61. For example, the unauthorised access to personal information, false notification information, unauthorised erasure, alteration of data, refusal to restrict processing.*

50 *Data Protection, Growing Reality in Angola, https://www.apd.ao/ao/noticias/proteccao-de-dados-realidade-crescente-em-angola/*

51 *Angola prepares to launch biometric passport, http://www.xinhuanet.com/english/africa/2021-06/02/c_139985648.htm*

52 *Angola and Cameroon Proceed With Biometric Passports, https://identityreview.com/angola-and-cameroon-proceed-with-biometric-passports/*

53 *Article 596 of Law No. 2017-20 of 20 April 2018 on the Benin Digital Code, https://bit.ly/3ndUBH1*

Article 53 of the Code of Criminal Procedure amended and supplemented by Law No. 2018-14 of May 18, 2018 empowers criminal investigation officers to carry out visits, searches and seizures during investigations relating to economic and financial offences, terrorism, drug trafficking, illicit enrichment and paedophilia. The law empowers Judicial Police Officers, with the prior authorisation of the public prosecutor, to among others, organise physical and electronic surveillance of any suspect. However, where requested by the investigating judicial police officer, the public prosecutor should seek the authorisation of the Senior Investigating Judge to conduct wiretaps. The interception warrant is not subject to appeal, but must be in writing, identify all the elements to be intercepted and state the offence that motivates the interception or electronic surveillance.

Failure to seek authorisation for surveillance is an offence under Book 5 of the Digital Code, with article 24 of the Code of Criminal Procedure specifying penalties.[54] The penalties provided for are warning and reprimands with entries in the file by the public prosecutor under the control of the Prosecutor General against the officers and agents of the judicial police who are at fault. Further, article 246 supplements these disciplinary sanctions with written observations, temporary or permanent suspensions of exercise, and withdrawal of authorisation to practice.

Article 619 of the Digital Code law, bases the use of encryption on the principle of freedom. However, this freedom is restricted as the import or supply of means of cryptology, when it does not exclusively provide authentication or integrity control functions, is subject to a prior declaration to the Cryptology Commission that is provided or authorisation by decree of the Council of Ministers as provided under article 622. The Cryptology Commission is provided for by the Benin Digital Code but the implementing decree remains to be adopted. Under article 623, where encryption services are for national defence and the internal or external security of the State, the Commission is not required to issue approval. Article 630 of the Code provides that anyone who obstructs a judicial inquiry by means of cryptology shall be imprisoned for between one to five years, fined between one million to 20 million Central African (CFA) francs (USD 1,767- 35,332), or both. Moreover, article 635 of the Code together with article 78 of the Benin Code of Criminal Procedure, requires any person at the request of the investigating judge or the public prosecutor to decrypt data to make it intelligible information.

The failure to comply with the conditions for carrying out cryptology activities is punishable under articles 626 to 629 with provisional or definitive withdrawal of the authorisation; fines of between 500,000 and 20 million CFA francs (USD 884-35,332); or imprisonment for between six months to five years. Aggravating circumstances such as the use of a cryptology means to plan or commit a crime or an offence, may lead to life imprisonment as provided under Article 631 of the Digital Code.

According to Article 391 of the Digital Code, cross-border transfer of personal data requires that the third state or international organisation offer an equivalent guarantee of protection of private data as provided for in Beninese legislation. The equivalent and sufficiency of the level of protection shall be assessed in light of all the circumstances relating to a data transfer or a category of data transfers. The Beninese legislation mentions the criteria for determining the equivalency, which include the rule of law and respect for human rights; existence of an independent supervisory authority; and compliance with international standards.

Prior authorisation from the Data Protection Authority (APDP)is required before any data transfer from Benin. Exceptionally, a transfer of personal data to a third state or an international organisation which does not ensure an adequate level of protection may be carried out if the data subject has expressly given their consent to the transfer; the transfer is necessary for the performance of a contract between the data subject and the controller; the transfer is necessary for the protection of an important public interest, or for the establishment, exercise or defence of legal claims; or the transfer is necessary to safeguard the vital interests of the data subject.

54 *Article 453(1) and Article 460(6) of the Benin Digital Code*

Articles 394(2) and 396 of the Digital Code considers biometric data to be sensitive data, and its processing for the purpose of uniquely identifying a natural person is prohibited except for the cases specified by the law. Provisions of article 407 allow the processing of personal data, including biometric data, only after prior authorisation by the APDP. There are some exceptions, however. Article 408 allows for processing of personal data, including biometric data, where the data is manifestly made public by the data subject; where the data subject offers explicit consent to processing; and where processing is necessary to safeguard the vital interests of the data subject. Other exemptions relate to reasons of public interest; requirements by laws relating to official statistics; medical reasons; performance of a contract by the data subject; compliance with a legal and regulatory obligation; and scientific research purposes.

Meanwhile, the Benin Electoral Code (articles 131, 174, 179, 180) allows state organs to collect personal and biometric data for voters' registration. Data collected includes pictures and fingerprints for both hands.

**Case study: Biometric data collection by a telco**

*In 2016, the telecom operator MTN Benin applied for authorisation to collect biometric data of its customers. In some quarters, the request was considered at odds with Law No. 2009-09 on the protection of personal data,[55] in particular articles 5 and 6. Indeed, the MTN request was rejected by the Beninese National Commission for Information and Liberties (CNIL),[56] a body that was later replaced by the data protection agency APDP.[57] The CNIL stated that, "as a private company whose activity consists in offering telecommunications services, MTN cannot collect biometric data." It considered that the collection and processing of data relating to surname, first name, address, age, sex, professional status, date and place of birth was sufficient for the purposes which MTN sought the data for.*

55 *Law No. 2009-09 of May 22, 2009, https://sgg.gouv.bj/doc/loi-2009-09/*

56 *MTN Benin wants to collect the biometric data of its users, the CNIL says no - Internet Sans Frontieres, https://internetwithoutborders.org/mtn-benin-veut-collecter-les-donnees-biometriques-de-ses-utilisateurs-la-cnil-dit-non/*

57 *APDP, https://apdp.bj/*

## 2.4 Burkina Faso

Law No. 61-2008 / AN laying down general regulations for electronic communications networks and services in Burkina Faso provides for the privacy of electronic communications.[58] Chapter 3 advocates respect for the privacy of users of electronic communications networks and services and requires operators of public networks and services to respect the secrecy of users' correspondence. Under article 35, all electronic communications must be guaranteed confidentiality, without prejudice to the investigative powers of justice and state security. Under article 37, operators of electronic communications networks are required to erase or anonymise any traffic or location data. However, to enable research, identification and prosecution of criminal offenses, the provision of information to judicial authorities, the same may be deferred for a maximum of one year.

Article 39 of the law provides that subject to judicial inquiries, location data may neither be used during the communication for purposes other than its routing, nor be kept and processed after the completion of the communication except with the consent of the subscriber, duly informed of the categories of data involved, the duration of the processing, its purposes and whether or not this data will be transmitted to third-party service providers. Article 40 requires that any location data collection or processing be carried out in accordance with the data protection law, and not to relate to the contents of correspondence. Under article 43, any subscriber of a network open to the public may oppose their identification by correspondents of their subscriber number. Under article 199, unless sanctioned by law, any person who violates the secrecy of a correspondence potentially faces imprisonment of one to four years, a fine of one million to five million CFA francs (USD 1,712-8,561), or both.

The Law No. 051/98/AN of December 4, 1998, reforming the telecommunications sector in Burkina Faso, defines cryptology services in article 5.16 as any service aimed at transforming, using secret codes, information or clear signals into information or signals unintelligible for third parties; or to carry out the reverse operation, using hardware or software means designed for this purpose. Article 17 of the law provides that the supply, operation, import of means or services of cryptology are subject to: prior declaration, when the means or the service has no other purpose other than to authenticate a communication or to ensure the integrity of the transmitted message; and prior authorisation in other cases. Further, the regulatory authority is mandated to set the conditions for prior authorisation. Under article 54, an approved operator is obliged to implement or provide the secret code of the means of providing cryptology if directed by a prosecutor or a judge.

Without prejudice to the application of customs legislation, article 85 provides that anyone who exports or imports a means of cryptology, or provides cryptology services without authorisation is liable on conviction to imprisonment for a period of between one month to three months, a fine of 100,000 to 500,000 CFA francs (USD 171-857), or both. In the case of a repeat offender, these penalties may be doubled as per article 86 of the law. In addition, a court may suspend the authorisation for up to two years, and order the confiscation of the means of cryptology.

**58** *Law N0 61-2008 / AN http://www.arcep.bf/download/lois/loi_no_061-2008-AN_du_27-11-2008-2.pdf*

According to article 42 of the law No. 001-2021 / AN on the protection of individuals with regard to the processing of personal data, a data controller may transfer personal data to a foreign country or to an international organisation only if the country or organisation ensures an adequate level of protection equivalent to that provided in Burkina Faso of the privacy, freedoms and fundamental rights of persons with regard to the processing of which this data are or may be subject.[59] Before any transfer of personal data beyond national borders, the data controller requires authorisation from the supervisory authority, the Data Protection Commission (CIL); a signed contract with the third party including data confidentiality and data reversibility clauses to facilitate the complete migration of data at the end of the contract; and implements technical and organisational security measures guaranteeing in particular data encryption, data availability, confidentiality, integrity, availability and constant resilience of processing systems and services as well as a testing procedure, analysis and evaluation of the measures taken.

However, it is also possible under article 44 to transfer personal data to a country which does not ensure an adequate level of protection, under various conditions, including law enforcement purposes; where the data subject has given their informed and unequivocal consent; and "when, in exceptional circumstances, the transfer is authorised by decree taken in the Council of Ministers after the assent of the supervisory authority".

The data protection law lays down conditions for processing of personal data. Per article 31, the processing of personal data relating to genetic or biometric data is subject to authorisation by the regulatory authority. The law No. 009-2017 on the biometric cards[60] provides for a digitised ID with biometric data (photo with facial recognition and data of two fingerprints are collected). According to article 1 of this law, a biometric identity card of the Economic Community of West African States (ECOWAS) applies in Burkina Faso. The ECOWAS identity card is individual and obligatory for every Burkinabè citizen of 15 years and above. It is an official identification document required for various aspects of civil life.

Biometric data is also collected in accordance with the Burkinabè electoral code (Law N ° 006-2012 / AN of 05 April 2012).[61] Article 50 of the law provides for the establishment of electoral lists by the Independent National Electoral Commission (CENI), to be carried out on the basis of a biometric electoral census, which entails the capture of the photograph and the fingerprint of the voter. The biometric electoral rolls are permanent but subject to annual review by the CENI. However, before each general election, an exceptional revision can be decided by decree.

Meanwhile, Law No.028-2021/AN of May 2021 which regulates the use of drones by civilians provides under its clause 53 that the use of civilian drones be done in compliance with the regulations on the protection of personal data, the right to image of others and the privacy of individuals.[62]

59 *Burkina Faso, law No. 001-2021 / AN on the protection of individuals with regard to the processing of personal data, https://bit.ly/3qtcOmw*

60 *Law No. 009-2017 on the Biometric Card, https://www.assembleenationale.bf/IMG/pdf/loi_009-2017_portant_carte_biometrique.pdf*

61 *Law No. 006-2012 / AN of 05 April 2012, https://tinyurl.com/y5jr3ruw*

62 *Law No.028-2021/AN of May 2021, https://www.assembleenationale.bf/IMG/pdf/loi_no028-2.pdf*

## 2.5 Burundi

Article 23 of Law No 1/011 of 4 September 1997 governing the telecommunication sector obliges all service providers and all their employees to protect users' privacy.[63] However, under article 24, a service provider may share confidential information when requested for judicial investigatory purposes. Articles 29 and 30 of Law No. 100/97 of 18 April 2014[64] on the conditions for operating electronic communication services provide that, for public security reasons and judiciary inquiries, telecom operators must provide the full identity and geo-location of their subscribers in real time whenever asked by the Regulatory Agency for Telecommunications (ARCT). Failure to identify subscribers attracts a fine of Burundian Francs 5,000,000 (USD 2,000).

Moreover, article 5 of Order No 540/356 of 17 March 2016[65] on fighting fraud in the ICT domain gives the ARCT the right to direct any operator to provide the detailed identity of any subscriber. Further, article 6 empowers the ARCT to provide a voice server where the operator shall divert all phone communications of a user where crime is suspected. Article 9 allows ARCT to request the full identity of an internet subscriber and their IP address, and install IP probes on the technical installations of an ISP. Moreover, article 10 of that order obliges operators to comply with any request by the ARCT and its technical partner in order to fight fraud in electronic communications. Failure to cooperate attracts a daily fine of five million Burundian Francs (USD 2,000).

The Law No 1/09 of 11 May 2018 amending the Code of Criminal Procedure[66] provides for "Special investigation methods" under article 46, which include surveillance of electronic communications and seizure of computer data. Article 69 empowers the Public Prosecutor's Office, where the needs of the investigation so require, to prescribe the interception, recording and transcription of correspondence transmitted by telecommunications. The operations under interception order must be conducted under the direct supervision of the cited officer and should be kept confidential. The interception order must be in writing and is valid for a period of two months, for which an extension may be obtained. Upon completion of interception, article 71 requires the officer in charge to write a detailed report, and send it to the public prosecutor. The report is stored as part of the criminal record of the monitored person. Also, the recordings may be destroyed under the supervision of the public prosecutor when the statute of limitations expires, or in the event of a final decision of acquittal.

Article 71 provides that the data recorded during the investigation should be destroyed after the inquiry, under the supervision of the Public Prosecutor. Article 78 provides that the data should be kept confidential and only data related to the object of the inquiry are taken. Burundi does not have a specific law on personal data protection, with a draft published in 2017 yet to be enacted.[67]

Encryption is not specifically regulated in Burundi. However, the 2017 Personal Data Protection Bill provides in its article 25 that any entity in charge of personal data processing should ensure that the data is kept confidential and secure against any accidental destruction, unauthorised access, or interception when transmitted via a network. The technology sector laws are silent on data localisation, but Law 1/17 of 22nd August 2017 on banking activities in Burundi,[68] under article 61 allows sharing of personal data with branches of any bank that could have opened abroad and the central bank of the country where the bank branch is located. However, the central bank shall ensure that any confidential data shared is only used for control or crisis resolution purposes, and the receiver has to abide by the confidentiality principle.

63 *Law No 1/011 of 4th September 1997, http://www.arct.gov.bi/images/decretslois/decret011.pdf*

64 *Law No. 100/97 of 18 April 2014, http://arct.gov.bi/images/decretslois/decret1.pdf*

65 *Order No 540/356 of 17 March 2016, http://arct.gov.bi/images/ordonnances/ordo540356.pdf*

66 *Law No 1/09 of 11th of May, 2018 on the Penal Code, http://www.assemblee.bi/IMG/pdf/9%20du%2011%20mai%202018.pdf*

67 *State of Internet Freedom in Africa: Privacy and data protection in the digital era: challenges and prospects, https://cipesa.org/?wpfb_dl=278*

68 *Law 1/17 of 22nd August 2017 on the banking activities in Burundi, https://tinyurl.com/2p8bcfhu*

Data localisation is specifically dealt with by the draft law on personal data protection with article 1 defining cross-border flow of data as international flows of personal data through electronic transmission or any other means of transmission. Chapter XI is about transboundary flow of personal data. Article 85 and 86 allow data flows to East African Community (EAC) member countries. The flow is allowed only if the data is needed by the receiver and is for legitimate use. The entity sending the data should check the necessity of transfer and ensure that the receiving entity has the necessary skills for processing data in a confidential way.

If the data is to be transmitted out of EAC country members, article 87 provides that the sending entity must ensure that the destination country has an adequate level of protection of personal data. In case the destination country does not have a strong policy for protecting personal data and is not an EAC member, article 88 provides that the owner of the data has to be consulted and to provide a written consent before sending that data. In addition, the national data protection authority must be consulted prior to the cross-border transfer.

Regulation of biometric data is also found in the personal data protection bill drafted in 2017, which classifies biometric data into the category of personal data as provided in the definition section (article 1). Article 12 provides that biometric data and other particular kinds of data cannot be processed, except when there is written consent of the data subject, or when it is necessary to the defence of vital interests of the subject, or if it is done by an officially recognised Non-Government Organisation (NGO) involved in the defence of human rights, or for medical purposes.

Burundi introduced biometric passports in 2010, and subsequently introduced biometric driving licences. To obtain a passport or driving licence, an applicant must be physically present, and their fingerprints collected. The applicant also has to provide a birth certificate and a national identity card. The Ministerial order No 215/05/cab/2010 of 6 July 2010 specifies the technical specifications of biometric passports and other documents[69] while Ministerial order No 215/224 of 2 March 2011 lays out the cost of biometric passports.[70] These laws have no provisions on protection of biometric data collected in order to obtain those official documents. The private company that produces these biometric documents in Burundi is called CONTEC Global.[71]

Mandatory SIM card registration commenced in October 2011, through a directive by the regulatory authority, the Agence de Régulation et de Contrôle des Télécommunications (ARCT). In July 2014, the ARCT ordered all telecom operators to deactivate any SIM card whose owner had not been properly identified.[72] An operator can be fined one percent of its annual turnover in case of failure to comply. If an operator fails to comply with this first sanction, the ARCT can revoke the operator's licence in accordance with article 10 of the order. The required information for SIM card registration includes the user's full names, full address and birth date. Moreover, the SIM user has to provide a copy of their national identity card which has itself some additional personal information such as their father's and mother's names, the profession and the marital status.

69 *Ministerial order No 215/05/cab/2010 of 6th July 2010, https://amategeko.bi/wp-content/uploads/2019/11/BOB_No7-ter-2010.pdf*

70 *Ordinance No. 215/224/02/03/2011, http://www.securitepublique.gov.bi/IMG/pdf/tarif_du_passeport_biometrique.pdf*

71 *State of Internet Freedom in Africa 2018 Report Focuses on Privacy and Data Protection, https://tinyurl.com/bdzffwzv*

72 *Circular No. 01/ARCT/DG/08/04/2014 https://arct.gov.bi/wp-content/uploads/2021/10/circulaire2.pdf*

## 2.6 Cape Verde

Article 20 of the 2017 law on cybercrime and the collection of electronic evidence,[73] provides that the interception and recording of computer data transmissions may only be authorised during an investigation if there are reasons to believe that it is necessary to uncover the truth or that evidence would otherwise be impossible or very difficult to obtain. Interception can be ordered by the investigating judge at the request of the Public Prosecution Service on grounds including investigation of crimes such as terrorism, violent or highly organised crimes, or when there are reasons to believe an imminent crime puts the life or intergrity of a person at serious risk.

Under article 17, the period of interception of communication is 30 days. In order to obtain an interception order, an application must be made to the Public Prosecutor's Office as per article 20, and be responded to within 72 hours. There is no clear obligation on intermediaries to assist in the interception of communications.

Article 6 of the Law No 134-V of 22 January 2001[74] on the processing of personal data in the telecommunications sector requires service providers and network operators to guarantee the confidentiality and secrecy of communications through telecommunications services. Thus, listening, taping, storage or other means of interception or surveillance of communications by third parties is prohibited without the express consent of the user, except in cases specifically provided for by law.

Cape Verde does not have legislation that specifically regulates encryption. Law No. 74-VI, of 4 July 2005 on electronic communications empowers the regulatory authority to manage and authorise the use of electronic communications networks and services accessible to the public. Further, article 61(3) of the law on electronic signatures requires electronic signature certification entities to respect the laws in force regarding protection, treatment, and circulation of personal data and the protection of privacy in the telecommunications sector.[75]

On data localisation, according to article 19 of the Data Protection Act,[76] the transfer of personal data that is to undergo processing is subject to compliance with this law and other legislation applicable to issues of personal data protection and, such transfer can only be made to a country which has a similarly adequate level of data protection. It is for the National Data Protection Commission (CNPD) to decide whether a foreign state ensures an adequate level of protection. The adequacy of the level of protection shall be assessed in light of all the circumstances surrounding a data transfer or set of data transfers, in particular, the nature of the data, the purpose and duration of the proposed processing, the country of origin and country of final destination, the rule of law, both general and sectoral, in force in the state in question, as well as the professional rules and security measures which are complied with in that country.

Article 20 spells out the conditions under which the CNPD can authorise personal data transfer to a state which does not ensure an adequate level of protection. These include where the data subject has given unequivocal consent to the proposed transfer; or if that transfer is necessary for the performance of a contract involving the data subject; or if the processing of the data is required on the grounds of important public interest. The Act also sets out a series of administrative offences, punishable by a fine, and criminal offences punishable either by a fine or a term of imprisonment. These fines range from 50,000 to six million Cape Verdean Escudos (CVE) (USD 670-80,000).

