How African Governments Undermine the Use of Encryption

October **2021**

Introduction

Encryption is the ability to encode communications (or information or data) so that only the intended recipient can access, read or understand them.[1] As such, encryption technologies enable internet users to protect the confidentiality of their data and communications from unwanted observation and intrusion.[2] Worryingly, many African countries have passed legislation that limits anonymity and the use of encryption, purportedly to aid governments' efforts to combat terrorism and crime.

Just as individuals have the right to protect their offline assets and property, they should have the right to use encryption and other tools to protect their data, digital assets, and online activities.
Internet Society, Encryption

Other governments limit the use of encryption to enable them to monitor the communications of critical journalists, human rights defenders, and opposition politicians.

These laws and practices undermine the privacy rights of citizens, which in turn hampers their right to free expression and to secure use of digital technologies.

Encryption and Human Rights

Anonymity and the use of encryption in digital communications are critical to freedom of expression and the right to privacy. This is because, without adequate protection of the right to privacy, there is no guarantee for anonymity of communications.[3] Likewise, encryption and tools that enable individuals to stay anonymous protect such individuals' privacy and offer them the confidence to use digital technologies with minimal fear of attracting reprisals.

The importance of the right to anonymity in the digital era has been recognised in the Declaration of Principles on Freedom of Expression and Access to Information in Africa of the African Commission on Human and Peoples' Rights. Principle 40(3) 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."[4]

Indeed, laws, policies and practices that undermine encryption and anonymity significantly and disproportionately violate the rights enshrined in article 19 of the International Covenant on Civil and Political Rights (ICCPR).[5]

1 *Global Partners Digital, Encryption Policy for Human Rights Defenders*
2 *Internet Society, Encryption*
3 *Privacy International, Submission to the UN Special Rapporteur on freedom of expression – anonymity, and encryption in digital communications*
4 *Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019*
5 *How Undermining encryption threatens Online User Security in Africa*

Encryption Concerns in Africa

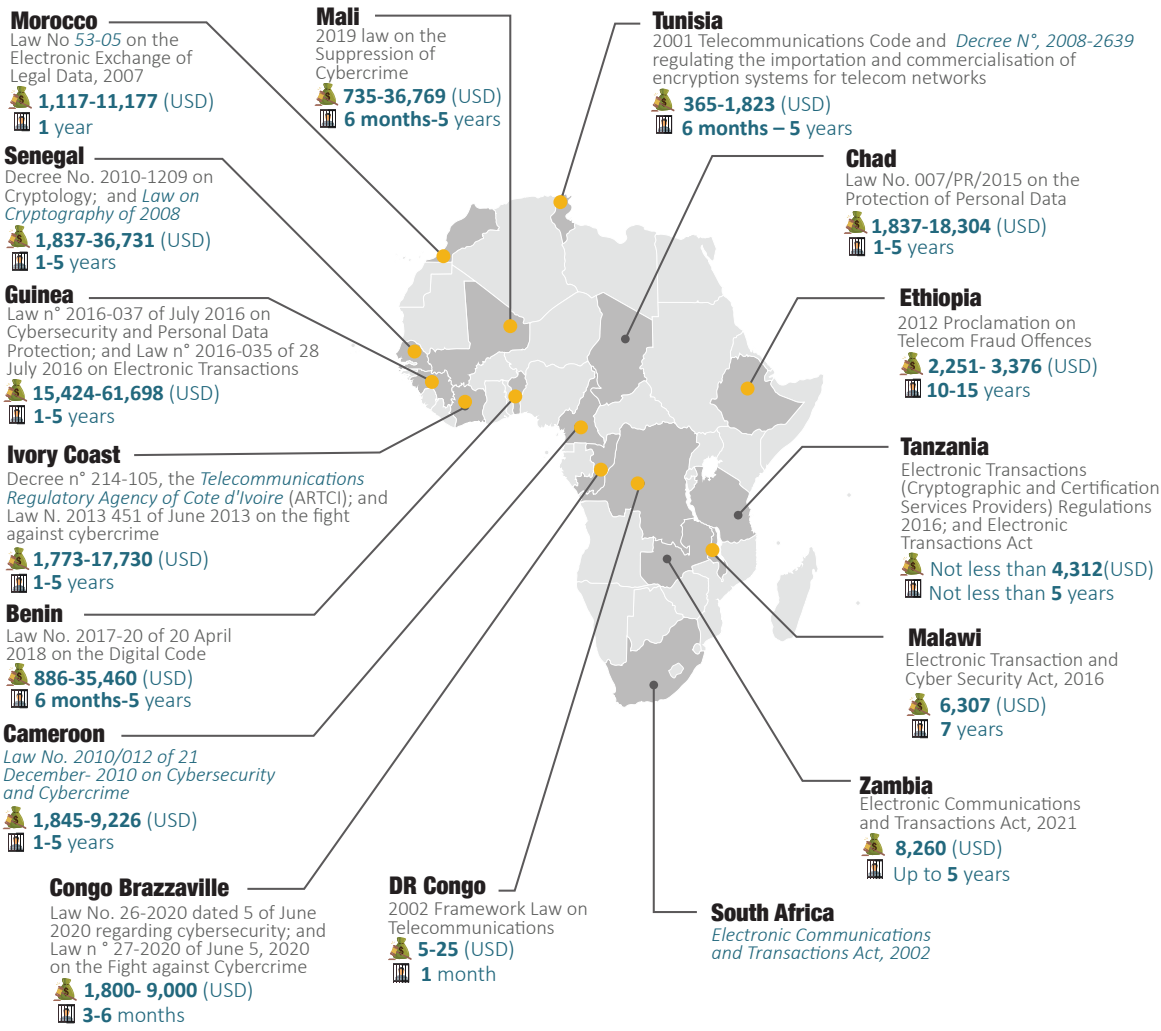
Encryption concerns in Africa include prohibitive regulation that hampers the use of encryption, compelled assistance by service providers, mandatory SIM card registration, and data localisation requirements. All these can be exploited especially by states and their agencies to undermine citizens' right to privacy and various other digital rights.