73 *Parlamento aprova Proposta de Lei sobre cibercrime e da recolha de prova em suporte eletrónico https://www.governo.cv/parlamento-aprova-proposta-de-lei-sobre-cibercrime-e-da-recolha-de-prova-em-suporte-eletronico/; Boletim oficial nº 13 https://kiosk.incv.cv/V/2017/3/20/1.1.13.2306/p318*

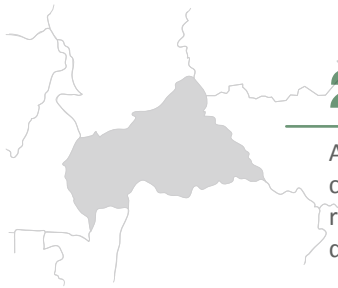
74 *Lei nº134/V/2001 https://www.arctel-cplp.org/app/uploads/membros/64280111205db2d99e5ca5a.pdf*

75 *Decreto-Lei nº 33/2007: http://www.anac.cv/images/stories/legislacao_sti/bocomercioelectronico33de2007.pdf*

76 *Law 41/VIII/2013 of 17 September, https://www.cnpd.cv/leis/DATA%20PROTECTION%20Law%20133.pdf. This law amended the general legal regime for the protection of personal data of individuals, approved by Law 133/V/2001 of 22 January 2001 https://www.cnpd.cv/leis/DATA%20PROTECTION%20Law%20133.pdf*

There is no law obligating SIM card registration in Cape Verde.[77] However, in 2014 the government adopted Decree-Law No. 19/2014 on the National Identification Card (NIC),[78] described as an authentic identification document that ensures protection against fraud, as well as providing facilities such as storage of personal data, protected access for electronic authentication services, digital signature, and e-banking services. Article 15 of the law stipulates that the NIC is composed of several data markers, including the date of birth, gender, a sequential enumeration of three digits and a control digit that will give security to the numbering system itself. The NIC is not linked to voting but it allows access to public services such as payment of taxes.

Whereas the NIC system collects fingerprints, pursuant to article 21, judicial authorities and the police are the only entities that can oblige a citizen, within the scope of their competences, to prove their identity through the functionality of the fingerprints contained in the system. Article 41 designates the National Commission for Data Protection as the entity to regulate the use of data and its protection. Furthermore, article 44 provides that the retention of data depends exclusively on the validity of the citizen's identification document.



## 2.7 The Central African Republic (CAR)

Article 61 of the Electronic Communications Law of 2018 requires the mandatory registration of users of telecommunications or electronic communications services. Article 112 requires operators and their employees to respect the privacy of correspondence subject to lawful requirements for the protection of public safety or national defence. Also, article 113 prohibits the interception, listening, transcription and disclosure of correspondence sent by electronic means.

However, article 136(2) provides for exceptions such as where there is consent of the author of the communications; the prior authorisation of the State Prosecutor or an investigating judge in pursuance of judicial or administrative investigations to protect public security, national defence, or to prevent acts of terrorism; or by staff of the regulator to identify, isolate and prevent unauthorised use of frequency of transmission.

Since CAR does not have a law on cybersecurity or on the fight against cybercrime, there is still concern that these exceptional cases are vague and ambiguous. Unauthorised interception of communications is punished under article 136(1) with imprisonment for two to three years, or a fine of two to three million CFA francs (USD 3,425-5,137).

Cryptology is regulated under the Electronic Communications Law of 2018,[79] whose article 100 requires the supply or use of cryptology to be declared in advance when its purpose is only to authenticate communication or to ensure the integrity of the message. Encryption for other purposes is subject to authorisation through the written opinion of the minister in charge of national security, based on the need to preserve the internal and external security of the state and national defence. The Electronic Communications and Postal Regulatory Authority (ARCEP) is mandated to set the rules governing encryption. Under article 147 of the law, the importation of cryptology equipment without prior authorisation attracts a penalty of between one and five million CFA francs (USD 1,763-8,816), imprisonment of between one and three months, or both.

77 *Africa: SIM Card Registration Only Increases Monitoring and Exclusion, https://tinyurl.com/yphcxjzy*

78 *Decree-Law No. 19/2014, https://tinyurl.com/4b5y2564*

79 *Electronic Communications Law of 2018, https://arcep.cf/images/textes/lois/Loi_18_002_regissant_les_communications_electroniques_en_RCA.pdf*

The country has no law or regulations that specifically deal with issues related to biometric databases and data localisation. The Electronic Communications Law of 2018 in article 112 requires service providers to respect the privacy and to protect customers' personal data, except when required by national defence and public security and the prerogatives of public authority. Those who process and store personal data are obliged to collaborate with the competent authorities by communicating their users' data in the framework of the fight against terrorism, public security and national defense as outlined in article 124. Although this law has provisions on the collection and processing of data, the duration of its storage, and its anonymisation and deletion (article 116), it does not mention biometric data. However, it has been reported that Securiport LLC, a global operator in civil aviation security and border management has entered into an agreement with the government of CAR to implement "full biometric screening to enhance existing immigration control at Bangui's M'Poko International Airport".[80] The CAR started a SIM card registration process in July 2014.[81]

## 2.8 Congo Brazzaville



Article 125 of the 2009 law regulating the electronic communications sector prohibits third parties from listening to, intercepting or subjecting any type of communications to surveillance, without the consent of the users concerned, except where such person is legally authorised to do so. Further, article 156 prohibits agents of telecom companies from disclosing the contents of electronic communications. In addition, article 127(a) provides that location data may only be processed after it has been anonymised or with the consent of users to the extent and for the duration necessary to provide a value-added service. Article 157 of the law prohibits the interception of electronic communications with the exception of where authorisation of the public prosecutor has been sought for purposes of ensuring the security of the State and public order; and enforcement of criminal and tax laws. The law does not explicitly provide for the process for lawful interception, the duration, or the persons responsible for its implementation.

Under article 21 of the Cybersecurity Act of 2020, operators of electronic communications networks and providers of electronic communications services are required to install traffic monitoring mechanisms, retain connection and traffic data for up to 10 years, and are liable for infringement of the fundamental rights and freedoms of users. Further, under article 97, providers of electronic communications or cryptology services are required to keep confidential the information received. Per article 180 of the law regulating electronic communications, a prison sentence of one to six months and a fine of 2,000,000 to 12,000,000 CFA francs (USD 3,600-21,000) is prescribed for anyone who violates professional secrecy and the secrecy of electronic communications, except in the exceptional cases provided for in the law.

The Law No. 9-2009 regulating electronic communications[82] provides under article 145 that the supply, transfer, and import of encryption tools for the sole purpose of ensuring authentication or integrity control, is free. However, even then the cryptology service provider must provide the National Agency for Information Systems Security (ANSSI) with the technical characteristics of the means of encryption as well as the source code of the software to be used. Also, article 146 of the law provides that the supply and importation of means of cryptology that are not exclusively for ensuring authentication or control should be declared to the regulatory authority.

80 *https://www.biometricupdate.com/202001/biometrics-and-digital-id-in-africa-genkey-in-niger-securiport-in-car-new-reseller-partner-for-daon-in-sa*

81 *SIM registration gets underway in the CAR, https://www.commsupdate.com/articles/2014/07/31/sim-registration-process-gets-underway-in-the-car/*

82 *Law No. 9-2009 of November 2009 regulating electronic communications, https://bit.ly/3oD54vC*

**Case study: Opposition surveillance**

*In the high-profile trial of a political opponent of President Denis Sassou Nguesso's regime, General Jean-Marie Mokoko, the prosecution requested to listen to some of his telephone conversations in order to prove the attempted coup d'etat charges against him. General Mokoko's lawyers considered the surveillance illegal, arguing that the conversations requested were outside the period during which the alleged events took place. During the trial, a prosecution witness gave evidence that General Mokoko purportedly used a DRC registered SIM card to communicate with his external collaborators in organising the coup.[83] It is not clear whether there was an official warrant for the interception of General Makoko's communications.*

Similarly, Law No. 26-2020 on cybersecurity[84] under article 34, provides that any organisation providing cryptology services intended for purposes other than those of authentication or integrity control must be approved by the ANSSI and should submit technical characteristics of the source code of the software to be used. Moreover, ANSSI is entitled to sanction any encryption service provider who fails to comply with the conditions imposed under the law, including through temporary or permanent withdrawal of a licence, as provided under article 38 of the law. Furthermore, article 177 of the electronic communications law punishes anyone who uses a means of cryptology without prior authorisation, or an expired authorisation with imprisonment for between three and six months, or a fine of between 1,000,000 to 5,000,000 CFA francs (USD 1,800-9,000). The law also empowers courts to confiscate the cryptology tools for the benefit of the regulator.

Law No. 29-2019 of October 10, 2019 on the protection of personal data lays down certain conditions, in article 23, for any cross-border transfer of personal data. For example, the third country must be able to ensure a sufficient level of protection of the privacy, freedoms and fundamental rights of individuals with regard to the processing of which such data are or may be subject; the prior informing of the commission in charge of data protection; and a sufficient level of privacy protection provided by the controller. These conditions are not mandatory if the transfer is one-off, not massive, if the data subject has consented, if the transfer is necessary to safeguard the public interest, or for court cases, as underlined in article 24. The conditions of cross-border transfer also do not apply if the controller offers sufficient guarantees of privacy as required by article 25.

Under article 4(a), the data protection law designates biometric data as a special category of personal data whose processing has special conditions. Biometric data is in the same category as genetic data, data on minors, and data on security measures. Under article 37 of the law, no controller or processor may handle biometric data without having obtained authorisation from the commission in charge of personal data protection. A data subject must consent before any processing of such data by a controller or its processor. The same law provides for circumstances under which personal data may be processed without necessarily requiring the consent of the subject. These circumstances include the performance of a mission of public interest or in the exercise of public authority, and the fulfilment of a legal obligation to which the controller is subject, per article 5. For investigative purposes, the public prosecutor or judge may collect or record data and communications in real time or compel the service provider to do so.

83 *Procès Jean-Marie Michel Mokoko: la Cour présente les preuves de l'accusation, https://tinyurl.com/29bxdxnr*

84 *Law n°26-2020 of June 2020 on cybersecurity, https://bit.ly/3x59glh*

On SIM card registration, article 130 of Law No. 29-2019 obliges telecom operators to register their subscribers. The provision requires operators of electronic telecommunication networks open to the public or their representatives, at the time of subscription to the telephone service, to identify subscribers for the purposes of defence and security, the fight against paedophilia and terrorism. These operators are required to retain electronic communications data, data they can be requested to disclose to "the individually designated and duly empowered agents of the national police and gendarmerie services specially entrusted with these missions". Notably, only "technical" data (such as the number called, the date and duration of the call) can be disclosed and not the content of the communication.

## 2.9 The Democratic Republic of the Congo (DRC)



Article 126 of the Framework Law No. 20/017 of 25 November 2020 on Telecommunications and ICT in the DRC provides for the right to privacy of correspondence sent by means of telecommunications and information and communication technologies. According to this law, the right to privacy may be limited at the request of the public prosecutor or with the authorisation of the Courts and Tribunals in the framework of the judicial investigation. The main justifications for the limitation include for reasons of internal or external security of the State, national defence or public order. Under article 129, a qualified agent under the authority of the ministry or from an operator can be required by the Public Prosecutor's Office at the Court of Cassation in order to install equipment to be used for interception and other similar operations.

The law does not specify who may apply for the warrant, or be authorised under the warrant or whether interception is allowed without a warrant. Article 128 provides that interception orders are valid for three months and are renewable if needed. The orders must specify all the elements for identifying the targeted connection, the offence that justifies it and its duration. Per article 179, unauthorised violation of the privacy of correspondence or any manipulation of personal data is punishable by penal servitude by the perpetrator, and a fine of 50 to 100 million Congolese Francs (USD 25,027-50,057). Further, under article 180, any interception, listening, recording, transcription by means of any device for the disclosure of a private communication or correspondence is punishable by one to three years' imprisonment, a fine of one to 10 million Congolese Francs (USD 501-5,005), or both.

The installation of CCTV has been adopted by citizens and private companies for their own security. However, there is no comprehensive regulation of the use of CCTV surveillance in public or private spaces.[85] The 2020 Telecoms and ICT law in Article 58(7) provides that remote surveillance and video surveillance systems in private spaces that are closed or open to the public are subject to prior declaration to the Regulatory Authority. The Regulator is required to deliver a certificate and inform the Minister about the declaration.

The circumstances that authorise the violation of privacy in the interest of national defence, national security, criminal investigations, the protection of public order and the prevention of crime, remain vague in the texts of the laws. Congolese government authorities make official information requests to telecom companies for either interception or for customer data. The 2017 Orange annual Transparency Reports on Freedom of Expression and Protecting Privacy indicated that the company received 981 customer data requests from the DRC authorities (up from 43 requests in 2014) and 26 interception requests. The data requested includes call details, customer identification data, geolocation, billing and payment data.

85 *Surveillance of public spaces and communications in the DRC, https://www.mediaanddemocracy.com/research.html*

## Case study: Opposition surveillance

*In January 2016 the DRC saw a massive deployment of video surveillance equipment in the capital, Kinshasa,[86] which led some observers to argue it was a strategy by former President Joseph Kabila to monitor and stifle dissent prior to the election. Around this time, several opposition leaders said their phones were under surveillance by the National Intelligence Agency.[87] "Uvda", an Israeli investigative media broadcast, accused President Kabila of employing an Israeli spy company, Black Cube, to spy on Congolese opponents at the end of 2015.[88] Similarly, several activists accused the government during the Kabila regime of using spyware to track opponents on social media as well as surveillance cameras in the streets of Kinshasa to monitor demonstrators during protests.[89]*

Regarding encryption, article 144 of the 2020 law on Telecommunications and ICT provides that cryptology (including cryptography and cryptanalysis) aims to ensure the protection and security of information, in particular for the confidentiality, authentication, integrity and non-repudiation of transmitted data through encoding or decoding. Under article 145, consular or diplomatic missions and the use of encryption related to state security agencies, are exempted from the regulations. Article 146a requires service providers to inform the telecoms regulatory authority of their intention to offer encryption services, upon which the regulator must issue a certificate of approval after noting the declaration and also inform the minister. The declaration by the service provider is required to include a description of the technical characteristics of the cryptology means, as well as the source code of the software used.

Article 148 provides that the conditions for granting approval to cryptology service providers and their obligations shall be defined by an Order of the Minister on the proposal of the regulatory authority. As per article 147, the order should also describe the modalities of using different sizes of keys. Article 146 provides that the use of encryption is free if used exclusively for ensuring authentication of a communication if they are based on secret codes managed by an approved body, or for controlling integrity of the transmitted message, but is subject to prior declaration.

The DRC does not have a data protection law, and only three articles (131, 132 and 133) in the 2020 telecoms law speak about protection of personal data. Article 133 provides that an order from the minister shall lay down, on the basis of proposals from the regulatory authority, the conditions and procedures for the collection, recording, processing, storage and transmission of personal data. The laws governing the finance sector have no specific provisions for where to host data or the conditions under which data can be transferred beyond the country's borders. Private banks attest that they store some of their customers' data overseas. It is the case of the Bank of Africa DRC (BOA-RDC): "In order to carry out these tasks, BOA-RDC may transfer the personal data collected to entities of the Bank of Africa Group, to its service providers and to its partners established outside the DRC. These data transfers take place under conditions and guarantees that ensure the protection of your personal data."[90]

86 RFI, Les Kinois réagissent à la présence de caméras de surveillance, https://tinyurl.com/39yrfhvh

87 J. Muyambo, Les services nous ont mis sur écoute, https://7sur7.cd/muyambo-les-services-nous-ont-mis-sur-ecoute

88 Spying in the DRC: an Israeli private intelligence agency implicated, https://tinyurl.com/yc5p7y37

89 RDC: les Kinois réagissent à la présence de caméras de surveillance, https://tinyurl.com/37rb38hk

90 Bank of Africa: Personal data, https://www.boa-rdc.com/pme/donnees-personnelles/

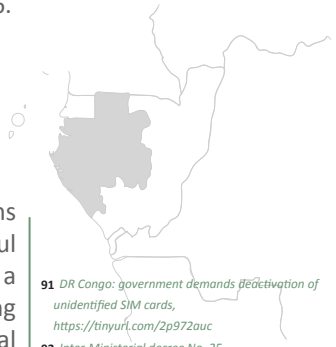
The 2020 telecommunications law requires the identification of subscribers. Article 92 obliges "any operator of a telecommunications network open to the public or any provider of internet access services" to identify "its subscribers at the time of subscription to telecommunications services". The operator "shall keep identification cards containing the minimum essential information". The law does not give clarity on what kind of information is to be collected; such details would be clarified by the minister as stated in article 95: "An order of the Minister shall determine the conditions and procedures for the identification of subscribers". Article 7 of the inter-ministerial order on SIM card registration requires telecom operators to respect the secrecy of information collected from their subscribers except for compelling reasons related to internal and external security or in the event of legal proceedings. In December 2015, the government instructed telecom operators to deactivate unregistered SIM cards for reasons of security and public order.[91] Whereas mandatory SIM card registration had been in effect since 2008, it did not mandate biometric data collection.[92]

As with personal data, the collection of biometric data is not regulated by any particular law. In turn, entities that collect biometric data are not subject to any particular law other than the general provisions dealing with privacy protection. According to article 50 of Law No. 04/028 of December 24, 2004 on the identification and registration of voters,[93] National Independent Electoral Commission (CENI) agents who disclose individual information relating to personal or family life for any purpose other than electoral purposes are subject to a penalty provided for in Article 73 of the Congolese Penal Code.[94] This code provides for a penalty of one to six months of imprisonment and a fine of 1,500 Zaïre (a currency that is obsolete). Article 56 of the same law states that the biometric data collected by CENI should be made available to the government, as it forms the basis of the national population file. Nothing is mentioned about how this data is stored or processed, let alone how long it is stored. The CENI has collected biometric data from citizens for voter identification purposes since 2006. The biometric voter's card also serves as a temporary ID and contains the holder's full identity, photo and fingerprint.

## 2.10 Gabon

Article 21 of the Order on Cyber Security and the Fight against Cybercrime of February 2018 prohibits any type of communications interception without consent, "except in the case of legal authorisation".[95] However, the law does not specify the procedure for lawful interception, which is permitted for judicial investigations. Unlawful interception is punished by imprisonment of five to 10 years and or a fine of 50to 100 million CFA francs (USD 85,902-171,804). Further, article 12 obliges intermediaries to install data traffic monitoring mechanisms on their networks, and to retain connection and traffic data for a period of 10 years in case it is required for judicial investigations. Article 31 requires Judicial Police Officers and agents authorised by the competent authority to "take an oath before the competent Court of First Instance ahead of investigations during which they may gain access to private and highly confidential documents". While there is no clear indication on whether the warrant is needed prior to any investigation, article 32 states that copies of data obtained can be destroyed on instruction of the Public Prosecutor for security reasons. The duration of the storage of such data before destruction is not specified.

Article 17 of the Order of February 2018 on eTransactions[96] obliges intermediaries to "identify the authors and publishers of content, to record and keep the content or information of all electronic transactions". Further, under article 17 of the Deliberation No. 090 of September 2020,[97] the National Commission for the Protection of Personal Data (CNPDCP) allows intermediaries to store and retain the identification data of anyone who has contributed to content creation or any of the services of which they are providers.



91 *DR Congo: government demands deactivation of unidentified SIM cards, https://tinyurl.com/2p972auc*
92 *Inter-Ministerial decree No. 25, https://tinyurl.com/h8mdhm4c l*
93 *Law No. 04/028 of December 24, 2004 on the identification and registration of voters, https://tinyurl.com/5bun28j8*
94 *Penal Code, https://tinyurl.com/mpnthsuj*
95 *Order No. 00000015 / PR / 2018 of 23 February 2018 on Cyber Security and the Fight against Cybercrime in Gabon, https://bit.ly/3kF2W5c*
96 *Order No. 00000014 / PR / 2018 of 23 February 2018 regulating electronic transactions in Gabon, https://bit.ly/3ceRLvr*
97 *Deliberation No. 090 / CNPDCP of 22/09/2020 bearing of the National Commission for the Protection of Personal Data relating to the bill on the regulation of eTransactions in Gabon, http://journal-officiel.ga/17800-090-cnpdcp/*

**Case study: Elections related surveillance**

*The Gabonese Presidency has had a communications interception centre, the Silam, for decades, which purportedly transmits regula interception reports to President Ali Bongo.[98] Benefiting from French expertise and utilising software such as "Cerebro" provided by Amesys, Silam "handles everything from wiretapping transcripts, text message interceptions and WhatsApp to email and social media monitoring". In 2016, the secret services are alleged to have intercepted the communications of European Union elections observers.[99] The recorded conversations revealed heavy suspicions of electoral fraud and malpractice, prompting the government to accuse the observers of corruption and supporting the opposition. Attacks by the partisan press increased to the point where one of the observers threatened with death was exfiltrated.[100]*

98 *Inside Africa's increasingly lucrative surveillance market, https://bit.ly/30yPZ5Q*
99 *Watergate in Gabon: how Bongo spied on emissaries from Europe, https://bit.ly/3cnZJTb*
100 *Ali Bongo spied on European observers, https://bit.ly/32e5PUn*
101 *Order No. 00000015 on cyber security and the fight against cybercrime https://bit.ly/3kF2W5c*
102 *Order No. 00000014 on eTransactions, https://bit.ly/3ceRLvr*

Article 28 of Order No. 00000015 on cyber security and the fight against cybercrime,[101] provides that the use, supply, import and export of cryptology is free when exclusively meant to ensure authentication of a communication or to control integrity of the transmitted message. Encryption for other purposes is subject to prior declaration and authorisation. Cryptology means and services that aim to ensure confidentiality functions must be authorised. Under article 37, a natural or legal person providing cryptography services aimed at ensuring a confidentiality function are required to deliver agreements allowing the decryption of the data to Judicial Police Officers or to the authorised agents, at their request. Moreover, article 34 provides that encrypted data must be decrypted during an investigation upon request by the Public Prosecutor, the examining Magistrate or the trial court.

Meanwhile, article 83 of Order No. 00000014 on eTransactions[102] subjects the import, export or supply of a means of cryptology for ensuring confidentiality functions to prior authorisation from the competent authority and to a special import or export authorisation. Also, article 113 requires the approval of the cryptology service provider by the competent authority. Under articles 82 and 84, the use, supply, import and export of means of cryptology ensuring exclusively authentication or integrity control functions is free. However, the supplier, importer or exporter is required to avail to the competent authority a description of the technical characteristics of the means of cryptology.

Under Order No. 00000015, the failure to seek prior authorisation attracts a penalty of imprisonment of between six months to five years, a fine of between one million and five million CFA francs (USD 1,720-8,600), or both. Also, under article 48 of the same law, the failure to comply with the requirement to deliver agreements is punishable with imprisonment of between three months to two years, a fine of 500,000 to 2,000,000 CFA francs (USD 860-3,440) or both. Further, under article 52, anyone who puts at the disposal of others a means of cryptology whose use has been banned, is liable on conviction to imprisonment for between one to five years, a fine of one million to 20 million CFA francs (USD 1,720-USD 34,399), or both.

Under article 94 of the Law No. 001/2011 on the protection of personal data, data may be transferred to another state only if that state ensures a sufficient level of protection of the privacy, freedoms and fundamental rights of individuals. The National Commission for the Protection of Personal Data (CNPDCP) prohibits any data transfer to a country that does not provide a sufficient level of protection (article 96). Under article 36 of Order No. 00000015 on cyber security and the fight against cybercrime, judicial authorities may issue warrants, both national and international, to any legal or natural person to search for data related to a cybercrime offence, when at least one of the acts was committed in Gabon or one of the perpetrators or accomplices is located on Gabonese territory. Subject to the rules of reciprocity between Gabon and foreign countries bound by a judicial cooperation agreement, warrants are executed in accordance with the provisions of the legislations in force.

Pursuant to article 123 of the eTransactions order, provision of electronic services in Gabon is not restricted to a member country of Economic Community of Central African States (ECCAS) or Central African Economic and Monetary Community (CEMAC), subject to reciprocity. Article 54 of the law on the protection of personal data requires authorisation from CNPDCP for automated processing of biometric data for identification purposes. Under article 56, the processing of several categories of personal data including those “carried out on behalf of the State, which relates to the biometric data necessary for the authentication or verification of the identity of persons”, is authorised by decree taken in the Council of Ministers, after a reasoned and published opinion of the CNPDCP.

By Deliberation No. 243 of October 2014 requiring the identification of subscribers of mobile telephone operators, the Regulatory Authority for Electronic Communications and Posts (ARCEP) prohibits “the sale of pre-activated SIM cards throughout the national territory” and requires the registration of all subscribers to mobile networks. The requirements for SIM card registration include any identity document containing the photo of the subscriber, their physical presence, professional information, and the physical address.

In 2017, the Gabonese Minister of the Interior announced the "Iboga" project (official biometric identity of Gabon) aimed at centralising individuals’ civil status and the national electoral register through the National ID Card.[103] To date, the project is yet to be implemented but Gabon's 2022-2024 Macroeconomic and Budget Framework Document[104] reiterates its establishment. Meanwhile, biometric enrolments authorised by the CNPDCP continue unimpeded and in the absence of a regulatory framework. For instance, the National Social Security Fund of Gabon, initiated a biometric enrolment process for retirees in April 2018.[105] Further, a directive of August 2021 from the CNPDCP authorises the transfer of data of personnel and policyholders of the firm Axa Gabon to Morocco and the use of a biometric identification device for personnel.[106]

## 2.11 Guinea Conakry

Law No. 2016-037 on Cybersecurity and Personal Data Protection[107] provides for lawful surveillance “in the event of a justified suspicion or a proven offence”, by sworn officers of the Centre for the Information Systems’ Security or police officers upon requisition or warrant from the prosecutor and following decision of the judicial authority (article 94). Under articles 96 to 105, the law permits a "competent authority" to require legal or natural persons who offer internet access, to carry out surveillance on their subscribers’ activities, without specifying the role of the judicial authority in triggering the surveillance procedure.

Article 67 requires users accessing internet services from a cybercafé to be identified by the cybercafé operators, in advance. This prevents users from enjoying their rights of anonymity and pseudonymisation, without specifying the liability of cybercafé operators regarding the personal data collected. Article 36 of the Telecommunications Act[108] requires the identification of all telecommunication service



103 *Gabon draws attention to the plan to establish a new national biometric identity card, https://bit.ly/30wRZvP*

104 *Document de Cadrage Macroeconomique et Budgetaire 2022-2024, https://bit.ly/2YUfHRY*

105 *Biometric registration of retirees, https://tinyurl.com/2p8twxcn*

106 *Deliberation N ° 037 / CNPDCP of 08/11/2021, http://journal-officiel.ga/17768-037-cnpdcp/*

107 *Guinea, Law No. 2016-037 of 28 July 2016 on Cybersecurity and Personal Data Protection in the Republic of Guinea, https://bit.ly/3CMAIMG*

108 *Guinea, New Telecommunications Law No. 018 of August 13, 2015, https://bit.ly/3iglMyA*

subscribers. It also requires operators to transmit the identification data to the "competent authorities" upon request from the public prosecutor's office. Based on this, the Guinean ICT regulator (ARTP) issued a decision[109] requiring mobile subscribers' identification from December 31, 2020. A penalty of 10 million Guinean francs (USD 1,000) is applied by the ARTP for any number or internet service activated without subscriber registration (article 11).

Law No. 2016-037 prohibits fraudulent interception, falsification or unauthorised modification of computer data and punishes the offences with imprisonment of five to 10 years, a fine of 500 million to one billion Guinean francs (USD 51,487-102,973) under articles 10-13. Failure to comply with an order from a competent authority under article 96 to 105 attracts a fine of 150 million to 700 million Guinean francs (USD 15,450-USD73,000).

According to article 57 of the cybersecurity and personal data protection law, the importation, sale or use of encryption is banned unless authorised by the government. Under article 49, an authorised cryptology service provider is obliged to hand over any data if requested by the Personal Data Protection Authority. The penalty for using encryption without authorisation is imprisonment for between one and five years, a fine of 150 to 600 million Guinean francs (USD 15,445-61,784), or both. Under article 28, any cross-border data transfer is subjected to control by the data protection authority. Data transfer to a third country may only be authorised if the third state ensures a higher or equivalent level of protection of privacy, fundamental rights and freedoms of individuals with regard to the processing of which these data are or may be the subject.

Despite the guarantee that the processing of biometric data is subject to prior authorisation by the competent authority,[110] biometric databases are used in various government and non-government services. Biometric data is collected for enrolment in the electoral register, for national identification cards, and for SIM card registration. Article 2 of the Decree D/95/254/PRG/SGG of September 1, 1995 establishing a New National Identity Card and a New Consular Card, requires that the holder of national ID must affix the imprint of their left index finger and signature, as well as a recent photograph with bare head. The implementation of the biometric ID card reportedly started in late 2020,[111] with a target of covering 80 percent of the population by 2024 and integrating with the regional ECOWAS scheme.[112] The data collected for the ID includes all fingerprints, a photo for facial recognition, physical address, and the extract of the birth certificate from which the rest of the information is copied.[113]

Meanwhile, although the new Electoral Code[114] does not mention the collection of biometric data, for several years the country has attempted to build a biometric register. However, due to challenges of data collection and issuance of biometric cards for all the voters, the biometric cards were not used for the 2010 and 2015 elections.[115]

**Case study: Opposition surveillance**

*In March 2020, the Director of the Judicial Police, Commissioner Aboubacar Fabou Camara, declared that he had wiretapped some members of the opposition party - the National Front for the Defence of the Constitution (FNDC)- and to have intercepted more than 200 telephone calls in 24 hours.[116] Following the Commissioner's allegation, lawyers from the opposition party lodged a complaint with the Public Prosecutor, for invasion of privacy and individual freedoms.[117] The Commissioner was then summoned to appear at a court hearing in Conakry in September 2020.[118]*

109 *Decision D/001/ARPT/CNRPT/2021 on the Identification of mobile Subscribers, https://bit.ly/3l0RSjA*
110 *Article 7 of the Law No. 2016-037, Op. cit.*
111 *Guinea: Biometric ID card - Prime Minister invites citizens to leverage modernization, https://bit.ly/3A2JvrR*
112 *Digital ID in Africa this week: Biometric ID for Guinea, continued ID controversy for Côte d'Ivoire, https://bit.ly/3l3agbq*
113 *Release of biometric identity cards: how to obtain it?, https://bit.ly/3DvWHrA*
114 *Decree D/2017/193/PRG/SGG promulgating the Organic Law L/2017/039/AN of 24 February 2017 on the Revised Electoral Code of the Republic of Guinea, https://bit.ly/3kS626G*
115 *Guinea: information on the voter card, including how to apply, its appearance and the information on the card, https://bit.ly/3mQyG7J*
116 *Are Guinean citizens tapped? The answer of the Minister of Telecommunications, https://bit.ly/3lSPOJ9*
117 *Guinea/Telephone tapping: the FNDC warns operators and accuses the authorities of wanting to shutdown the internet, https://bit.ly/3oDMXar*
118 *TPI of Dixinn: summoned to appear, Commissioner Fabou reacts, https://bit.ly/3FOA83r*

# 2.12 Ivory Coast

Article 5 of the Law on Orientation of the Information Society of December 2017[119] prohibits communication interference, regardless of the sender, recipient, type of content, device, service or application. In addition, the Data Protection Act of June 2013 also prohibits the unlawful interference with privacy, family, home, or correspondence. Article 42 of the Cybercrime Act requires prior identification of every person accessing the internet on Ivorian territory. Cybercafé operators are required to "carry out this identification according to the procedures set by decree". The law does not provide for how this identification data should be collected, processed, secured or duration of storage. Further, article 72 requires service providers to retain data relating to subscribers and protect its integrity for a period of 10 years.

Under articles 74 to 76 of the Cybercrime Act, the competent authority,[120] on requisition of the prosecutor or order of the examining magistrate, may carry out seizures and searches of an information system or a computer storage medium, obtain traffic data through intermediaries within the framework of an investigation and in accordance with the Code of Penal procedure. Article 71 defines the competent authorities as "judicial police officers, experts approved by the courts and any other person whose skills are required, oath taken beforehand". The data obtained can be stored "as long as the investigation goes on". Article 75 empowers the competent authority to access data relevant to the ongoing investigation and stored in another information system, as long as the data are accessible from the initial system or available for the initial system.

Articles 46, 47, 50 and 52 provide that intermediaries are not obliged to monitor the information they transmit or store, nor to research facts or circumstances revealing unlawful online activities. However, the judicial authority may require intermediaries to provide "targeted and temporary surveillance of the activities carried out through their services", or to "prevent damage or to put an end to damage caused by the content of an electronic communication service". The law does not further specify the duration or the conditions of such surveillance.

The Cybercrime Act, under article 8, prescribes punishment for anyone who intercepts or attempts to fraudulently intercept computer data by technical means during their non-public transmission with five to 10 years' imprisonment and a fine of 40 to 60 million CFA francs (USD 70,743-106,115).[121] Further, under article 24, anyone who processes personal data by fraudulent, unfair or illicit means is liable to imprisonment of one to five years and a fine of five to 100 million CFA francs (USD 8,843-176,853). Failure to store subscriber data, attracts a fine of 10 to 50 million CFA francs (USD 17,685-88,426).

Article 6 of Decree No. 2014-105 defines the conditions for providing cryptology services.[122] The use of cryptology means and services to ensure confidentiality functions is only free if the service provider is approved by the Telecommunications Regulatory Authority (ARTCI). The ARTCI is obliged to ensure that the authorised service providers' encryption services are not contrary to public order and do not undermine the interests of national defence, internal or external security of the state. Under article 16 of the law, competent administrative or judicial authorities can access secret codes of encrypted data upon request to the ARTCI, or order decryption of data through the help of ARTCI.

Under articles 7 and 8 of the 2014 law on encryption, the use of the means and services of cryptology beyond 32 bits for confidentiality is subject to authorisation. Further, the supply or import of cryptology means that is not exclusively used for ensuring authentication or control of the integrity, is subject to prior declaration. Also, the licences of service providers have to be renewed by the ARTCI every three years.

119 *Law No. 2017-803, Op. cit.*

120 *Article 71 defines the competent authorities as judicial police officers, experts approved by the courts and any other person whose skills are required, oath taken beforehand*

121 *Law No. 2013-451 of June 19, 2013 on the fight against cybercrime: https://tinyurl.com/563y8uka*

122 *Decree No. 2014-105 of March 12, 2014 defining the conditions for providing cryptology services, https://www.artci.ci/images/stories/pdf/decrets/decret_2014_105.pdf*

In addition, article 47 of the eTransactions Act 2013 subjects the supply of cryptology services to conditions defined by the Council of Ministers. Article 48 requires professional secrecy while also holding cryptology services providers liable in the event of an attack on the integrity, confidentiality or availability of data. Under article 49, ARTCI can prohibit the exercise and withdraw the means of cryptology from a service provider who does not comply with their obligations. Moreover, article 20 of the Cybercrime Law of 2013 provides that anyone who does not respect a ban on exercising the profession of cryptology services provider or the obligation to withdraw cryptology means, can be published with imprisonment for between one to five years and a fine of between one to 10 million CFA francs (USD 1,768-17,685).

Under article 7 of the Data Protection Law of 2013, the transfer of personal data to a third country is subject to prior authorisation from the data protection authority. Article 26 specifies that "the controller may not be authorised to transfer personal data to a third country unless this State ensures a higher or equivalent level of protection of the privacy, freedoms and fundamental rights of individuals with regard to the processing to which these data are or may be subject." Under article 2 of Decree No. 2015-79 of February 4, 2015,[123] only natural persons residing in Ivory Coast or legal persons governed by Ivorian law can complete a declaration and present an authorisation request for processing personal data. Under article 8, each data controller establishes and submits to the ARTCI an annual activity report relating to the transfer of personal data to third countries, and the authority can impose administrative and pecuniary sanctions against data controllers who do not comply with these obligations.

Pursuant to the 2016 law on the Fight against Money Laundering and the Financing of Terrorism,[124] the National Financial Information Processing Unit (CENTIF) can disclose the identification data[125] of customers of banking institutions and the history of related financial transactions to a CENTIF counterpart in an ECOWAS member state as part of an investigation, following a duly motivated request (Article 76). Similarly, under article 78, the CENTIF can, "subject to reciprocity, exchange information with the financial Intelligence Services of foreign states responsible for receiving and processing suspicious transaction reports, when the latter are bound with similar professional secrecy requirements". Disclosures by CENTIF are subject to prior authorisation by the Minister responsible for finance, and foreign state guarantees of a sufficient level of protection of privacy as well as the fundamental rights and freedoms of individuals, in accordance with the regulations in force. Article 78 also provides that this cross-border data sharing may be prohibited if it infringes the state sovereignty or national interests as well as security and public order.

The Data Protection law subjects the processing of biometric data to prior authorisation from the protection authority. That authorisation is requested by the controller or their legal representative and is not exempt from liability towards third parties.[126] Article 3 of the Decree No. 2017-193[127] requires telecom operators and service providers to identify their subscribers through collection and storage of identification data. Under article 13, the identification data collected includes photo, date and place of birth, profession, email and physical address, plus the biometric national identity card or biometric national driving licence or biometric passport – which all enclose fingerprints, photo, signature, names, parentage.[128]

Article 14 specifies that "subscriber data is kept up to date and can only be accessed by third parties in the event of an investigation or judicial information, upon written request from the competent judicial authority, and by agents appointed by ARTCI as part of their control mission, in accordance with the regulations in force". Under article 15, the operator is required to collect and keep copies of documents and data relating to subscribers' identification throughout the duration of their subscription and, at least, three years from the end of the subscription.

123 *Decree n ° 2015 -79 of February 04, 2015, fixing the modalities for filing declarations, submitting requests, granting and withdrawing authorizations for the processing of personal data, https://www.artci.ci/images/stories/pdf/decrets/decret_2015_79.pdf*

124 *Law No. 2016-992 of November 14, 2016 on the Fight against Money Laundering and the Financing of Terrorism, https://bit.ly/3mSu80E*

125 *Under article 26, customers' identification data contains a valid official document containing his photo, address, names, date and place of birth.*

126 *Law No. 2013-450, Op. cit., Article 7.*

127 *Cote d'Ivoire, Decree No. 2017-193 identifying subscribers of Telecommunications / ICT services open to the public and users of cybercafés; https://bit.ly/3oe9kmT*

128 *See the Law No. 2019-566 of June 26, 2019 establishing a national biometric identity card; https://bit.ly/3zyQZTr and the related Decree No. 2019-945 of November 13, 2019 on the implementation modalities of Law No. 2019-566 of June 26, 2019 establishing a national biometric identity card, the Decree No. 2012-224 of February 29, 2012 granting diplomatic passports with biometric chips and biometric service passports with electronic chips, https://bit.ly/3aAQzBL*

## Case study: Surveillance for safety or state control?

*The Ivorian government has been operating video surveillance in the capital Abidjan since 2013, for safety and security, without this being supported by a law.At the time of its establishment, the surveillance command centre known as the Center for the Coordination of Operational Decisions was equipped with screens linked to cameras, 60 all-terrain pick-ups and750 staff.[132] Since then, the project has been extended to other territories.[133] The deployment of technology for surveillance in Ivory Coast is perceived as a means of state control. Illustrative examples include arrests by the Directorate of Territorial Surveillance between 2010 and 2013 of bloggers for dissemination of information regarding a stampede at New Year Festivities and alleged suspects of armed attacks against state symbols based on SMS messages.[134] As of September 2021, the country had installed video surveillance as part of road traffic safety and penalty enforcement.[135]*

Under article 2 of the Decree No. 2016-674,[129] SNEDAI Groupe in a partnership contract with the Ivorian government is authorised to process personal data on behalf of the Institute for Social Welfare under the National Fund of Health insurance (IPS-CNAM),[130] for establishing a biometric enrolment system for universal medical coverage. Under article 3, collected data includes the names, gender, date and place of birth, fingerprints, physical address, postal address, email, administrative or professional registration number, passport photo, and profession. The storage and retention of data by SNEDAI Groupe is restricted to the duration of the data subject's entitlement to the Universal Health Coverage Scheme.[131]

In 2016, the ARTCI[136] authorised the Socoprim Company to collect, store and process data from video surveillance of the Henry Konan Bédié Bridge. The data includes the identification of bridge users (images of people, licence plate number as well as make, model and colour of vehicles) and location data (date, arrival and departure times of bridge users, place of recording, the various movements detected by cameras in monitored places). In its Decision No. 2016-0205 of November 2016,[137] ARTCI stated that data processed by the Socoprim Company shall be kept for a maximum period of 30 days, and can only be disclosed to its authorised agents, the Public Prosecutor and judicial police officers provided with a requisition.

According to an INTERPOL report, biometric data from suspected terrorists arrested during joint operations by Côte d'Ivoire and Burkina Faso are being shared in order to uncover possible links to other terrorist attacks and groups in the region and beyond.[138] This happened with Operation Comoé which took place in the two countries on May 24, 2020, and resulted in the arrest of 24 suspects in Burkina Faso and 16 in Côte d'Ivoire, who were then handed over to intelligence services. The same happened with an operation which resulted in the arrest of around 30 suspected terrorists, carried out after a terrorist attack in Kafolo (Côte d'Ivoire) on June 11, 2020 in which several soldiers were killed.[139]

129 *Cote d'Ivoire, Decree No. 2016-674 of August 31, 2016 authorising the processing of personal data for the implementation of a biometric enrollment system for those insured with universal health coverage, https://bit.ly/3i1qHTI*

130 *National Health Insurance Fund*

131 *Decree No. 2016-674, Article 6.*

132 *Côte d'Ivoire: an operational center to streamline police surveillance in Abidjan, https://bit.ly/3kmZMUc*

133 *Securing of the City of Abidjan by CCTV cameras; https://bit.ly/2YIiD48*

134 *Jean-Jacques Maomra BOGUI and N'Guessan Julien ATCHOUA, Regulating the use of ICT in Côte d'Ivoire: between identification and fears of profiling populations, https://doi.org/10.4000/terminal.1468*

135 *Video surveillance at the service of road safety in Côte d'Ivoire, https://bit.ly/3DEEd86*

136 *Appointed as Data Protection Authority by the Data Protection Act*

137 *Decision No. 2016-0205 of the protection authority of the Republic of Côte d'Ivoire of 22 November 2016 authorising the processing of personal data by the company SOCOPRIM "video surveillance", https://bit.ly/2YJB2Ng*

138 *Biometric data to help identify potential links with attacks across the region and beyond, https://bit.ly/3BdPZ92*

139 *Biometric data to help identify potential links with attacks across the region and beyond, https://bit.ly/3BdPZ92*

# 2.13 Lesotho

The Lesotho Communications Rules (Administrative) 2016[140] provide for personal data protection and privacy unless the customer has provided consent under section 43(1)-(2). In addition, section 43(3) requires licensed operators to cooperate with law enforcement officials with a court order from a competent jurisdiction. The National Security Services (NSS) Act 1997[141] in section 27(2) empowers the minister to give direction for the interception of communication if convinced by an application from an authorised NSS officer that there is an offence that has been, is being or is likely to be committed, and is a threat to the national security or that the information has or could have a bearing on the functions of the NSS. The minister is required to sign the interception authorisation which is valid for a period of six months and can be extended for a similar period if the minister finds it necessary as per section 27(3). With respect to urgent requests, section 27(4) empowers the NSS Director General or an officer authorised by the Director General to sign the authorisation if the minister has expressly authorised its issue. In such a case, the authorisation is valid for two working days.

The proposed Communications (Compliance Monitoring and Revenue Assurance) Regulations 2021[142] seek to "provide for the conditions, requirements and procedures for monitoring telecommunications traffic in Lesotho through the installation of tools and systems." Regulation 12(3) empowers the Lesotho Communications Authority (LCA) to carry out the "necessary regulatory surveillance" for the detection and handling of fraudulent telecommunications traffic. Regulation 10(1) requires licensees to submit to the Authority Call Data Records (CDR) or information related to telecommunications traffic every month. Also, regulation 16(2) permits the Authority to share the collected information with any law enforcement or national security agency, court of law or for any national security purpose, and there is no requirement for a court order or warrant before the information is shared.