Most of us use encryption every day without even realising it: whether that's storing information on our computers or smartphones with a PIN or password, visiting secure websites (such as those whose addresses start with 'https'), or using instant messaging apps like WhatsApp.
Global Partners Digital, Encryption Policy for Human Rights Defenders

Prohibitive Regulation

In several African countries, the regulation of encryption services is overbearing with emphasis on prohibition and limitation of usage. Various countries' laws require registration and licensing of encryption service providers, and regulators have extensive powers to prohibit the use of some encryption technologies. Moreover, offering encryption services without licenses attracts penalties, as does failure to hand over secret encryption codes to state authorities, or using prohibited encryption tools.

Figure 1: Regulation of Encryption



The requirement for registration of encryption services providers makes it easy for regulators and other government agencies to access information held by encryption services providers, including decryption keys and encrypted data. This undermines *best practices* which require governments to reject laws, policies, and practices that limit access to or undermine encryption and other secure communications tools and technologies.

For instance, in Morocco, according to the law No 53005 on Electronic Exchange of Legal Data, the purpose of regulation of encryption is "to prevent its use for illegal purposes, and to protect the interests of national defense and the internal or external security of the State". *Decree* No 2-13-881 of January 2015 shifted responsibility for authorising and monitoring “electronic certifications” including encryption, from the civilian National Telecommunications Regulatory Agency (ANRT) to the military’s General Directorate for the Security of Information Systems (DGSSI).

In Namibia, prohibitive provisions point to possession, import, export, distribution, or sale of any equipment or software contrary to Article 76 of Namibia's Communications Act that "may be used to prevent lawful interception or monitoring or to render it less effective with a fine of N$20,000 (USD 1,343), imprisonment for five years, or both. Similarly in Nigeria, Rule 11 of the *Lawful Interception of Communication Regulations* prohibits licensees from providing any communications services that cannot be monitored and intercepted. It is the same story in Zimbabwe, where Section 12(1)(a) of the Interception of Communications Act of 2007 bars telecom service providers from providing service which the state lacks the capability to intercept.

Limitation on Use of Certain Types of Encryption

It is imperative that governments do not prohibit the use of encryption by grade or type. Further, governments *should not mandate* insecure encryption algorithms, standards, tools, or technologies. Yet, some African countries prohibit the use of some types of encryption and require disclosure to regulators of the characteristics of cryptology, as examples in figure 2 show.

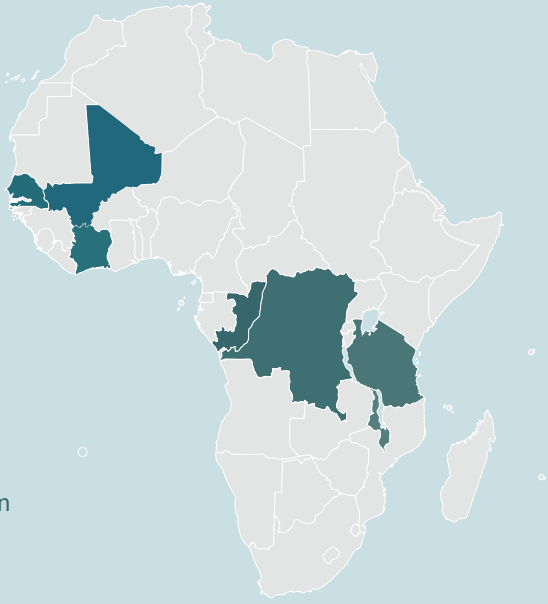
Users should have the option to use – and companies the option to provide – the strongest encryption available, including end-to-end encryption, without fear that governments will compel access to the content, metadata, or encryption keys without due process and respect for human rights.
Secure the Internet