Section 44(f) of Lesotho Communications Act 2011 punishes unauthorised interception of communications with a fine of up to Lesotho Loti (LSL) 50,000 (USD 3,500), imprisonment of up to five years, or both. Any contravention of the provisions of the Communications (Compliance Monitoring and Revenue Assurance) Regulations 2021 attracts a fine of up to LSL 50,000 (USD 3,500), imprisonment of up to five years, or both. The proposed Computer Crimes and Cybersecurity Bill 2021 which is under review,[143] under clause 23 punishes illegal interception with a fine of up to LSL 10 million (USD 674,791), imprisonment of up to 15 years or both. Clause 46 punishes any person who unlawfully or without authority intercepts electronic messages or processes through which money or information is being conveyed. This bill has been withdrawn and the responsible Minister instructed to review it.

The Data Protection Act 2011 defines biometric as a technique of personal identification that is based on physical characteristics including fingerprinting, DNA analysis, retinal scanning, and voice recognition. The act specifies in section 16 that personal information be collected directly from the data subject and be processed only for the reason it was collected, not anything else. Lesotho has not yet implemented e-voting for national elections, but the electoral register is digitised, and the system collects fingerprints.

Section 3(1) of National Identity Cards Act 2011 provides for the establishment of a registry to maintain the records of personal information on all citizens eligible for national identity cards. The registry is digitised, but the country is not offering digital IDs yet. Section 4(6) provides for collection of fingerprints in the case of a person who is 16 years or older. Under section 13, one is eligible for an identity card after they have attained the age of 16. In section 6(2), the Act permits access to information contained in the registry by some third parties, including government departments. Section 7 prohibits communication or publishing of the registry information for any other purposes except provided for by the Act. Anyone who contravenes these provisions is liable to a fine of LSL 25,000 (USD 1,700) or to imprisonment of 15 years or both.

140 *Lesotho Communications Rules (Administrative) 2016, https://www.lca.org.ls/download/lesotho-communications-authority-administrative-rules-2016/*

141 *National Security Services Act 1997, https://lesotholii.org/ls/legislation/act/1998/11/nssa1998285%5B1%5D.pdf*

142 *Communications (Compliance Monitoring and Revenue Assurance) Regulations 2021, https://www.lca.org.ls/public-consultations/*

143 *Facebook, https://www.facebook.com/581773632001354/posts/1998213150357388/*

Registry information sharing with third parties is already in place as provided by the law. For instance, for an individual to qualify to be a "tier two" or standard mobile money user (Mpesa or Ecocash), which provides for increased transaction limits, one must provide their ID number which the mobile money providers authenticate against the Registry, and only then would one be upgraded.

In May 2021, the LCA issued the Communications (Subscriber Identity Module and Mobile Device Registration) Regulations 2021 which require that all customers of telecom services in Lesotho register SIM cards and mobile devices that use SIM cards. The information required under section 21(1)(a) for individual registration includes a national identity document or number, mobile device and proof of ownership. The information is verified by fingerprint, against the national identity card registry. Section 9 permits security agencies access to the central database with a written request, which must include the purpose for which the information is requested, to the Authority from an official of the requesting agency and the official's rank must not be below Assistant Commissioner of Police or equivalent. The regulations met with a lot of public backlash and the Portfolio Committee recommended in September 2021 that they be revoked and revised.[144]



## 2.14 Liberia

The National Security Reform and Intelligence Act of 2011[145] under Section 6(a) authorises the National Security Agency (NSA) to collect, retain, analyse and disseminate for lawful government purposes information concerning citizens and non-citizens of Liberia. These activities are to be done in accordance with the procedures established by the Director of the Agency and approved by the Ministry of Justice.

The law permits the collection of information through lawful intelligence and surveillance activities, lawful physical security investigation, and information concerning persons who are reasonably believed to be potential sources or contacts for the sole purpose of determining their suitability or credibility. Section 9(a) provides that if there are reasonable grounds to believe that a warrant is required in order for the agency to carry out its duties and responsibilities under the act, the Director or designated employee shall apply for the issuance of a warrant for that purpose. The application is made in writing to a judge.

The Act provides that the electronic surveillance and physical search may only be conducted by the NSA upon order of a court of competent jurisdiction as specified under Section 9. The law requires that "only the judge of a court of competent jurisdiction shall authorise the interception of communication under this act and that, "all warrants shall specify the purpose for which it has been issued and to whom". The application to a court of competent jurisdiction for a search warrant shall be done by the Attorney General of the Republic. Section 7(c) states that, in furtherance of the authority and responsibility of the Director of NSA to protect intelligence sources and methods, and other classified information, the NSA shall be exempted from the provision of any laws which require the public disclosure of the organisation operational activities, names, official titles, salaries, budget or number of people employed by the NSA.

Meanwhile, section 50 of the Liberia Telecommunication Act of 2007 states that "for the purposes of tracing and locating a source of harassing, offensive or illegal telecommunications, or as otherwise provided under the laws of Liberia: (a) the Liberia Telecommunications Authority (LTA) or other duly authorised authority in Liberia may direct a service provider to monitor telecommunications to and from a customer's telephone and the service provider shall comply with any such direction; (b) the service provider shall provide the LTA or other duly authorised authority in Liberia the information resulting from its monitoring of the customer's telecommunications, including the telephone numbers or other electronic identifiers that indicate the source of the harassing, offensive, or illegal telecommunications and the time and dates of occurrence of such telecommunications".

144 *Lesotho rejects Communications (Subscriber Identity Module & Mobile Device Registration) Regulations 2021, https://tinyurl.com/2p958d36*

145 *National Security Reform and Intelligence Act of 2011, https://www.nsa.gov.lr/web/web/sites/default/files/documents/NSA%20ACT%200F%202011.pdf*

Journalists, civil society activists have alleged that the NSA has often spied on them but there is no record to show that any of these accusations have ended in court so far. In 2016, Representative Acarous Gray, then an opposition member of the Parliament, alleged that businessman and politician Benoni Urey, leader of the All Liberian Party (ALP) and shareholder in Lonestar Cell MTN, was using his influence to use subscribers' information for political gain. Lonestar Cell MTN denied the allegations.[146]

Liberian law does not explicitly regulate encryption. However, there are some provisions which can be used in regulating encryption. For instance, under the Telecommunication Authority Act of 2007, article 61, the LTA may issue regulations, rules or orders: (a) requiring that certain types of telecommunications equipment be certified or approved prior to being imported, commercially supplied or attached to any telecommunications network; (b) identifying criteria for certification and/or standards for approval of telecommunications equipment for use in connection with telecommunications services or telecommunications networks; and d) establishing a register of certified or approved types of telecommunications equipment, criteria for certification and standards for approval. Under article 69(1), service providers shall comply with any directions, regulations, rules, orders or other requirements communicated by the Attorney General, following consultation with the LTA, regarding access to any part of the service provider's telecommunications network or telecommunications services or related information in connection with national security requirements or the detection or prevention of illegal activities.

Liberian legislation does not contain data localisation requirements. The country does not have a dedicated data protection law although other legislation contains some provisions relevant to data protection. Section 5.2.1 of the National ICT Policy mentions the National Data Centre, a core infrastructure for supporting e-government that seeks to consolidate services, applications, and infrastructure to provide efficient delivery of e-government services through a common platform seamlessly supported by core connectivity infrastructure. However, it does not restrict hosting of data and other related services to Liberian territory, nor does it mention cross-border data transfer.

Regarding biometric data, the Liberian government enacted the National Identification Registry (NIR) Act in 2011 to establish and maintain the National Biometric Identification System (NBIS). The law designated the NIR as the body responsible for issuing a biometric-based identification card to each citizen and resident in Liberia. The NIR is mandated 'to collect, organise, store, secure, and grant access to secure biometric data to be collected from individuals applying for national biometric identification cards; and other key documents such as Passport, Drivers license and Social Security cards'. To obtain a biometric national identification card, an applicant must submit their birth certificate, fingerprint, photograph, proof of citizenship of parents, date of birth, place of birth, gender, colour of skin, hair and eyes (section 8.1). Citizens who complete registration are issued a National Social Security Number and a Biometric Citizen Identification Card.

Section 3(2)(j) of the Act states that the NIR shall 'ensure that the collection and release of data are in conformity with the Freedom of Information laws of Liberia and do not in any way infringe on the right to privacy guaranteed by the Constitution'. Under 9(2), all biometric information collected "shall be securely stored with adequate technical and procedural safeguards maintained to ensure the integrity of both the biometric data and the conditions of access thereto" and, according to section 9.3, "all biometric information collected under this Act shall be encrypted." Under section 10(1), the law grants the right to everyone to have access to the biometric and other information obtained from them and stored under this Act. The right of access granted here includes the right to review and connect any erroneous information.

Under 10(2), the NIR determines protocols under which third parties may access the biometric information. However, government agencies "may at any time be granted access to specified biometric information upon the production of a warrant or court order that specifies the information to be accessed."

146 *Lonestarcell Responds to Call Monitoring Allegation, https://tinyurl.com/2p88y4kd*

Meanwhile, the 2020 Order Implementing the SIM Card Registration Regulations requires "compulsory and verificable registration" of all activated SIM/RUIM cards and SIM/RUIM card users and establishes subscriber databases managed by telecom service providers. SIM card registration became mandatory January 1, 2021. According to the Order, the implementation of the SIM Card Registration Regulation "will improve national security in the country, provide a platform for the efficient functioning of other electronic communications services including mobile money transfer and other such services, enhance the chance of subscribers replacing their SIM cards in the event of loss, minimise the opportunity for communication frauds (grey routing of calls) as operators are mandated to activate only registered SIM/RUIM cards on their networks, and ensure the creation of a reliable database of subscribers by operators."

The Amended SIM Card Registration Regulations 2020 provide for the use of the NIR verification platform to verify the authenticity of the identity documents presented during registration (objective 1.3(d)). The Regulations define biometric information as "the fingerprints and/or facial image of a subscriber in accordance with the Data Dictionary provided by the LTA for the registration of subscribers". While service providers are obligated to maintain the confidentiality of subscribers' information, under section 8.5 this information may be released to government authorities in keeping with section 52 of the Telecommunications Act of 2007 or by an order of a court of competent jurisdiction.

## 2.15 Madagascar

In Madagascar, Law No. 2016-017[147] of 22 August 2016 which modified some provisions of the Penal Code in section 9 empowers an investigating judge to order the surveillance of bank accounts, access to systems and phone tapping during investigation of money laundering or financial crimes. However, Law No. 2016-019[148] on the Media Communication Code, in article 12, provides that individuals classified as 'information sources' of journalists and their collaborators should not be subjected to either digital or physical surveillance unless the required information is required to prevent the commission of an offence under article 11 and the request is sanctioned by a judicial authority.

Articles 129 and 130 of the Penal Code[149] provides that judges may issue warrants for police to intercept communication required for their investigation if it concerns bank accounts or phone conversation historical data. Service providers are not required to disclose incerceptated data without a warrant. In emergency situations, a warrant is not required. However, in such emergency cases, service providers can only disclose correspondent data. Under article 103, a warrant is valid for a maximum of three months.

Article 13 of the Law No. 2014-006 on cyber criminality[150] punishes unauthorised interception of computer data with a term of imprisonment of between two and 10 years, a fine of between two million Ariary (USD 517) and 100 million Ariary (USD 25,775), or both. Under article 6, the penalty for illegal access to an information system is a fine between 100,000 Ariary (USD 277) and 10 million Ariary (USD 2,577). Under article 27, the maximum duration for communication and information operators to retain data is one year.

Article 16 of Law No. 2014-038 on Personal Data Protection[151] requires entities undertaking personal data processing as the core of their activities to take reasonable measures to ensure data protection and confidentiality. However, it does not specifically provide for encryption use. The law No. 2005-023 of 17 October 2005 on Telecommunication Sector Institutional Reform, in article 7, requires all service operators to have encryption devices to ensure the confidentiality of messages and communication data. The same law, in article 41, punishes unauthorised interception, decryption, disclosure or publication of private communications with a fine between two million and 100 million Ariary (USD 503-25,162).

147 *Law No. 2016-017, https://www.dcn-pac.mg/uploads/loi/01e1e719a953c3d80a192026fe4cd6cf.pdf*

148 *LOI No. 2016 - 029 Portant Code de la Communication Mediatisee, https://tinyurl.com/2s3c35a7*

149 *Code de Procédure Pénale, https://sherloc.unodc.org/cld/uploads/res/document/mdg/code-de-procedure-penale_html/Madagascar_Code_de_procedure_penale.pdf*

150 *Loi n°2014-006 sur la lutte contre la cybercriminalité, https://www.afapdp.org/wp-content/uploads/2015/01/Loi-n%C2%B02014-006_fr.pdf*

151 *Personal Data Protection Law No. 2014-038 of 2014, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/99469/118746/F384159671/MDG-99469.pdf*

Under Article 40 of the cybersecurity law, a person who commits a digital infraction and/or refuses to reveal the encryption key to authorities in their investigation can be punished with imprisonment for between one and five years or a fine of between two million Ariary (USD 503) and 100 million Ariary (USD 25,162).

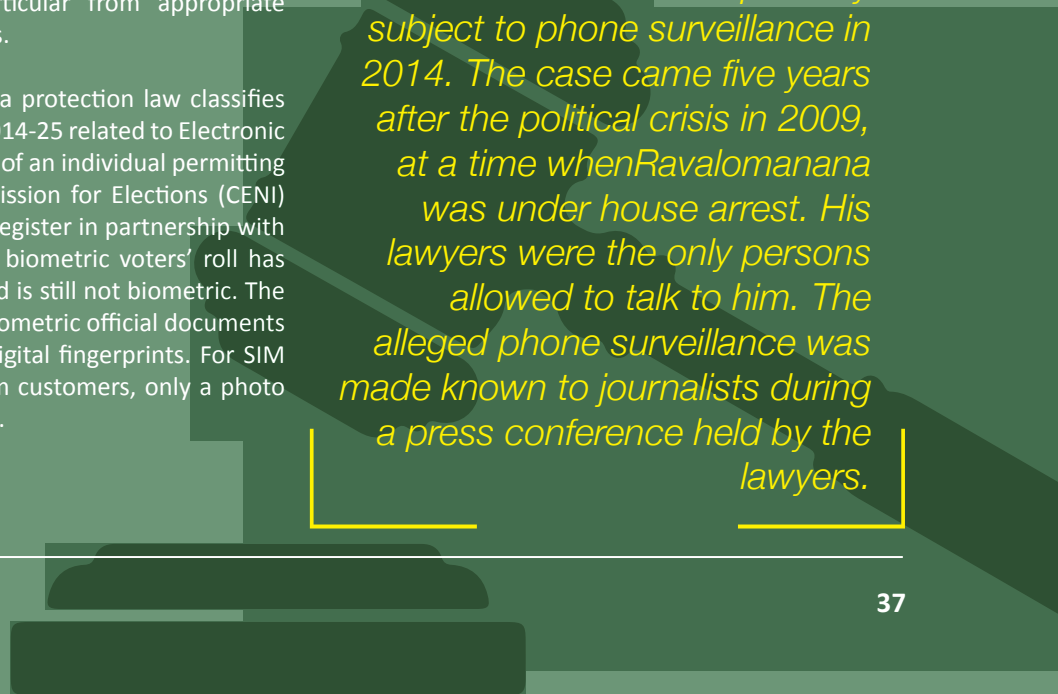
The use of VPNs in Madagascar is legal.[152] In its terms of service, Telma Madagascar, one of the main national telecommunication operators, indicates that the use of VPNs on its network is allowed for professional accounts, but in case of other uses, Telma reserves the right to suspend or cancel the contract without prior notice.

Article 20 of the data protection law provides for cross-border transfer of personal data to a foreign state only if the recipient state has legislation ensuring a level protection of persons similar to that provided by this law. The level of protection offered by a third country is assessed in light of all circumstances relating to a transfer or category of data transfers, including the nature of the data, the purpose and the duration of the transfer or the planned processing, the countries of origin and final destination, and the legal rules, general or sectoral, in force in the third country in question, as well as the professional rules and security measures observed therein. In the absence of a similar level of protection, the Malagasy Commission of IT and Civil Liberties may authorise the transfer of personal data if the controller offers sufficient guarantees with regard to the protection of privacy and fundamental rights and freedoms of individuals. Those guarantees may result in particular from appropriate contractual clauses or from adoption of internal rules.

Without specifying types of biometric data, the data protection law classifies biometric data as sensitive data. However, Law No. 2014-25 related to Electronic Signatures describes biometric data as "physical data of an individual permitting his/her identification". In 2019, the National Commission for Elections (CENI) explored the establishment of a biometric electoral register in partnership with the German firm VERIDOS.[153] To-date, however, no biometric voters' roll has been established. Similarly, the National Identity Card is still not biometric. The Malagasy passport and driving license are the only biometric official documents currently offered in the country and both contain digital fingerprints. For SIM card registration, no biometric data is collected from customers, only a photo and data from the national identity card are required.

**Case study: Complaints against unlawful surveillance**

*In 2015, a complaint of unlawful access to a computer system and phone surveillance was lodged against two former employees of CONNECTIC, a telecommunications equipment and computer consumables supplier.[154] However, the case was dismissed in September 2016 on grounds of insufficient evidence against the accused. In another case of alleged phone surveillance, three lawyers of former President Marc Ravalomanana[155] were reportedly subject to phone surveillance in 2014. The case came five years after the political crisis in 2009, at a time whenRavalomanana was under house arrest. His lawyers were the only persons allowed to talk to him. The alleged phone surveillance was made known to journalists during a press conference held by the lawyers.*



152 *See: Where are VPNs legal and where are they banned? https://www.comparitech.com/vpn/where-are-vpns-legal-banned/#M; and VPN: is it legal? not legal? We answer you https://www.aeres-evaluation.fr/legalite-vpn-pays/*

153 *https://www.ceni-madagascar.mg/projet-de-liste-electorale-biometrique-la-ceni-a-consulte-veridos/*

154 *Computer intrusion in Madagascar: the complainant finds himself in prison for 5 months and the Advocate General defends the defendants, https://intrusion.ovh/*

155 *Marc Ravalomanana : Ses avocats sur écoute!, http://www.midi-madagasikara.mg/a-la-une/2014/11/24/marc-ravalomanana-ses-avocats-sur-ecoute/*

## 2.16 Mauritius

The right to privacy is governed by sections 3 and 9 of the constitution. The Data Protection Act, 2017[156] provides the legal framework for the protection of privacy and personal data in the country. Section 18(1)(m) of the ICT Act 2001[157] mandates the ICT Authority (ICTA) to "take steps to regulate or curtail harmful and illegal content on the internet and other information and communication services." In 2011, the ICTA put in place an Online Content Filtering (OCF) mechanism for access to Child Sexual Abuse (CSA) websites. In November 2021, there were 17,879 attempts at CSA sites and 582 Mauritian IP addresses were blocked.[158]

Section 32(5)(a) of the Act stipulates that a public operator (e.g., an Internet Service Provider) or any of its employees or agents can intercept, withhold, or deal with a message which is believed to be abusive or indecent, in contravention of the Act or of a nature that can compromise the state's defence or public safety. The public operator is required to refer to the regulator for any appropriate written directions for any message withheld. Moreover, section 35(6)(a) of the Act permits a Judge, where satisfied by application by the Police or the Independent Commission Against Corruption relating to a criminal proceeding, to issue an order authorising a public operator, or any of its employees or agents, to intercept or withhold a message, or disclose it to the police or the Commission. Such orders remain valid for a maximum of 60 days and should specify the exact location of the interception or withholding of the message.

In addition, section 15 of the Computer Misuse and Cybercrime Act 2003,[159] permits an investigatory authority, for purposes of investigation or prosecution of an offence, and after having sought an order from a judge, to collect or record traffic data, in real-time, associated with specified communications transmitted by means of any computer system or to compel a service provider, within its technical capabilities, to perform such lawful surveillance. Also, section 25A of the Prevention of Terrorism Act 2002[160] permits the Commissioner of Police, where there is reasonable belief that an offence has been, is being or is likely to be committed, to make an application to a judge for the grant of an order, allowing the police to "use such electronic and technical device as may be required for the purpose of intelligence gathering or surveillance".

Under section 46 (1)(o) of the ICT Act 2001, a person who intercepts, authorises or permits another person to intercept a message passing over a network without authorisation by a Judge commits an offence punishable with a fine of up to 1,000,000 rupees (USD 24,000) and imprisonment for a term of up to 10 years. Section 28 of the Data Protection Act 2017, requires data controllers to obtain consent prior to any monitoring activities. Any person contravening the provision can be punished on conviction with a fine of up to 100,000 rupees (USD 2,400) and imprisonment of up to five years.

The Government of Mauritius implements the Safe City project[161] which is a nationwide CCTV system (4,000 cameras at 2,000 sites) for the purpose of safeguarding national security as well as public security. While there is no specific provision in the legislation for its regulation, the Data Protection Office issued a "code of practice"[162] for the operations of the project.

Section 18(v) of ICT Act 2001, empowers the ICTA to control the importation of any equipment capable of being used to intercept a message. The law does not specifically mention encryption, or restrict the use, development or importation of encryption software and products under the Clearance to Import ICT Equipment Regulations 2019. Nonetheless, section 12(c) of the Computer Misuse and Cybercrime Act 2003 allows an investigatory authority, for example the police, in the course of criminal investigation or prosecution, to apply to a judge for an order for the disclosure of an electronic key enabling access to or the interpretation of data.

156 *Data Protection Act 2017, https://www.icta.mu/documents/2021/08/dpa_2017.pdf*
157 *ICT Act 2001, https://www.icta.mu/docs/laws/ict_act.pdf*
158 *Child Sexual Abuse Filtering Statistics, https://www.icta.mu/observatory-csa/*
159 *Computer Misuse and Cybercrime Act 2003, https://www.icta.mu/documents/2021/08/cyber.pdf*
160 *Prevention of Terrorism Act 2002, https://www.bom.mu/sites/default/files/prevention-terrorism-act-2002.pdf*
161 *Safe City system: Data can be stored for at least 30 days on a 24-hour basis, indicates PM, https://tinyurl.com/2p9ca76n*
162 *The Code of Practice for the basic conditions for the use of Safe City system, https://tinyurl.com/37bj96s7*

The Electronic Transactions Act 2000, provides a definition of "secure electronic records" to include a prescribed security procedure or commercially reasonable security procedure agreed to by the parties involved. It defines a "secure Electronic Signature" to mean where application of a prescribed security procedure or a commercially reasonable security procedure is agreed to by the parties involved. It also defines the obligations of Certificate Authorities, namely to use a "trustworthy system" to perform their services. There is no mention of the type of system or any underlying restriction on the importation of such systems.

In addition, section 31(1) of the Data Protection Act 2017, requires data controllers to implement "appropriate security and organisational measures" to protect personal data against accidental loss, alteration, unauthorised disclosure or access, especially when processing involves the sending of data over an information and communication network. Section 31(2) includes the pseudonymisation and encryption of personal data and the ability of security measures to ensure the ongoing confidentiality and integrity of processing systems and services.

Section 36 of the Data Protection Act prohibits the transfer of personal data outside Mauritius unless the Data Protection Commissioner has given consent to such transfer. A transfer outside Mauritius can only take place if the third country ensures an adequate level of data protection. Under section 36(4), the Data Protection Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as the Commissioner may determine.

The transfer of personal data to a third country not ensuring an adequate level of data protection may take place, for example, on the condition that the data subject has given his or her consent unambiguously to the proposed transfer, or the transfer is necessary for the performance of a contract between the data subject and the data controller, or for taking steps at the request of the data subject with a view to their entering into a contract with the data controller. The transfer of personal data to a third country may also be allowed on such terms as the Commissioner may approve for the protection of the rights of the individuals. Offences are covered by Section 42 of the Data Protection Act 2017, which deals with the unlawful disclosure of personal data.

Mauritius has a long history[163] of involvement in data protection issues and is only the second non-European state, after Uruguay, to ratify the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108.[164] While the Data Protection Office keeps track of all decisions on complaints[165] made, no cases related to data localisation were registered.

The Data Protection Act 2004 was repealed and replaced by the Data Protection Act 2017 in order to strengthen the control and personal autonomy of data subjects over their personal data, and to comply with international data protection norms, namely Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR). The 2017 Act aims to simplify the regulatory environment for business in the digital economy, and to promote the safe trans-border flow of personal data to and from foreign jurisdictions. The DPA 2017 has introduced new features like Encryption ("the process of transforming data into coded form") and Pseudonymisation ("the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information and the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual").

163 *Mona Farid Badran, "Economic impact of data localization in five selected African countries", Digital Policy, Regulation and Governance, Vol. 20, June 2018, https://bit.ly/3D5wujN*

164 *Chart of signatures and ratifications of Treaty 108, https://bit.ly/3wAmDQs*

165 *Mauritius DPO, Decisions on complaints, https://bit.ly/3koVpHy*

**Case study: Court challenge to Mauritian National ID processes**

*The Mauritian government introduced a new smart identity card in October 2013, which incorporates citizen's fingerprints and other biometric information (photo) relating to their external characteristics. The National Identity Card (Miscellaneous Provisions) Act 2013 is the legislative vehicle for this scheme, as per section 12 of which the collection and processing of data is subject to the Data Protection Act.*

*In the case of Madhewoo v The State of Mauritius & Another 2015 SCJ 177, the litigants argued that the ID exercise contravened various human rights, including the right to privacy.*

*The Supreme Court acknowledged that the laws in question amounted to an interference with the constitutional right to privacy of Mauritian citizens. Nonetheless the court considered this to be a proportionate interference in the public interest of protection against identity fraud.*[166] *On the other hand, the indefinite retention and storage of data under the DPA 2004 was considered to be not justifiable and not proportionate to the aim of protection against identity fraud pursued in a democratic society. In an appeal, the Judicial Committee of the Privy Council concurred with the judgement of the Supreme Court.*

*Additionally, the UN Human Rights Committee found that Mauritius' 2013 National Identity Card Act violated its citizens' privacy rights, as there were no sufficient guarantees that the fingerprints and other biometric data stored on the identity card would be securely protected.*[167]

Processing data without the data subject's consent is punishable by a fine not exceeding Mauritian Rupees (Rs) 100,000 (USD 7,350) and imprisonment for a term not exceeding five years. After data is processed, every controller is mandated to destroy the data as soon as is reasonably practicable (section 27).

166 *Madhewoo v State of Mauritius 2016 (Judicial Committee of the Privy Council), https://www.jcpc.uk/cases/docs/jcpc-2016-0006-judgment.pdf*

167 *Views adopted by the Committee under the Optional Protocol, concerning communication No. 3163/2018, https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/MUS/CCPR_C_131_D_3163_2018_32840_E.pdf*

**Case Study: Mauritius Regulator's Bid to Undermine Encryption**

*Facing issues with fake news and fake profiles on social media platforms in Mauritius, the ICT Authority (ICTA) initiated a public consultation process in April 2021 on the introduction of a lawful interception mechanism to decrypt and re-encrypt social media traffic.[168] In the proposal, ICTA sought to set up a National Digital Ethics Committee (NDEC) with an enforcement unit empowered to take down and censor social media posts. The ICTA proposed setting up a proxy to segregate from all incoming and outgoing internet traffic in Mauritius, social media traffic, which would then need to be decrypted, re-encrypted and archived for inspection purposes as and when required. These proposals faced national and international backlash and were dropped.*

168 *How African Governments Undermine the Use of Encryption, https://cipesa.org/?wpfb_dl=477*

# 2.17 Morocco



Under article 108 of the Law No 22-01 of October 2002[169] relating to criminal procedure, as amended by the antiterrorism law in 2015, the Investigative Judge and the Crown Prosecutor are permitted under certain conditions to initiate surveillance operations including intercepting, recording, copying and seizing phone calls and any other telecommunications. The surveillance order should be in writing and may be initiated for the investigation of crimes such as: undermining state security; terrorism; criminal association; homicide; poisoning; kidnapping; hostage-taking; counterfeiting of currency; drugs and weapons trafficking; and crimes that undermine public health.

The Crown Prosecutor can request in writing the District's First President of the Appeals Court to issue a warrant allowing a surveillance operation. Additionally, the Crown Prosecutor may also conduct surveillance without a written warrant in cases of "extreme emergency" or when there is fear of potential destruction of evidence. In such cases, the Crown Prosecutor must immediately inform the District's First President of the Appeals Court who must issue a final decision either supporting, amending or cancelling the procedure within 24 hours. The warrants must include all elements necessary to identify the specific communications to be monitored, the exact motive behind the operation and the duration which must not exceed four months and is renewable once.

The judicial authority or judicial Police officers may request any agent under the authority of the Ministry of Communications, or service or network providers to place a surveillance device on any public network or telecommunications. The judicial officers are required to keep a written record of the surveillance operation, including its start and finish date. Also, the recordings must be kept under seal, and only destroyed after the lapse of the statute of limitation date related to the legal action, or when the case has been subject to a final judgement and is no longer subject to an appeal.

Under article 115, the unauthorised interception, destruction, publication or use of private communications, or the unlawful installation of listening devices is punishable by imprisonment for between one month and one year, a fine of 10,000 to 100,000 Moroccan Dirhams (DH) (USD 1,117-11,177) or both. When the crime is related to a terrorism act, the imprisonment is enhanced to between five and 10 years. In addition, under article 116, a similar penalty may be imposed on any public authority agent, employee of a public telecommunications network, or a provider of telecommunications services who, in the exercise of their duties, discloses the existence of a surveillance operation or order.

Article 13 of Law No 53-05 of 2007 on the electronic exchange of legal data restricts the import, export, supply, operation or use of means of cryptographic services.[170] According to the law, the purpose of this restriction is to prevent the use of encryption for illegal purposes, and to protect the interests of national defence and the internal or external security of the State. The law requires a prior declaration when the sole purpose of the encryption means or service is to authenticate or ensure the completeness of a transmission, and a prior authorisation in any other case. In addition, Decree No. 2-13-881 of January 2015 shifted responsibility for authorising and monitoring "electronic certifications" including encryption, from the National Telecommunications Regulatory Agency (ANRT) to the military's General Directorate for the Security of Information Systems (DGSSI).[171] Under article 32 of Law 53-05 of 2007, the import, export, supply, operation or use of means or cryptographic services without the required declaration or authorisation carries a penalty of imprisonment for one year, and a fine of between 10,000 to 100,000 DH (USD 1,117-11,177). The court may also order the confiscation of the cryptographic means involved.

169 *Law No 22-01 of October 2002, https://tinyurl.com/5chf4uek*

170 *Law No 53-05 of 2007 on the electronic exchange of legal data, https://www.dgssi.gov.ma/fr/content/loi-53-05-relative-l-echange-electronique-de-donnees-juridiques.html*

171 *Decree No. 2-13-881 of January 2015, https://adala.justice.gov.ma/production/html/Fr/188896.htm*

Articles 43 and 44 of the law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data, 2009,[172] restricts cross-border transfer of personal data and only permits it when certain conditions are met. According to article 43, the foreign state to which the data is being transferred needs to ensure a sufficient level of protection of privacy and of the fundamental rights and freedoms of individuals with regard to data processing. The adequacy of the level of protection provided by a state is assessed in particular on the basis of the provisions in force in that state, the security measures applied there, the specific characteristics of the processing such as its purposes and duration, as well as the nature, origin and destination of data processed.

***The National Commission for the Protection of Personal Data (CNDP) establishes the list of countries that offer a sufficient level of protection and complies with the requirements of Moroccan legislation relating to processing of personal data. In its Decision No. 236-2015 of 2015, the CNDP listed 32 countries considered to satisfy these requirements. No African country was included on the list.[173]***

Article 44 of the law defines exceptions allowing cross-border transfer of personal data including the data subject's consent, the necessity of the transfer in the interest of the data subject, public interest and the existence of a bilateral or multilateral agreement to which Morocco is a party. The CNDP can issue reasoned authorisation if the processing guarantees a sufficient level of protection of the privacy and fundamental rights and freedoms of individuals, in particular by reason of the contractual clauses or internal company rules to which it is the subject. Under article 60 of the 2009 data protection law, unauthorised cross-border transfer of personal data is sanctioned with three months to one year of imprisonment or a fine of 20,000 to 200,000 DH (USD 5,445-54,451) or both.

Since 2016, according to decree No. 2-15-712 on protecting sensitive information systems of vital infrastructures,[174] companies and organisations operating in sectors of vital importance and using data deemed sensitive must host their infrastructure and digital databases on Moroccan territory. The concerned entities are defined as those that undertake activities related to the production or distribution of "goods and services essential to the satisfaction of the basic needs for the life of the populations or to the maintenance of the security capacities of the country". Meanwhile, the National Telecommunications Regulatory Agency requires[175] service providers commercialising the ".ma" domain name to set up and maintain a secure DNS service platform made up of at least two DNS servers, with at least one server hosted in Morocco.

Meanwhile, in its Decision No. 478-2013 of November 2013[176] on the conditions for using biometric devices for access control, theCNDP recognises biometric data as personal data and therefore considers it subject to the provisions of Law No. 09-08 on processing of personal data. The CNDP decision requires obtaining the commission's authorisation before installing a biometric device. The controller can only keep the biometric data in its raw state for the time necessary for carrying out the operation of extracting the character-defining elements.

In August 2019, the CNDP issued a seven-month ban,[177] extended in March 2020 until December 2020, on authorisations for the use of facial recognition technology to allow for consultations on balancing security, economic efficiency and service delivery against privacy and data protection. Following the outbreak of COVID-19, in April[178] and July[179] 2020, while still expressing its reservations, the commission issued two decisions allowing the implementation of facial recognition systems by banks and payment institutions and social security institutions after obtaining authorisation from the commission. In 2014, the National Telecommunications Regulatory Agency (ANRT) issued a decision requiring all mobile service subscribers to be registered.[180] Registration requires the customer's full name and national identity number.

172 *Morocco, law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data, 2009, https://bit.ly/3F6HGxi*

173 *CNDP Morocco,Deliberation No. 236-2015 of 2015, https://www.cndp.ma/images/deliberations/deliberation-n-236-2015-18-12-2015.pdf*

174 *Morocco, Decree No. 2-15-712 on protecting sensitive information systems of vital infrastructures, https://bit.ly/3C58PyF*

175 *ANRT Morocco, Service provider agreement n ° ../ma/20../ANRT relating to the marketing of ".ma" domain names, https://bit.ly/3c24At4*

176 *Decision No. 478-2013 of November 2013, https://www.cndp.ma/images/deliberations/deliberation-n-478-2013-01-11-2013.pdf*

177 *Decision N° D-194-2019, https://www.cndp.ma/fr/avis-et-decisions/m-deliberations/78-decisions/591-deliberation-d-194-2019.html*

178 *Decision N° D-108-EUS-2020, https://www.cndp.ma/fr/avis-et-decisions/m-deliberations/78-decisions/671-deliberation-d-108-eus-2020.html*

179 *Decision N° D-126-EUS-2020, https://www.cndp.ma/fr/avis-et-decisions/m-deliberations/78-decisions/686-deliberation-d-126-eus-2020.html*

180 *Identification des abonnés mobiles: Les nouvelles mesures, https://www.anrt.ma/sites/default/files/CP-identification-abonnes-Fr.pdf*

The law No. 35-06,[181] as promulgated by a Royal Decree No. 1-07-149 of Nov. 30, 2007, instituted the electronic national identity card (CNIE) containing personal details and biometric data including facial image and fingerprints. The card includes a barcode and microchip including encrypted and encoded personal information. The law allows the cardholder to access the data stored in the card's microchip and barcode. The implementation of the CNIE system is the responsibility of the National Directorate of National Security (DGSN). Every Moroccan citizen over the age of 18 is required to be issued the CNIE. Under article 9, any person who fails to have his personal CNIE issued is sanctioned with a 300 DH (USD 33) fine.

Meanwhile, according to Decree No. 2-08-310 of 23 October 2008[182] establishing the biometric passport (e-passport), the passport is available for all new Moroccan applicants regardless of age. Each e-Passport contains a concealed microchip and barcodes storing personal details, a digitised passport photo, and two fingerprints. Additionally, Law No 36-11 of 2011[183] provides for a computerised electoral register. Applicants need to provide their first and last names, date and place of birth, occupation, address,national biometric ID card numbers, signatures, or fingerprints. The CNIE alone is required for voting.

**Case study: State sanctioned surveillance**

*Morocco has been identified as one of the states that have acquired surveillance tools.[184] In 2019 and 2020, Amnesty International published reports detailing the targeting of Moroccan human rights defenders and journalists whose devices were breached by Pegasus, a spyware software developed by the NSO Group, an Israeli technology firm. Pegasus is known to be used by governments to spy on journalists, human rights defenders, and the opposition. Earlier in 2015, a report by The Citizen Lab[185] published evidence that the Moroccan government had used FinFisher malware produced by the British-German Gamma group of companies against "Mamfakinch",[186] a group of Moroccan citizen journalists. Also in 2015, Morocco was included among the list, published by the Swiss government, of countries that had purchased surveillance technologies from Swiss companies.*

181 *Law No. 35-06, http://www.egov.ma/sites/default/files/loi_ndeg35-06_carte_nationale_didentite_electronique.pdf*

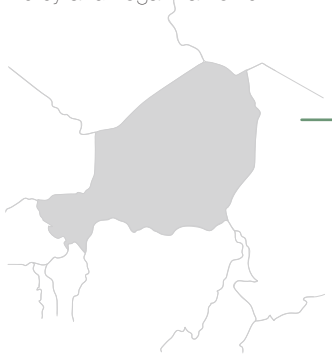
182 *Decree No. 2-08-310 of 23 October 2008, https://www.passeport.ma/PDF/passeport12/fran%C3%A7ais/Passeport_d%C3%A9cret.pdf*

183 *Law No 36-11 of 2011, https://www.chambredesrepresentants.ma/sites/default/files/36.11.pdf*

184 *State of Privacy Morocco, https://privacyinternational.org/state-privacy/1007/state-privacy-morocco*

185 *Pay No Attention to the Server Behind the Proxy Mapping FinFisher's Continuing Proliferation, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/*

186 *Their eyes on me: stories of surveillance in Morocco, https://privacyinternational.org/sites/default/files/2018-02/Their%20Eyes%20on%20Me%20-%20English_0.pdf*



# 2.18 Niger

Article 1 of the Law on the Interception of Communications of May 2020[187] provides that only a "public authority" can intercept correspondences and communications where it is necessary, in the public interest and provided for by law. Under article 2, communication interception can occur in investigations related to attacks on national security or unity, attacks on national defence and territorial integrity, prevention and combating of terrorism and transnational organised crime, and prevention of all forms of foreign interference and collusion with the enemy.

Interception operations are authorised by the president based on proposals from the Prime Minister, or the Minister in charge of defence, Interior, Justice, or Customs. Article 11 provides that interception records may be destroyed on the president's order and after investigation reports on the operation of the interception are written. The interception orders are valid for one month. Under article 12, the Prime Minister authorises and supervises the destruction of interception records as soon as their preservation is no longer necessary to preserve national security.

Under Article 15, the National Commission for the Control of Security Interceptions (CNCIS) is mandated to provide oversight of interceptions. The CNCIS is an independent administrative authority led by a magistrate from the Court of Cassation as per Article 16 who is a presidential appointee. The Commission executes the interception decisions of the president or any person delegated by him/her, controls any interception operation to ensure their legality, and can make a recommendation to the Prime Minister to stop an interception operation deemed illegal (Article 22). Apparently, the commission is not functioning yet. Under 24, 32 and 33, public officials, network operators and service providers are obliged to cooperate with interception operations.

The Law on the Suppression of Cybercrime[188] provides under article 45, that in certain criminal matters, the examining magistrate at the request of a judicial police officer can prescribe the collection, interception, recording and transcription of data relating to the content of specific communications within their jurisdiction, transmitted by means of a computer system. The interception order is valid for three month, is renewable and not subject to any appeal as per article 45(2-4). The investigating judge or the judicial police officer appointed may request any qualified person to install interception devices.

In addition, the eTransactions Law[189] obliges intermediaries to carry out surveillance activities on the content stored on their platforms, or possibly block access to some content through judiciary or police order. In addition, the Law of May 26, 2015 on the smuggling of migrants[190] under article 8, prescribes the surveillance of bank accounts, tapping of fixed or mobile telephone lines and the surveillance of any activities placed on systems or the internet for exchanging computer data, in relation to persons suspected of committing or to have committed an offence under the law.

Articles 19 and 27 of Law of October 31, 2016 on the Fight Against Money Laundering and the Financing of Terrorism[191] requires financial institutions to collect and store information relating to customers for a period of 10 years. The collected data for a natural person includes name, date and place of birth, address, and an original official document including a photograph. Under article 36, the information may be shared with judicial authorities or state agents upon presentation of a warrant, or to supervisory authorities such as CENTIF (the National Financial Information Processing Unit).

187 *May 2020; Law on the interception of certain communications sent by electronic means in Niger.*
188 *Law No. 2019-330 of 03 July 2019 on the repression of cybercrime in Niger.*
189 *Law No. 2019-03 of April 30, 2019, on electronic transactions in Niger, https://bit.ly/3kCL2R3*
190 *Law No. 2015-36 of May 26, 2015 on the Smuggling of Migrants in Niger.*
191 *Law No. 2016-33 of October 31, 2016, on the Fight Against Money Laundering and the Financing of Terrorism in Niger*

The failure to cooperate in facilitating interception is punishable under the Law on the Interception of Communications with imprisonment for a period of between one and five years and a fine ranging from two to 10 million CFA francs (USD 3,445-17,222). Under the Law on the Suppression of Cybercrime, illegal interception, digital identity theft, reproduction, extraction, copying of computer data, as well as breach of trust in computer data are punished with imprisonment of between one to five years and fines ranging from one to 20 million CFA francs (USD 1,768-35,370).[192]

> ***In 2020, Niger's Minister of Justice Marou Amadou admitted that the opposition was under surveillance by the intelligence services. The admission came during a parliamentary debate on the Interceptions of Communications bill. Under questioning by an opposition member who expressed his fears that the government would monitor the population under the pretext of counterterrorism, the minister stated: "Are you afraid of being tapped? You have been and still are. It is just going to be organised now."[193]***

Under article 52 of the Law No. 2017-28 on the protection of personal data,[194] cryptology service providers are required to decrypt data when requested by the High Authority for the Protection of Personal Data (HAPDP). Under article 24, a cross-border transfer is subject to the data protection authority's authorisation. Personal data transfer to a third country may only be authorised if the state ensures a higher or equivalent level of privacy protection as well as freedoms and fundamental rights of persons. Prior to any transfer of personal data to a third country, the data controller must be authorised by the HAPDP.

Under article 64 of the Cybercrime Law,[195] unspecified "competent authorities" can access data stored across borders that is open to the public regardless of the geographical location of such data and without the authorisation of the state where the data is located. Further, the article grants authorities powers to access data located in another country, through a computer system located in Niger, with legal and voluntary consent.

The Law No. 2019-29 on the Civil Status Regime in Niger establishes a national population register based on civil status data to contain biographical data, and biometric data that is not specified.[196] Meanwhile, the Nigerien Electoral Code of July 2019[197] under article 36, establishes a biometric electoral database that is developed, managed, and updated by the National Electoral Commission (CENI).[198] The system issues biometric electoral cards valid for 10 years. Under article 38, the biometric registration of voters is voluntary for Nigerien citizens aged 18 years or older. The biometric enrolment, which was initiated in February 2020 by President Mahamadou Issoufou,[199] captures the voter's photo and fingerprints as well as information related to birth date, names, parentage, physical and electronic addresses, profession, gender and marital status (articles 39–40).

Similarly, Decree No. 2012-433 on the identification of mobile telecommunications services buyers and/or users[200] requires telecom operators to collect the identity data of all subscribers. For purposes of this identification, the physical presence of the subscriber is required with their biometric national identity card,[201] which is scanned into the SIM card registration system together with the electronic signature. Article 7 of the Niger Data Protection Law subjects the processing of biometric data to the prior authorisation of the HAPDP The controller or their legal representative submits the authorisation request, and authorisation does not exempt third parties from liability.

192 *Niger, Law No. 2019-330, Article 7 (Illegal interception) Article 14 (Identity theft), Article 21 (Reproduction, extraction, copying of computer data), Article 23 (Breach of trust in computer data).*
193 *Digital Business Africa, Niger, https://bit.ly/3l5Qdt8*
194 *Niger, Law No. 2017- 28 of 03 May 2017, on the protection of personal data, https://bit.ly/3HCq3r5*
195 *Law No. 2019-330 of 03 July 2019 on the repression of cybercrime in Niger.*
196 *Law No. 2019-29, Article 76; the nature of the biometric data contained here is not specified.*
197 *Organic Law No. 2017-64 of August 14, 2017 on the Electoral Code of Niger (Special OG No. 19 of September 14, 2017), amended and supplemented by Law No. 2019-38 of July 18, 2019 (Special OJ No. 13 of August 15, 2019), https://bit.ly/3CTumv8*
198 *Under article 9, the CENI is an Independent National Electoral Commission.*
199 *Niger launches biometric electoral cards, https://bit.ly/3oO1NeJ*
200 *Decree No. 2012-433/PRN/MC/NTI/MISP/D/AR/MJ, identifying the buyers and/or users of mobile telecommunications services offered to the public in Niger.*
201 *The Biometric National Identity Card which encloses photo and fingerprints of the holder is established by the Decree n ° 2003-257 / PRN / MI / D of October 17, 2003.*

## 2.19 São Tome & Principe

Article 31 of Law No. 15 on cybercrime stipulates that the judicial body that has ordered or authorised the monitoring of telecommunications shall be the first to know its contents and may order its transmission to the Force or Service in charge of the investigations, if the data obtained may be considered useful for the investigation of criminal proceedings.[202] According to this law, the request for an interception can be done by the police and is authorised by a judge. Under article 18, the surveillance period is limited to 30 days. However, the judicial police may carry out a search, without prior authorisation from the judicial authority, when the search is voluntarily consented to by whoever has the availability or control of such data, provided that the consent given is documented in any way.

The cybercrime law defines interception as the act of capturing information contained in a computer system by means of electromagnetic, acoustic, mechanical or other devices. Further, information obtained from interception is according to article 21, admissible in proceedings concerning crimes committed by means of a computer system or for which it is necessary to collect evidence on an electronic medium, when such crimes are provided for in article 258 of the Penal Code. Moreover, the interception and recording of computer data may only be authorised during an enquiry, to find out the truth or that evidence would otherwise be impossible or very difficult to obtain.

Interception orders must specify the scope of the interception which shall be based on the needs of the investigation. Under article 29, Judicial Police may make interception requests, which are then presented to the Public Prosecutor's Office for onward submission to the criminal investigation judge for authorisation. Article 19 of cybercrime law states that the judicial police may carry out seizures, without prior authorisation from the judicial authority, during a computer search when there is urgency or danger in delay. Article 26 provides that expedited requests may be refused if the computer data concerned relates to a political offence or an associated offence under the law; or undermines the sovereignty, security, public order, or other constitutionally defined interests of the Republic. Article 8 of the cybercrime law prohibits ''illegal interception'' and publishes the offence with imprisonment for a period of up to three years or an unspecified fine.

Law No. 07/2017[203] provides for the creation of the National Agency for Personal Data Protection (NAPPD),[204] which is statutorily empowered to authorise the interconnection of automated processing of personal data and the transfer of personal data, as well as generally ensure compliance with the data protection law.

Under article 19 of the law on data protection enacted in 2016,[205] the transfer of personal data to a location outside the national territory may only take place in compliance with the law and if the legal system in the country to which the data is transferred ensures an adequate level of protection. In addition, it shall be for the NAPPD to determine whether a legal system ensures an adequate level of protection as per article 19(2). The transfer of personal data to a country that does not ensure an adequate level of protection is governed by article 20. The article provides that such transfers can only be done upon notification of the NAPPD that the data subject has authorised the transfer or where the transfer is necessary for, among others, the execution of a contract or is in the interest of the public. Further, under article 20(2), the NAPPD may authorise a transfer or a set of transfers of personal data to a legal system that does not ensure an adequate level of protection, provided that the controller ensures sufficient guarantee mechanisms for protection of privacy and rights and freedoms fundamental rights of people, as well as their exercise, through suitable contractual clauses.

**203** *Law No. 15 of 2017 on Cybercrime, http://cipstp.st/wp-content/uploads/2018/03/Lei_15_2017-Lei-sobre-Cibercrime.pdf*

**204** *Law No. 07/2017, https://www.anpdp.st/docs_comprimidos/legislacao_nacional/dr40_lei7_2017_organizacao_e_funcionamento.pdf*

**205** *National Agency for the Protection of Personal Data (NAPPD), https://www.anpdp.st*

**206** *Law No. 03/2016 of 10th May 2016, https://www.anpdp.st/docs_comprimidos/legislacao_nacional/dr39_lei3_2016_proteccao_de_dados_pessoais.pdf*

In 2012, Sao Tome & Principe adopted a Regulation on the Registration and Identification of SIM Cards – Decree No. 20 of 2012.[206] In article 4(a), it states that it aims to create a public integrated telecommunications electronic database containing all mobile phone data and numbers, as well as information associated with their respective holders, to serve as a source of information for operators and providers of public telecom services and for competent state authorities. Article 7 specifies the form which providers of public telecom services shall use in registering SIM cards. It must contain the name of the subscriber; identification document; identification number; date and place of issuance of the identification document; validity of the identification document; serial number of the subscriber's SIM card; telephone number of the subscriber; subscriber's home and/or work address; subscriber's signature or fingerprints.

Article 12 creates an Integrated Public Numbering Database (B-PIN) containing the data of all subscribers to public telecommunications services, whether individuals or corporate entities. Under article 2, the regulation provides that all subscribers shall register their SIM cards within three months of initial activation, after which they shall be blocked. Under article 13, operators that fail to comply with the provisions of the regulation or violate the confidentiality of information shall be subject to the sanctions provided for in the telecommunications legislation. In March 2017, the largest São Tomé and Principe opposition party, the MLSTP-PSD, claimed to have detected irregularities in the voter registration.[207] The process started in 2017 and is regulated by the electoral legislation. It collects personal data such as name, location and date of birth. However, the process is not linked to the personal IDs.[208]

## 2.20 Sierra Leone

Section 13(1)(b) of the Anti-Money Laundering and Combating of Financing of Terrorism Act[209] empowers the country's Financial Intelligence Unit to request and obtain any information that it considers relevant to an unlawful activity, money laundering, terrorism financing from sources such as commercially available databases, databases maintained by government ministries, departments and agencies, from reporting entities such as banks and financial institutions.

Section 21(1) of the National Security and Central Intelligence Act[210] permits the Director General of the Office of National Security (ONS) or his designated employee to apply for a warrant to a judge for the interception of communication. Such an application is required under section 22 of the Act to specify certain details such as the identity of the person whose communication is to be intercepted and the justification. Additionally, such warrants, when issued, are valid for up to 60 days. However, there are gaps in the oversight of, and transparency on surveillance activity to prevent possible abuse by law enforcement or state security agencies. For instance, some government agencies such as the Integrated Intelligence Unit within the police purportedly use a range of unsanctioned methods including surveillance for intelligence gathering.[211]

206 *https://www.arctel-cplp.org/app/uploads/membros/161632648825d4ae6943267a.pdf*

207 *MLSTP accuses the CNE of having prepared electoral fraud, https://www.rfi.fr/pt/sao-tome-e-principe/20170301-mlstp-acusa-cne-de-ter-preparado-fraude-eleitoral*

208 *Legislation, https://www.cen.st/index.php/legislacao*

209 *Anti-Money Laundering and Combating of Financing of Terrorism Act, https://tinyurl.com/mwfdbvpn*

210 *National Security and Central Intelligence Act, http://www.sierra-leone.org/Laws/2002-10.pdf*

211 *Interview with a police officer who wishes to remain anonymous,*

Regulation 19 of the Telecommunications Subscribers Identification and Registration Management Regulations 2020[212] mandates the National Telecommunications Commission (NATCOM) to maintain the central subscriber information database, in which all subscriber information obtained from service providers are stored. Further, regulation 19 provides for access to the data by "authorised" persons who include law enforcement agencies to safeguard national security. However, the regulation does not define the term "authorised person".

The Cybersecurity and Cybercrime Act 2021 prohibits, under clause 27, the intentional and unauthorised interception of non-public transmission of data. Clause 9 empowers a High Court Judge to order a service provider to collect or record real-time traffic data, on the application of a police officer or an authorised person, where there are reasonable grounds to believe such data is required for a criminal investigation. Such orders are valid for up to 90 days and may be extended, but the period is not specified by the law. Further, clause 28(1) permits a law enforcement officer where there are reasonable grounds to believe that an offence has been committed, is likely to be committed or is being committed and for the purpose of obtaining evidence of the commission of an offence under the Act, to apply, ex-parte, to a Judge, for an interception of communications order. The prior consent of the Attorney-General in writing is required before such an application is made.

An interception order may: require a service provider to intercept and retain a specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that service provider; authorise the law enforcement officer to enter specified premises with a warrant and install any device for the interception and retention of a specified communication or communications of a specified description and to remove and retain such device; require any person to furnish the law enforcement officer with such information, facilities and assistance as the Judge considers necessary for the purpose of the installation of the interception device; or impose the terms and conditions for the protection of the interests of the persons specified in the order or any third parties or to facilitate any investigation. The interception of communications orders are valid for three months and may, on application by a law enforcement officer, be renewed for such a period as may be determined by the Judge.

Clause 29(1) permits a law enforcement officer to intercept any communication and orally request a service provider to route duplicate signals of indirect communications specified in the request to the Central Monitoring and Coordination Centre under certain circumstances such as for investigation of specific criminal activities relating to bodily harm, death, damage to property or financial loss. An electronic communication service provider is required on receipt of such a request, to route the duplicate signals of the indirect communication to the Central Monitoring and Coordination Centre. In addition, such a law enforcement officer is required to immediately furnish the service provider with a written confirmation of the request setting out the information given in connection with the request. Section 27(1) states that unauthorised interception is punishable with a fine or a term of imprisonment as the Minister may prescribe in regulations. Section 78 of Telecommunications Act 2006 criminalises the unlawful interception and or disclosure to third parties of telecommunications data.

Sierra Leone does not have a specific law regulating encryption or the provision of encryption services, programs or products. Additionally, the 2019 Electronic Transaction Bill[213] is silent on the regulation or restriction of the use, importation and exportation of encryption programmes and products. Nonetheless, article 5(2)(f) of the Cybersecurity and Cybercrime Act 2021 empowers a judge to issue a warrant authorising a police officer or other authorised persons to "access to any information, code or technology which has the capability of unscrambling encrypted data contained or available to a computer system into an intelligible format for the purpose of the warrant.

212 *Telecommunications Subscribers Identification and Registration Management Regulations 2020, https://tinyurl.com/yckzbxwv*

213 *Electronic Transaction Bill, https://www.parliament.gov.sl/uploads/bill_files/The%20Electronic%20Transaction%20Bill%202019.pdf*

Data localisation requirements are found in Article 22(3) of Sierra Leone's Telecommunications Subscribers Identification and Registration Management Regulations 2020.[214] It states that subscribers' registration information shall not be transferred outside Sierra Leone without prior approval by the National Telecommunications Commission. Article 22(4) states that any request for approval to transfer or utilise customer registration information outside the country shall include justification of the purpose for which such data is required to be transferred. There are no reported breaches, or active enforcement, of this regulation.

The Cybersecurity and Cybercrime Act 2021[215] also has provisions relevant to data localisation. Whereas the Act does not prohibit cross-border data transfer, it provides in article 17(1) 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. Section 7(d) provides that a presidential order would designate rules for access to, transfer and control of data in Critical National Information Infrastructure.

Sierra Leone does not have stand-alone legislation on data protection although section 22 of the country's constitution of 1991 guarantees the right to privacy. Section 37 of the National Civil Registration Act 2016[216] mandates the National Civil Registration Authority (NCRA), the entity created to undertake compulsory and continuous registration of citizens and non-citizens and to establish and maintain an electronic registration system known as the Integrated National Civil Registration System, which shall be used to register individuals in the country and act as a source of personal data. The system is designed by law to collect and maintain biometric details of citizens and to generate a national identification number. Biometric details of individuals can include the face, fingerprint, blood group, eye colour, and height, according to section 38(c) of the Act. The NCRA is also now responsible for providing national identity cards, a role it has failed to execute as of November 2021. In November 2020, the Authority said arrangements to issue identity cards were underway.[217]

Sierra Leone developed a biometric voters' register for the 2018 elections through joint efforts by the NCRA and National Electoral Commission (NEC). However, Sierra Leoneans have not been provided with national identity cards since NCRA took over the responsibility in 2016 from the National Registration Secretariat that was previously responsible for ID card management. The 2018 exercise collected personal information of registrants including name, date of birth, place of birth, address, occupation, and a facial image of the registrant taken at the time of registration. Similar details of the registrant's parents were also requested.[218]

Meanwhile, section 3 of the Telecommunications Subscribers Identification and Registration Management Regulations 2020 requires licensed communications service providers to obtain, record and store information of subscribers. SIM-card registration became mandatory in December 2020, prior to which the regulator only encouraged operators to register their customers.

214 *The Telecommunications (Subscribers Identification and Registration) Regulations 2020, https://bit.ly/3C6M8Kv*

215 *Cybersecurity and Cybercrime Act 2021, https://tinyurl.com/yxfnsfed*

216 *National Civil Registration Act 2016, \\192.168.1.200\gpd\ACTS\Act 20 (sierra-leone.org)*

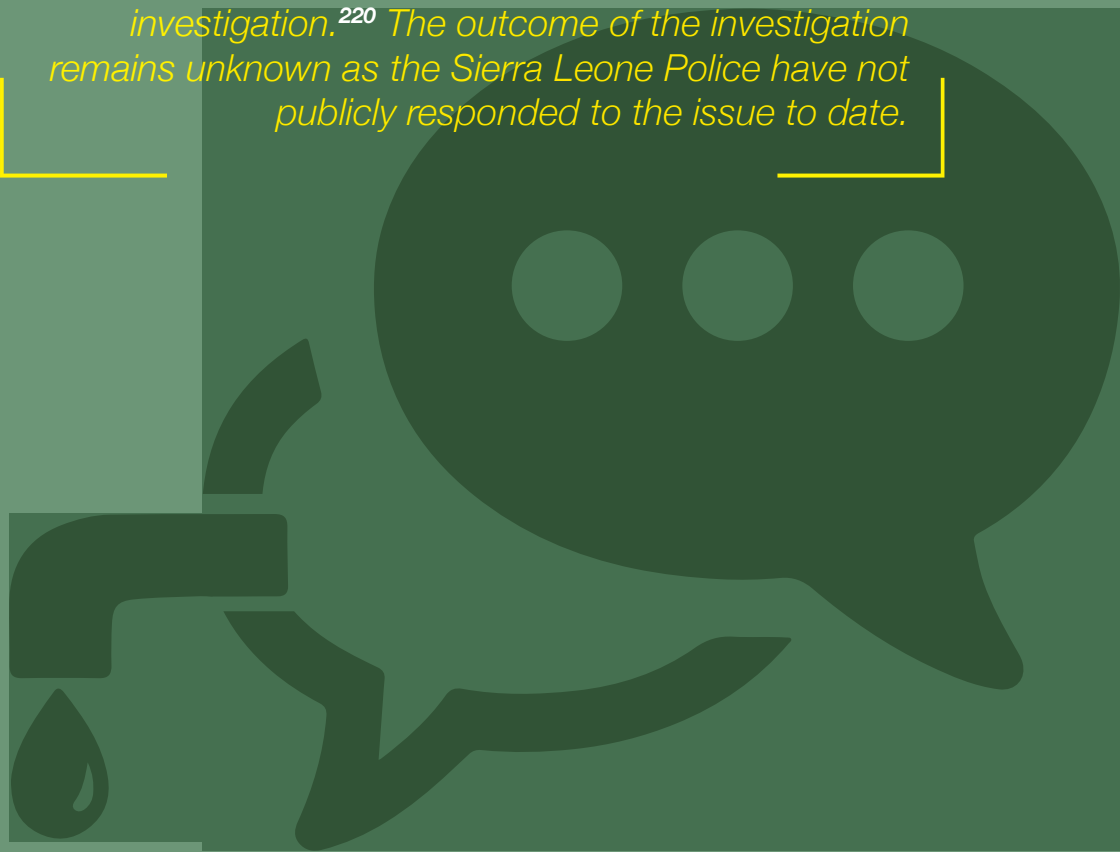
217 *Sierra Leone Assures of national photo ID cards starting December, https://politicosl.com/articles/sierra-leone-assures-national-photo-id-cards-starting-december*

218 *How is the National Electoral Register Created? - Sierra Leone, https://www.idea.int/answer/ans73587765284*

According to the 2020 Regulations, the required customer registration data includes a passport-sized photograph clearly depicting the facial image of the customer and/ or biometric information or a copy of a valid identification document. The regulations define biometric information to mean "fingerprints and facial image" of a subscriber. Other registration data required per specifications provided by the regulator includes the names, date of birth and gender of subscribers. Failure to register subscribers attracts fines specified in Section 34 of the 2020 Regulations. While the Regulations require service providers to keep subscribers' information securely and confidentially, law enforcement officers can access it under section 21(4).

**Case Study: Former President's conversation with police official leaked**

*In 2020, a leaked telephone conversation between[219] the Inspector General of Police and Sierra Leone's former president who was being investigated as part of a high-profile anti-corruption case led many to speculate that the conversation may have been intercepted. The Office of the Former President released a public statement expressing concern over the leak and called for a speedy and impartial investigation.[220] The outcome of the investigation remains unknown as the Sierra Leone Police have not publicly responded to the issue to date.*



219 *SLPP Govt Leaks Private Conversation between Ernest Koroma & Sierra Leone Police Boss, https://tinyurl.com/ysz3f2a3*

220 *Police IG accused of leaking audio recording of conversation with former President Koroma, https://tinyurl.com/3nu6daxr*

# 2.21 South Sudan



Section 13(11) of the National Security Act 2014 empowers the National Security Service to "monitor frequencies, wireless systems, publications, broadcasting stations and postal services in respect to security interests so as to prevent misuse by users." The law requires warrants to be sought under section 55 where there are reasonable grounds by the Director General or a designated employee through an application to a court. The application should contain the purpose of the warrant; the level of urgency for the warrant to be granted; the impracticability of carrying out the investigation in another way; the type of information, material, record or document proposed to be obtained; the identity of the person being investigated; and the general description of the place where the warrant is to be executed. The warrants are valid for one month with a possibility of extension. Also, a person on whom a warrant is issued has the right of appeal.

Section 8(d) of the Southern Sudan Police Service Act 2009 empowers the police to carry out surveillance subject to the provisions of the Code of Criminal Procedure Act 2008. Also, section 6(d) of the Cyber Crimes and Computer Misuse Provisional Order 2021[221] requires private or public entities that provide means of communication through computers and store computer data on behalf of their users, to maintain confidentiality of data saved and stored and not to disclose them without an order from a competent judicial authority.[222]

Section 98 of the National Communication Act 2012[223] prohibits any person from intercepting, interfering, jamming or hacking into any communication network, and punishes such persons with imprisonment, a fine or both, but these are not specified. Under section 12 of the Cyber Crimes and Computer Misuse Provisional Order 2021, the unauthorised transmission of data attracts a penalty of 10 years imprisonment, a fine or both. In addition, section 96(2) prohibits the eavesdropping, monitoring or hacking of communications unless authorised by an order of the Attorney General, Director of Persecutions or by a court of Competent Jurisdiction. Section 96(3) of the same law provides for compensation for a victim of a breach of confidentiality and eavesdropping. Also, under section 97 of the law licensees are required to remedy a breach of confidentiality and eavesdropping immediately and within 30 days of receiving a notice of contravention. Failure to comply attracts penalties such as the shortening, suspension or cancelation of licence or a financial penalty.

There is no specific law on regulating encryption in South Sudan. There have been no recorded instances of direct prohibition on the use of encryption but human rights defenders who are worried about state surveillance often rely on encrypted apps for their communications.[224] The National Security Service is reported to have carried out surveillance of perceived critics or threats to the government, including by tapping phones.[225] During the trial of senior government officials accused of treason, a recording of their phone conversations was played in court as prosecution evidence.

South Sudan also has no formal law on data protection and any law that has a provision on data protection makes no reference to the data being specifically stored within the borders of South Sudan. The law allows for disclosure of the data with consumer consent,[226] to an authorised body[227] or on the basis of a court order[228] and provides for penalties of 10 years imprisonment or a fine or both when there is a violation.[229] Notwithstanding the above, Section 63(6) of the Banking Act 2012 states that "no bank shall move all or any part of their admin, operations, books or records outside South Sudan without prior written consent of the [central] Bank." Section 84(2) provides that financial ledgers and other financial records shall be kept in South Sudan for a period not less than 10 years. Section 84(6) relates to non-financial records, which must also be kept within South Sudan.

221 *Cyber Crimes and Computer Misuse Provisional Order 2021, https://drive.google.com/file/d/1-t9CYZiuACctg90bsS1ROdXjtLPW9z08/view?usp=sharing*
222 *Cyber Crimes and Computer Misuse Provisional Order 2021 Section 7*
223 *National Communication Act 24/2012, https://ictpolicyafrica.org/en/document/bfc7dffmhixj*
224 *South Sudan: Rampant abusive surveillance by NSS instils climate of fear, https://tinyurl.com/yz8emacf*
225 *Amnesty international, These Walls have Ears: The Chilling Effect Of Surveillance In South Sudan, https://tinyurl.com/2p8nsw65*
226 *Credit Reporting Systems Regulation 2014 Section 24(2) , Electronic Money Regulation 2017 Section 21*
227 *Banking Act 2012 Section 63(6)*
228 *Cybercrimes and computer misuse provisional order 2021 Section 6(d) , Electronic Money Regulation 2017 Section 21*
229 *Ibid Section 12*

Although the country does not have a data protection law, the government collects a wide range of information including through registration for national identity cards, passports, certificates of good conduct, and the use of iris scanners at many entry points into the country.[230] Information collected for the national ID includes fingerprints, parents' names, place of birth, date of birth, and full names. Mandatory SIM card registration was introduced in 2012, with the requirements including one's national identity card or passport which has details like full names, date of birth, ID number and state.[231] The government claims mandatory SIM card registration assists in fighting crime but there is little evidence to support this. According to Amnesty International research, SIM card registration data has become an enabler of surveillance.[232]

Section 63 of the Criminal Procedure Code 2008 allows the police to take fingerprints, eye prints and or photograph of any accused person during their trial, or during interrogation or investigation, if it is essential. This data can be kept for up to six months then destroyed unless the accused is convicted.

Since August 2018, the International Organisation for Migration (IOM) and the World Food Programme have been collaborating on the project "Enhancing targeted food distribution through biometric data management" which seeks to contribute to increased food security throughout South Sudan, although IOM's biometric registration system has been active since 2014.[233]



## 2.22 Sudan

Article 74 of the 2018 Telecommunications and Postal Regulation[234] permits interception, surveillance and eavesdropping. These can be ordered by a prosecutor or a specialised judge. Interception may also be ordered by the General National Intelligence Service, Military Intelligence and the Federal Police. Unauthorised surveillance is an offence punishable with imprisonment for five years, a fine or both. Article 25 of the Act obliges telecom operators to permit the Telecommunication and Postal Regulation Authority to enter their sites, network and equipment and install the necessary devices to measure and monitor their performance. Article 25 of the Sudan's national security law of 2020[235] empowers the intelligence agency to request information, data, or documents from anyone.

Under article 23(1) of the Anti-Cybercrime Law (Amendment), 2020[236] anyone who photocopies private writing, or intercepts or eavesdrops on correspondence, can be punished with imprisonment of up to four years, a fine or both. Under article 23(2), the same actions are not considered crimes where they are authorised by the public prosecutor, judiciary or a competent authority. The term ''competent authority'' is not defined, making the law subject to abuse. Under article 8, a person who hacks or intercepts any data or information or captures it through an information or communication network by any tool of information or applications without permission from the competent prosecution shall be punished with imprisonment for a period of up to three years, a fine or both. If the data is of a security nature or related to the national economy or the structure of communications or sensitive information, the punishment is imprisonment for a period of up to five years, a fine or both. The Anti-cybercrime law amends the 2018 Cybercrimes law.[237]

Sudan does not directly restrict encryption, but SIM-card registration requirements limit anonymous communication.[238] Article 15(8) of the regulation for licensing and regulating the work of financial institutions for mobile payment for the year 2020 provides that all transaction data is subject to end-to-end encryption during the transfer process.[239] In addition, article 28 of the 2007 Electronic Transactions Act punishes anyone who discloses encrypted data to any unauthorised party or accesses any piece of information without authorisation with imprisonment for a term of 10 years, a fine, or both.[240]

230 *The State of Identification Systems in Africa: Country Briefs, https://tinyurl.com/y5x7jc9a*
231 *South Sudan Mobile Phone Registration Extended, https://tinyurl.com/5dtyx62*
232 *Africa: SIM Card Registration Only Increases Monitoring Exclusion, https://tinyurl.com/bddpcbfa*
233 *South Sudan — Biometric Registration Update (May 2020), https://tinyurl.com/4pksy748*
234 *Telecommunications and-Postal Regulation Act, 2018, https://tinyurl.com/2p8ebabs*
235 *Sudan's national security law amendments of 2020, https://tinyurl.com/5hc6r86m*
236 *Anti-Cybercrime Law (Amendment), 2020, https://moj.gov.sd/files/download/204*
237 *Cybercrimes bill, 2018 https://drive.google.com/file/d/1IFMoDS6o31hKS7jgg-sq1yHbCUo-djEF/view?usp=sharing*
238 *Freedom House, Freedom on the Net 2020: Sudan, https://freedomhouse.org/country/sudan/freedom-net/2020*
239 *Regulations for licensing and regulating the work of financial institutions for mobile payment for the year 2020, https://bit.ly/3Hx9H25*
240 *Electronic Transactions Act 2007, http://moj.gov.sd/sudanlaws/#/reader/chapter/265*

Article 30(a) of the Regulation of Electronic Authentication Service Providers, 2018[241] requires service providers to use encryption or any other technique as a tool to protect the privacy of electronic transactions, verify the identity of the transaction's creator and to prevent interception, distortion or modification. Article 16(J) of the regulation of filtering and blocking websites and web pages on the internet for the year 2020[242] enacted under article 88(1) of the Telecommunication and Postal Regulation Act for the year 2018[243] prescribes total block of websites that facilitate bypassing of blocking systems.

Article 9 of the General Regulations of the National Telecommunications Authority of 2012,[244] which is based on the Telecommunications Law of 2001, obliges mobile phone service providers to maintain a complete record of subscribers' data, and the authorities began to impose mandatory registration of SIM cards in late 2017. December 31, 2017 was set as the deadline to register subscribers' phone numbers using national identity cards, which include detailed personal information such as residential address and birthplace or passport. Article 20(3)(j) of the Licensing Regulations in the Telecom and Postal Sector of the year 2019 also obliges mobile phone service providers to maintain a complete record of subscribers' data. Registration for a National ID requires a photograph, and fingerprints (all fingers), among others.[245]

**Case Study: State-sanctioned surveillance**

*In February 2017, Citizen Lab published a report mapping the use of spyware sold by Hacking Team, an Italy-based company, by governments across the worlds.[246] The study found that 21 governments, including Sudan, used the company's Remote-Control System (RCS) which ''enables government surveillance of a target's encrypted internet communications, even when the target is connected to a network that the government cannot wiretap." According to the same report: "RCS's capabilities include the ability to copy files from a computer's hard disk, record Skype calls, emails, instant messages, and passwords typed into a web browser. Furthermore, RCS can turn on a device's webcam and microphone to spy on the target".*

*In February 2014 the head of the communications committee in the National Assembly claimed that spying on phone calls and internet censorship would stop.[247] The Sudanese Army has in the past cited the vague terms of the cybercrime law to threaten activists, journalists[248] and even politicians[249] in government for their activities online.*

241 *Regulation of electronic authentication service providers of 2018, https://bit.ly/3eMfgNR*
242 *Regulation of filtering and blocking websites and web pages on the Internet for the year 2020, https://bit.ly/3Hr3PqY*
243 *Telecommunication and Postal Regulation Act for the year 2018, https://tpra.gov.sd/wp-content/uploads/2018/06/Telecommunications-and-Postal-Regulation-Act.pdf*
244 *Telecommunications Law of 2001, https://moj.gov.sd/sudanlaws/#/reader/chapter/214*
245 *General Guide to Facilitating Business Performance, http://www.moi.gov.sd/detailmurshid.php?id=3*
246 *Mapping Hacking Team's "Untraceable" Spyware, https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/*
247 *Online surveillance and censorship in Sudan, https://www.apc.org/en/blog/online-surveillance-and-censorship-sudan*
248 *Sudan's Army Threatens Activists, Journalists with Lawsuits, https://tinyurl.com/3y3z66vb*
249 *Twitter, https://twitter.com/orwaalsadig/status/1359957970793213954*

# 2.24 Togo

Togo's Law No. 2012-018 of 17 December 2012 on electronic communications provides for privacy of communications under article 88, subject to the limitations under the law.[250] Article 92 of the law empowers the Prime Minister, and the Ministers responsible for the economy and finance, defence, justice, and security and civil protection, to trigger the interception of communications and electronic content. The permitted grounds include to protect the security of the state, public order, public health, morals or freedoms and fundamental rights; to safeguard Togo's scientific and economic interests; or to prevent and combat terrorism, drug trafficking, money laundering, criminality, cybercrime and human trafficking.

Under article 91 of the law, a judge can order the interception of electronic communications of a suspect for criminal offences whose penalties are at least two years of imprisonment. The interception decision is not appealable, and the order is valid for up to four months, and is renewable. The law in article 93 provides for the establishment of a Security Interceptions Commission composed of five members whose mandate, and rules of organisation and operation are to be defined by regulation.

Under section 89 of the law, the disclosure of the existence or content of judicial or security interceptions and failing to assist in the execution of an interception decision is punished by imprisonment for between two months to two years, a fine of between five to 30 million CFA francs (USD 8,658-51,949), or both. Section 368 of Law No. 2015-10 of November 24, 2015 on the New Penal Code [251] defines violation of a person's privacy to include among others, organising, by any means whatsoever, the interception, listening or recording of private communications, oral, optical, magnetic or other exchanges received in a private place, without the knowledge or consent of those in the communication or the owner of the premises. Illegal interception by telecommunications service providers is punishable under article 370 of the Penal Code with imprisonment for between one to five years, a fine of five to 20 million CFA francs (USD 8,658-34,633), or both.

Article 94 of Law No. 2012-18[252] on electronic communications obliges encryption service providers to comply with lawful interception orders as stipulated in article 91 and 92. Under article 95 of the same law, cryptology services providers are required to keep content and data allowing the identification of anyone who has used their services, and to provide the technical means that enable the identification of those users for one year. The service providers may also be required to avail this data, on request, to an investigating judge, Prime Minister, Minister for the Economy and Finance, the Minister of Defence, the Minister of Justice, or the Minister of Security. A person who seeks to provide electronic communication services must be licensed by the Electronic Communications and Postal Regulatory Authority (ARCEP). Further, article 61 requires such persons to comply with the laws relating to the supply, export, import or use of means or services of encryption, and declare in advance or request authorisation from the regulator.

Under Law No. 2012-18, the refusal to provide secret decryption codes to government agencies, when required, is punishable by a fine of between USD 3,544 to USD 14,178. Also, article 373 of the Law No. 2015-10 on the Penal Code[253] provides that operating a telecoms network, or providing a telecoms or electronic communications service, cryptology and hosting services without complying is punishable with imprisonment for a period of between six months to two years, a fine of between 25and 200 million CFA francs (USD 42,828-342,629), or both.

250 *Law No. 2012-018 of 17 12 2012 on electronic communications provides for privacy of communications, http://droit-afrique.com/upload/doc/togo/Togo-Loi-2012-18-communications-electroniques.pdf*

251 *Law No. 2015-10 of November 24, 2015 on the New Penal Code, https://www.policinglaw.info/assets/downloads/Code_p%C3%A9nale_du_Togo_(2015).pdf*

252 *Law No. 2012-18 on electronic communication, http://droit-afrique.com/upload/doc/togo/Togo-Loi-2012-18-communications-electroniques.pdf*

253 *Law No. 2015-10 on the Penal Code, https://tinyurl.com/mr3nu97a*

Article 28 of law No. 2019-014 of October 29, 2019 relating to the protection of personal data[254] in Togo provides that a data controller can only transfer personal data to a third country if that country ensures a sufficient level of protection of the privacy, freedoms and fundamental rights of individuals with regard to the processing to which the data is subject or may be the subject.

Article 29 provides for authorisation of one-off transfers of personal data, stating that the controller may transfer personal data to a third country that does not meet the conditions provided for in article 28 if the transfer is one-off, not massive, and the person to whom the data refers has expressly consented to the transfer. Further, the transfer may be authorised if it is necessary to safeguard the life of this person; to safeguard the public interest; in compliance with obligations to ensure the establishment, exercise or defence of a legal right; or the execution of a contract between the data controller and the interested party, or of pre-contractual measures taken at the request of the latter. According to article 82, unauthorised processing of identifying personal data is punished with imprisonment for one to five years or a fine of one to 10 million CFA francs (USD 1,747-17,472) or both.

In 2020, the Togolese parliament passed Law No. 2020-009 of September 10, 2020 relating to the biometric identification of natural persons in Togo.[255] Per article 1, the objective of this law is to establish a system for the identification and authentication of natural persons. It aims to establish a "secure and reliable methodology" for obtaining, maintaining, storing and updating data on the identity of registered individuals. This law applies to all Togolese citizens present or not on the national territory as well as any person staying temporarily or permanently in Togo (article 2). Biometric data is defined according to article 3 as "photograph and / or facial recognition, fingerprints, retinal recognition or any other biological attribute of an individual which may be specified by the regulations."

Any Togolese and any person residing temporarily or permanently in Togo has the right to obtain a Unique Identification Number (NIU) by submitting their demographic and biometric data (article 4). To obtain the NIU, biometric data are mandatory and are provided by each candidate for registration with the exception of children under five years old. The biometric data specified in article 7 are photography and / or facial recognition; the 10 fingerprints; and a scan of both irises. For people with biometric exceptions, the following data is collected: the available biometric data of the person; and the photograph of the biometric exception.

The 2020 law on biometric identification strengthens the Law No. 2019-014 of October 29, 2019 relating to the protection of personal data[256] but also allows the government to launch the e-ID project,[257] with an aim to modernise public services and social inclusion mechanisms and promote the establishment of a single social register, universal health coverage, and the digitisation of civil status.

**254** *Togo, Law No. 2019-014 of October 29, 2019 relating to the protection of personal data, https://bit.ly/3kv4778*

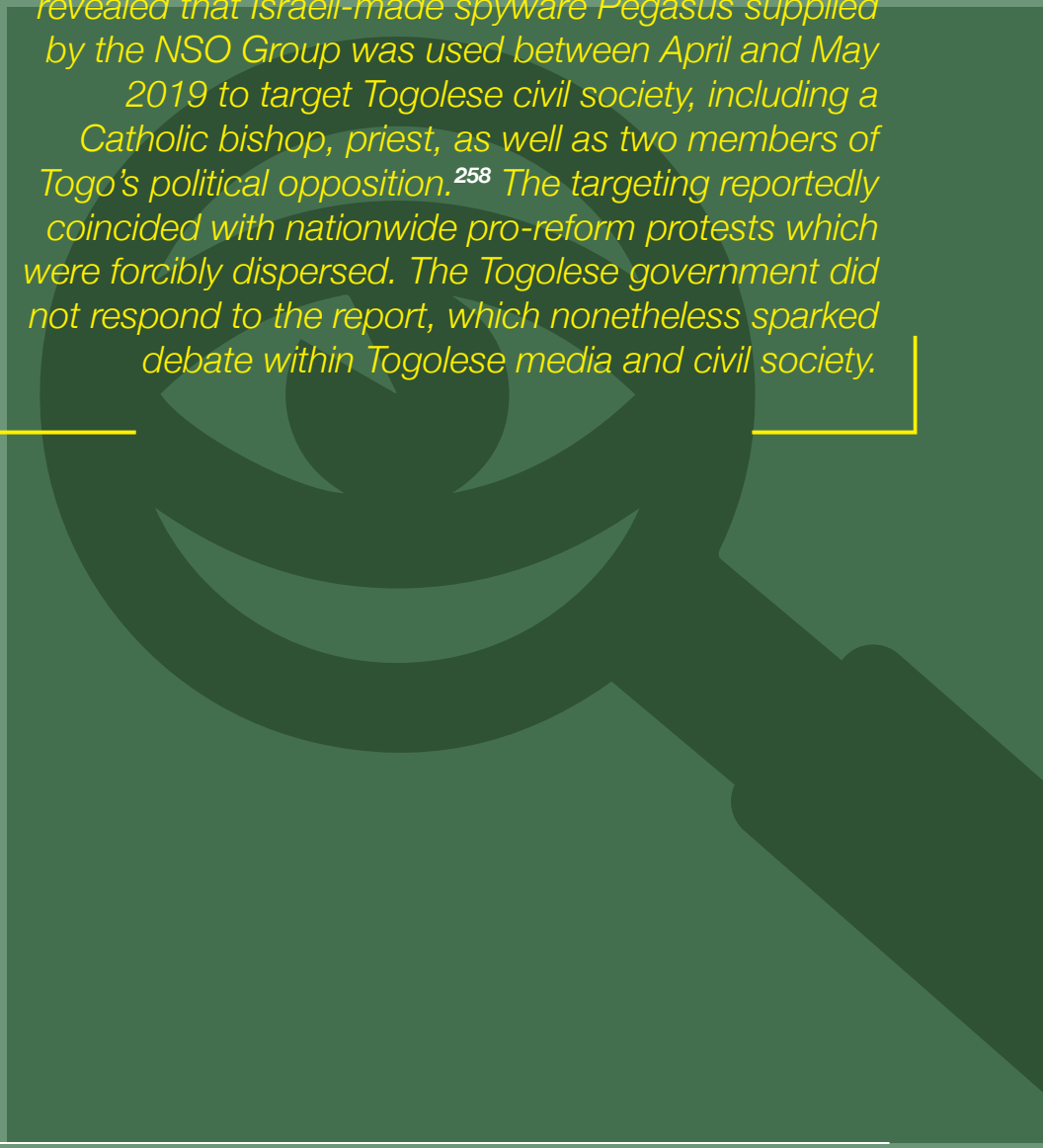
**255** *Law No. 2020-009 of September 10, 2020 relating to the biometric identification of natural persons in Togo, http://citizenshiprightsafrica.org/wp-content/uploads/2020/12/Togo-Loi-relative-a-lidentification-biometrique-2020.pdf*

**256** *Law No. 2019-014 of October 29, 2019 relating to the protection of personal data, https://tinyurl.com/ypayerkz*

**257** *Le projet de loi sur l'identification nationale biométrique « e-ID Togo » adopté en Conseil des Ministres, https://tinyurl.com/mry7he6t*

In July 2021, a campaign to identify mobile phone subscribers and to limit the number of SIM cards per user to three each per network was launched by the telecommunications regulatory authority ARCEP, supported by the telecom operators Moov Africa Togo and TogoCom. To purchase a SIM card in Togo, a subscriber needs to submit a national identity card or passport.

**Case Study:** *In 2020, lingering suspicions that the Togolese government was undertaking interceptions of communications gained credence when it was revealed that Israeli-made spyware Pegasus supplied by the NSO Group was used between April and May 2019 to target Togolese civil society, including a Catholic bishop, priest, as well as two members of Togo's political opposition.*[258] *The targeting reportedly coincided with nationwide pro-reform protests which were forcibly dispersed. The Togolese government did not respond to the report, which nonetheless sparked debate within Togolese media and civil society.*



258 *Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware, https://citizenlab.ca/2020/08/nothing-sacred-nso-spyware-in-togo/*

# Discussion and Conclusions 3.0

## 3.1 Surveillance

### 3.1.1 Imposition of Liability on Intermediaries

Laws in countries such as Angola, require intermediaries such as telecom companies and Internet Service Providers (ISPs) to facilitate surveillance. The measures required include the installation of software and equipment to facilitate surveillance operations by the designated government bodies. For example, in Burundi, article 10 of Order 540/356 requires service providers to comply with any request from the ARCT. In Gabon, intermediaries are required to install data traffic monitoring mechanisms on their networks, and to keep connection and traffic data for a period of 10 years in case required for judicial investigations.

In some instances, intermediaries are also required to identify the authors and publishers of content and to keep the content of all electronic transactions. In Lesotho, intermediaries are obliged to cooperate with law enforcement with court orders. In Liberia, intermediaries may be required to monitor telecommunications to and from a customer's telephone, and provide authorities with the information obtained from the monitoring. In Mauritius, the ICT Authority (ICTA) is mandated to prevent the spread of abusive, harmful and illegal content, and intermediaries are obliged to intercept, withhold or deal with such content with ICTA's direction. In Niger, intermediaries are obliged to monitor or block access to some content stored on their platforms when ordered by the police or courts.

Where a service provider fails to cooperate, the laws impose punitive penalties. For example, in Burundi, the failure to cooperate attracts a daily fine of USD 2,000. Moreover, service providers are in some countries required to retain data for specific periods. For example in Niger, financial institutions are required to maintain customer information for up to 10 years. Emerging good practice includes in Burkina Faso, Congo Brazzaville, where service providers are required to erase or anonymise any traffic or location data. Likewise, in The Gambia, intermediaries are required to take technical and organisational measures to block unauthorised interception, and to only use communication apparatus to ensure the privacy of communications.

### 3.1.2 Weak Oversight of Surveillance Operations

The place of independent judicial oversight over surveillance operations remains problematic in various countries. In some countries, surveillance operations are entirely carried out and overseen by bodies within the executive. For instance, in Congo Brazzaville, surveillance is overseen by the Public Prosecutor; in Lesotho, the warrants may be issued by the Minister responsible for the National Security Services; in Niger, interception is ordered by the President; in South Sudan the Director General of the National Security Service; in Sudan, by the Public Prosecutor or a specialised Judge; in The Gambia, the Minister of Interior; while in Togo, the Prime Minister, and the Ministers responsible for the economy and finance, defence, justice, and security and civil protection.

Another emerging issue is the requirement for warrants prior to the conduct of surveillance operations, and the duration of such warrants once issued. In countries such as Madagascar, warrants are not required during emergency situations, while in Sierra Leone, they may not be required during the investigation of specific criminal activities relating to bodily harm, death, damage to property or financial loss.
The period of validity of warrants varies across countries. In Cape Verde and South Sudan the period is 30 days; in Mauritius and Sierra Leone it is 60 days; in the Democratic Republic of the Congo (DRC), Madagascar, and Niger the period is three months; in Togo, the period is four months; while in Guinea, it is for as long as it is considered necessary.

Some countries also provide wide exceptions where the surveillance is justified. In Benin, Democratic Republic of the Congo (DRC), Morocco, Niger, Togo, these justifications are specified under the law. The key justifications provided in most countries for conducting surveillance include: the preservation of national security or defence, investigation of crimes, prevention of terrorism, organised crime, and activities that undermine public peace or public order. However, these crimes are not defined, or are vaguely defined, in the various laws, which gives latitude to state authorities to broadly interpret these laws in undermining the rights of critics and opponents.

Good practice was noted in some countries where warrants are issued by a judicial authority subject to the application for intercept meeting the threshold provided for under the law. In Benin, Cape Verde, Côte d'Ivoire, Liberia, Madagascar, Mauritius, Sao Tome & Principe, and Sierra Leone, surveillance is supervised by a judge. Unlawful surveillance is prohibited in Benin, Burkina Faso, Cape Verde, Central Africa Republic (CAR), Congo Brazzaville, Côte d'Ivoire, Democratic Republic of the Congo (DRC), Gabon, Lesotho, Madagascar, Mauritius, Morocco, Niger, Sierra Leone, South Sudan, and Sudan. Notably, illegal interception in Lesotho will attract the highest fine of USD 674,791 and imprisonment of up to 15 years if proposals in the Computer Crimes and Cybersecurity Bill 2021 are adopted.

From the foregoing and even as discussions on the need to respect privacy of citizens continues across the continent, surveillance laws and practices vary across countries, mostly diverting from well-established international human rights standards, including Principle 41 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa. Surveillance laws continue to be implemented indiscriminately and in an opaque landscape with limited transparency and oversight by competent judicial authorities. More importantly, the failure to enact comprehensive privacy laws, in the absence of effective constitutional guarantees to the right, opens the door for unchecked executive surveillance powers, and leaves citizens with weak due process safeguards, and limited opportunities to exercise or enjoy their rights, and seek redress in cases of abuse.

# 3.2 Limitations on the Use of Encryption

## 3.2.1 Prohibitive Encryption Regulation

Encryption concerns in Africa include prohibitive regulation that hampers the use of encryption and compelled assistance by service providers,[259] which can be exploited by states and their agencies to undermine citizens' right to privacy and various other digital rights. As the present research found, a number of countries have requirements for registration of encryption service providers, regulators can ban the use of some types of encryption services, and service providers are under obligation to decrypt data at the behest of courts of law or sector regulators. Such provisions limiting the use of encryption are not found in stand-alone laws but are scattered in various laws, including those on data protection, on computer misuse and cybercrime, on regulating telecom and internet service providers. Not all African countries have laws and regulations related to the use of encryption, yet others have more than one law that deals with encryption.

Majority of the countries that restrict the use of certain types of encryption require the licensing of services providers with the regulator who is empowered to withdraw licences and order the prohibition of some means of encryption. Oversight is not always clear: some countries have telecom regulators in charge, others give a role to the Council of Ministers, while some have vested the regulation of encryption matters in the hands of security agencies.

In Algeria, acquisition and use of encryption by individuals and organisations must be authorised by the Regulatory Authority of Post and Electronic Communications (ARPCE) after a favourable opinion from the Ministry of Defence and the Ministry of the Interior (articles 17 and 20 of Executive Decree No. 09-410 of December 10, 2009 setting the safety rules applicable to sensitive equipment). Further, Algerian law requires that the type and nature of the equipment that will be used, list of cryptography algorithms, the size of the encryption keys, the type of VPN used, the authentication methods, and the Public IP address be provided to the regulator while applying for authorisation.

Many other countries require registration, with many of them also requiring service providers to disclose the technical characteristics of the cryptology means, and the source code of the software used. In many countries, mostly in Francophone Africa, authorisation is only needed if the encryption is not exclusively for providing authentication or integrity control functions. This is the case in DR Congo (article 146a of the 2020 Law on Telecoms and ICT); The Central African Republic (article 100 of the Electronic Communications Law of 2018); Gabon (article 30 of the cybersecurity and cybercrime law); Niger (article 52 of the law on protection of personal data); Benin (article 622 of the Digital Code); Guinea Conakry (article 57 of the cybersecurity and personal data protection law); Ivory Coast where the service providers' licences have to be renewed by the regulator ARTCI after three years (article 7 and 8 of the law on encryption); Congo Brazzaville (article 145 of the law on electronic communications); Morocco (article 13 of 2007 law on the electronic exchange of legal data); Togo (article 61 of the electronic communication law); Burkina Faso (article 17 of the 1998 law reforming the telecommunications sector).

Angola also requires encryption service providers to register with the regulator INACOM (article 31 of the Law on Protection of Information Networks and Systems) as does Sierra Leone (article 41 of the Cybersecurity and Cybercrime Act 2021).

Moreover, some countries place more blatant limitations on the use of certain types of encryption. For instance, under articles 7 and 8 of the Ivory Coast's 2014 law on encryption, the use of the means and services of cryptology beyond 32 bits for confidentiality is subject to authorisation. Besides the countries studied, another African country that places such limits on the types of encryption is Senegal where encryption is to be used only if the key length is less than or equal to 128 bits (article 13 of Decree No. 2010-1209 on Cryptology).

259 *Mapping and Analysis of Privacy Laws and Policies in Africa, https://cipesa.org/?wpfb_dl=454*

Other countries, such as Mali (Article 37 of the Cybercrime Act 2016), Tanzania (Section 35(2)(d) of the Electronic Transactions Act, 2015), Congo Brazzaville (article 145 of the Law on Electronic Communication), and Malawi (Section 67(1) of the Electronic Transaction and Cyber Security Act, 2016) require service providers to disclose the technical characteristics of the source code of the software to be used.[260]

The evidence from several countries thus shows that many governments have prohibited the use of encryption by grade or type, whereas they should not mandate insecure encryption algorithms, standards, tools, or technologies.[261] Such prohibitive regulations undermine privacy and freedom of expression since encryption facilitates the enjoyment of rights by assuring individuals of the privacy of their communication. Further, these limitations go against Principle 40(3) of the Declaration of Principles on Freedom of Expression and Access to Information in Africa, which 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."

## 3.2.2 Compelled Assistance by Service Providers

A common element in the laws of several countries is the requirement for encryption service providers to render assistance to state agencies such as law enforcement units, whenever such assistance is required. The laws in several countries specify that, at the request of state agencies, including courts of law and regulators, service providers should not only hand over the encrypted data they hold but should also decrypt such data before passing it on to state authorities. Such compelled assistance is quite worrisome as this gives governments and their agencies unfettered access to individuals' private data beyond prescribed limits.[263]

In Benin, the Digital Code specifies compelled assistance to judicial authorities (article 630) as does article 52 of Niger's 2017 data protection law that requires cryptology service providers to lift the encryption if requested by the regulator, HAPDP, and in Ivory Coast (article 16 of Decree No. 2014-105), competent administrative or judicial authorities can access secret codes of encrypted data upon request to the regulator (ARTCI), or order decryption of data through the help of ARTCI. Article 34 and 37 of Gabon's law on cyber security and the fight against cybercrime demand that encrypted data must be decrypted during an investigation upon requisition by the Public Prosecutor, the Examining Magistrate or the trial court.

On its part, Sierra Leone's Cybersecurity and Cybercrime Act 2021 under articles 38 and 40, requires an electronic communication service provider to ensure that they use a system that is technically capable of supporting lawful interceptions. Sierra Leone's cybercrimes law of 2021 also empowers a judge to issue a warrant authorising a police officer or other authorised persons to "have access to any information, code or technology which has the capability of unscrambling encrypted data contained or available to a computer system into an intelligible format for the purpose of the warrant."

Whereas many countries do not explain the rationale behind the prohibitive regulation of encryption, others have indicated that this is to safeguard national security interests. In Ivory Coast the ARTCI is tasked to ensure that no service provider employs encryption that is contrary to public order or which undermines the interests of national defence, internal or external security of the state. Moroccan and Central African legislation states that the reason for restricting import and use of encryption is "to prevent its use for illegal purposes, and to protect the interests of national defence and the internal or external security of the State." In that spirit, in 2015 the responsibility for authorising and monitoring "electronic certifications" including encryption in Morocco, was moved from the civilian National Telecommunications Regulatory Agency (ANRT) to the military's General Directorate for the Security of Information Systems (DGSSI).

260 *How African Governments Undermine the Use of Encryption, https://cipesa.org/?wpfb_dl=477*
261 *Secure the Net, https://securetheinternet.org/#letter%E2%80%9D*
262 *How African Governments Undermine the Use of Encryption, https://cipesa.org/?wpfb_dl=477*

It is also notable that countries have set hefty fines for those who offer encryption services without authorisation or that use prohibited encryption means - a measure intended to compel compliance by citizens and service providers. A typical example is Congo Brazzaville, where the sanctions the ANSSI can slap on any encryption service provider include temporary withdrawal to the definitive withdrawal of a licence, as presented by article 38 of the law on cybersecurity; and penalties of between three to six months in prison, or a fine USD 1,800 to USD 9,000 for anyone who uses a means of cryptology without prior authorisation. In Guinea Conakry the punishment is imprisonment of one to five years.

In Togo, refusal to provide secret decryption codes to government agencies is punishable by a fine of USD 3,544-14,178. Cryptology services providers are required to keep for one year, content and data allowing the identification of anyone who has used their services, and to avail this data, on request, to the investigating judge, Prime Minister, Minister for the Economy and Finance, the Minister of Defence, the Minister of Justice, and the Minister of Security (article 95 of the 2012 electronic communication law). And in Madagascar, declining to reveal the encryption key to authorities to aid their investigation can be punished by one to five years imprisonment or a fine between USD 2,777 and USD 25,775.

## 3.3 Data Localisation

Most of the countries studied have prohibited cross-border transfers of personal data unless authorised by the data protection authorities or other designated entities. These include Algeria (article 44 of data protection law; article 10 of ARPCE directive on cloud computing; and the 2018 law on e-commerce), Niger (article 24 of the data protection law), Morocco (articles 43 and 44 of the law No. 09-08 on Processing of Personal Data, 2009), Angola (article 34 of DPA), Benin (article 391 of the Benin Digital Code), Burkina Faso (article 42 of the law No. 001-2021 / AN), Cape Verde (article 19 of the Data Protection Act), Madagascar (article 20 of the Personal Data Protection Law), Mauritius (section 36 of the Data Protection Act), Lesotho (article 52 of the Data Protection Act 2011), Guinea Conakry (article 28 of the cybersecurity and personal data protection law), Ivory Coast (article 7 of the data protection law), Congo Brazzaville (article 23 of the personal data protection law), Sao Tome & Principe (article 19 of the law on data protection), and Togo (article 28 of the data protection law).

The conditions for cross-border transfer authorisation are the same in most countries. They require the regulator (mostly the Data Protection Authority, in some instances the telecoms industry regulator) to allow data export after establishing that the country or organisation to which the data is to be transferred has a similar or higher level of data protection as that of the country of origin of the data. The laws also generally provide similar grounds for when personal data may be sent across borders to a country that does not have an adequate level of data protection. Such transfers may be authorised if the individual has given their consent unambiguously to the proposed transfer, or the transfer is necessary for the performance of a contract between the individual and the data controller, or for law enforcement purposes.

Some countries have gone beyond the provisions of personal data protection laws to legislate other data localisation requirements. Morocco requires companies and organisations operating in sectors of purported vital importance and using data deemed sensitive, to host their infrastructure and digital databases on Moroccan territory. Additionally, the National Telecommunications Regulatory Agency requires[263] service providers commercialising the ".ma" domain name to set up and maintain a secure DNS service platform made up of at least two DNS servers, including at least one server hosted in Morocco. Similarly, Algeria requires operators of public cloud computing services to establish its infrastructure on Algerian territory and to host and store their data locally (article 10 of decision No. 48/SP/PC/ARPT/17 of 29 November 2017).[264] Algeria also requires local e-commerce operators to host their websites in Algeria and with an extension of the ".dz" domain name (article 6 Law No. 18-05 of May 10, 2018 relating to electronic commerce). Meanwhile, Sierra Leone's Telecommunications Subscribers Identification and Registration Management Regulations 2020 prohibit the cross-border transfer of subscribers' registration information without approval by the National Telecommunications Commission.

A previous study by CIPESA found that several African countries have adopted different approaches towards data localisation.[265] Several countries use laws on financial services (Nigeria, Ethiopia and Rwanda), cybersecurity and cybercrimes (Rwanda, Zambia and Zimbabwe), telecommunications (Cameroon, Rwanda and Nigeria) and data protection (Kenya, South Africa, Tunisia and Uganda) to place restrictions on cross-border transfer of data. Some countries have specified the data that cannot be exported without authorisation. Kenya specifies all public data; Nigeria mentions all government data and all subscriber and consumer data; while Zimbabwe, Malawi and Tunisia cite personal information. Previous research also showed that among the growing number of African countries that have been legislating on data localisation, this has mostly taken the form of a requirement to store data locally and forbidding unauthorised cross-border data transfers.[266]

While law provisions are in place, enforcement is still largely lacking. Data protection bodies created by the countries' respective laws are, in many instances, not operational, and in others, there is limited evidence as to how - if at all - they enforce the legal provisions relating to cross-border data transfers. Ivory Coast, as an example, has some novel provisions, notably article 8, which requires controllers to submit to the ARTCI an annual activity report on the transfer of personal data to third countries, yet there is no evidence that this measure is implemented.

Nonetheless, in a few countries there is some evidence of implementation of data localisation measures. For instance, the National Commission for the Protection of Personal Data (CNDP) published the list of countries that offer a sufficient level of protection and complies with the requirements of Moroccan legislation relating to processing of personal data. In its Deliberation[267] No. 236-2015 of 2015, the CNDP listed 32 countries (none of them African) considered to satisfy these requirements.

It is also noteworthy that in many instances, the laws are not clear on the rationale behind the data localisation requirements. Nonetheless, a few have provided justifications, including those related to national security. For example, article 44 of Algeria's 2018 data protection law prohibits any transfer of personal data to a foreign state when it is likely to harm public security or the vital interests of Algeria. Ivory Coast's 2016 law on fighting money laundering and financing of terrorism provides that cross-border data sharing may be prohibited if it infringes the Ivorian sovereignty or national interests as well as security and public order (article 78).

263 *ANRT Morocco, Service provider agreement n ° ../ma/20../ANRT relating to the marketing of ".ma" domain names, https://bit.ly/3c24At4*

264 *Algeria, Decision No. 48/SP/PC/ARPT/17 dated 29 November 2017, https://bit.ly/3F9rKKH*

265 *How Surveillance, Collection of Biometric Data and Limitation of Encryption are Undermining Privacy Rights in Africa https://cipesa.org/2021/07/how-surveillance-collection-of-biometric-data-and-limitation-of-encryption-are-undermining-privacy-rights-in-africa-2/*

266 *CIPESA, Mapping and Analysis of Privacy Laws and Policies in Africa, https://cipesa.org/?wpfb_dl=454*

267 *CNDP Morocco, Deliberation No. 236-2015 of 2015, https://bit.ly/3C5aKmE*

## 3.4 Biometric Data Collection Concerns

In all the countries studied there has been mass collection of data amidst lack of adequate data protection safeguards, both legal and practical. The common grounds for data collection include registration of persons for purposes of issuing national identity cards, drivers' licenses and passports, as well as SIM card registration. Thus, there has been massive collection, storage and processing of personal data in some instances without proper oversight mechanisms and provision for remedies in case of data breaches. Most of the countries studied fall short of prescribed safeguards under international human rights law and there are insufficient checks and balances on collection, processing, and access to personal data.

It can thus be deduced that a number of countries studied fail to comply with Principle 40 of the Declaration, which recognises everyone's right to privacy, including the confidentiality of their communications and the protection of their personal information. Equally, several countries also fail to meet the expectations of Principle 42 of the Declaration, which enjoins states to adopt laws to protect the personal information of individuals in accordance with international human rights law and standards. Some of the laws in place have flaws, while others are partially implemented, thereby undermining their effectiveness. Principle 42 requires that these laws should provide effective remedies and adequate oversight for the protection of personal information. In numerous countries, the element of adequate oversight is hugely lacking.

Indeed, consistent with previous research,[268] the present study found that government agencies in most countries are collecting and processing personal data without adequate data protection laws, amidst limited oversight mechanisms and inadequate remedies; and 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.

Mandatory SIM card registration is a common denominator around the continent, and the SIM registration data is linked in many countries to other databases and services provision. The SIM card registration requires a national ID or passport or driving licence in such countries as Algeria, Angola, Burundi, Gabon, Guinea Conakry, Ivory Coast, Liberia, Niger, Sao Tome, Sierra, and Togo. Among the attendant worries is that the threshold for access to information in the SIM card databases is low in some countries, with the regulatory authority often having the powers to direct telecom operators to hand over such data. Similarly worrying is the ease of access to this data by security agencies, particularly in instances where there is no robust judicial oversight. This goes against best principles that would require judicial authorisation for access to such sensitive data.

The continent has in recent years seen countries enact data protection laws including in Kenya, Gabon, Uganda, Lesotho, Mauritius, Morocco, Niger, Sao Tome, Togo, Algeria, Congo Brazzaville and Ivory Coast. However, some of these laws fall short of minimum standards for the guarantee of the right to privacy. Indeed, the respective countries have other pieces of legislation which facilitate access to personal data by the state and its agencies, such as security entities, in the name of keeping national security and maintaining law and order and the general public good. For instance, in Algeria, under article 18 of the Law No. 18-07 of 2018 on protection of personal data, sensitive personal data may be processed in public interest. The country started issuing biometric passports in 2012 and in 2017, a national biometric electronic identity card was established, and then in 2019 the country embarked on converting driving licences to biometric format. Morocco similarly has a biometric ID, e-passport, and voters registration system, while in Algeria there is an electronic biometric passport, national ID, and biometric card for justice sector professionals.

268 *Mapping and Analysis of Privacy Laws and Policies in Africa Summary Report https://cipesa.org/?wpfb_dl=454*

Mass data collection and storage is a major threat to individual privacy since data subjects have limited control over their data and given the poor data protection practices. Indeed, in most cases state agencies are given an upper hand of control over access to personal data, as well as surveillance and interception of communications, as opposed to placing complete oversight in the judiciary. For instance, under article 14 of Ivory's Coast 2017 decree on SIM card registration, subscriber data can only be accessed by third parties in the event of an investigation or judicial process, upon written request from the competent judicial authority, and by agents appointed by the regulator, ARTCI.

# 4.0 Recommendations

The report has identified and revealed 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.

## It is recommended that Governments should:

- Swiftly enact data protection laws where they are yet to do so, such as in Liberia, Sierra Leone and South Sudan to provide for and guarantee protection of personal data. Such laws should comply with regional and international human rights standards on data protection and privacy and should be developed through multi-stakeholder participation processes.
- 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.
- Comply with their obligations under article 9 of the African Charter on the right to receive information and free expression, as supplemented by Principle 40(3) of the Declaration which provides that States shall not adopt laws or other measures that prohibit or weaken encryption or that impose data localisation requirements.
- Cease blanket compelled service provider assistance and provide for clear, activity-bound and court-mandated assistance.
- Submit periodic reports to the different international human rights treaty body monitoring mechanisms such as the African Commission on Human and Peoples' Rights, the Human Rights Committee and the Universal Periodic Review process, on the status of implementation of relevant national, regional and international laws and the measures taken to guarantee the right to privacy and data protection.

## It is recommended that Civil Society should:

- Work collaboratively with other stakeholders such as the private sector and academia, including through litigation to challenge laws and measures that violate privacy rights and push for internationally recognised privacy and data protection legislation and practices.
- 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 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.
- Participate in law making processes by conducting analysis of proposed laws on surveillance, data protection, privacy, and encryption to identify the gaps and make proposals for reform before they are enacted into law.
- 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.

## It is recommended that the Private sector should:

- 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.
- Regularly publish transparency reports that highlight all cases of personal data and information disclosure to government agencies as well as other assistance offered to governments to enable communication interception and monitoring.
- Develop technologies and solutions and use privacy-enhancing technologies that embed and integrate privacy principles by design and default.
- Work in partnership with other stakeholders such as the civil society for collective action in mechanisms that would better the enjoyment of human rights.
- 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.

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