Figure 2: Limitations on Types of Encryption

Senegal
Article 13 of *Decree No. 2010-1209 on Cryptology*
Encryption is to be used only if the key length is less than or equal to 128 bits

Disclosure of the technical characteristics of the cryptology to the National Cryptology Commission

Mali
Article 37 of Cybercrime Act 2016
Cryptographic services service providers must inform the regulator of the technical characteristics of the means of cryptology and the source code of the software used.



Ivory Coast
Articles 7 and 8 of Decree n° 214-105
Use of the means and services of cryptology beyond 32 bits for confidentiality is subject to authorisation

Tanzania
Section 35(2)(d) of *the Electronic Transactions Act, 2015*
Applicants for a license must disclose a description of the technology to be applied in their services.

Congo Brazzaville
Article 145 of the Law on Electronic Communication
Disclosure of the technical characteristics of the source code of the software to be used to the National Agency for Information Systems Security (ANSSI)

DR Congo
Article 146a of the the 2020 Law on Telecoms and ICT
Disclosure of the description of the technical characteristics of the cryptology means, as well as the source code of the software used

Malawi
Section 67(1) of the Electronic Transaction and Cyber Security Act, 2016
Declaration of "the technical characteristics of the encryption as well as the source code of the software used" to the Malawi Communications Regulatory Authority (MACRA)

A notable exception is Zambia, whose section 85 of the *Electronic Communications and Transactions Act, 2021* permits the use of encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

Compelled Assistance by Service Providers

Laws on interception of communications across the continent including in Benin, Cameroon, Chad, Ivory Coast, Malawi, Mali, Niger, Nigeria, Rwanda, Senegal, Tanzania, Togo, Tunisia, Uganda, Zambia and Zimbabwe require communication service providers to put in place mechanisms, including the installation of software, that facilitates access and interception of communications by state agencies. Moreover, state agencies in several countries can request for decryption of data held by service providers, which poses a big concern over privacy.

Laws in Namibia (Part 6 of the 2009 Communications Act), Senegal (article 90-17 of law n° 2016-33 of December 14, 2016), and in Mali (Cybercrime Act in article 77), require service providers/intermediaries to decrypt any encrypted information that they may hold in aid of lawful interception.

Further, in Cameroon, sections 49-51 of the 2010 law on Cybersecurity and Cybercrime empowers courts to order decryption of encrypted content. At the same time, section 58(1) requires encryption service providers to disclose their encoding system to criminal investigation officers or authorised officials of the National Agency for Information and Communication Technologies (ANTIC), upon request.

Similarly, in Ivory Coast, under Decree n° 214-105, competent administrative or judicial authorities can access secret codes of encrypted data upon request to the *Telecommunications Regulatory Agency of Cote d'Ivoire* (ARTCI), or order decryption of data through the help of ARTCI.[6]

Article 94 of Togo's 2012 electronic communication law likewise obliges encryption service providers to comply with lawful interception orders, with refusal to provide secret decryption codes to government agencies punishable by a fine of USD 3,544- 14,178.

In Chad, articles 19 and 36 of Law no 009/PR/2015 on Cybersecurity and Cybercrime stipulate that judicial authorities may order decryption, while article 22 requires encryption service providers to provide court or the criminal police with agreements allowing the decryption of transformed data. Benin's Digital Code (article 635) and the Code of Criminal Procedure (article 78) similarly give powers to the investigating judge or the public prosecutor to order decryption of data.

Under Zimbabwe's Interception of Communications Act, cryptography services providers must decrypt data at judicial authorities' request or provide them with codes allowing the decryption of data they have encrypted (article 78). Section 11(1)(d) permits security agents to demand that information is decrypted before it is handed to them, where the disclosure is necessary for national security, to prevent or detect a severe criminal offense, or in the interests of the country's economic well being. Failure to comply is punishable with up to five years' imprisonment, a fine not exceeding USD 373, or both.

According to *article 95* of Togo's 2012 electronic communication law, 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 provide the technical means that enable the identification of those users. The service providers are required to avail this data, on request, to the investigating judge, Prime Minister, Minister for the Economy and Finance, the Minister of Defense, the Minister of Justice, and the Minister of Security.

6 *Id., Article 16.*

In South Africa, Section 21 of the Regulation of Interception of Communication and Provision of Communication-Related Information Act (RICA) provides that an officer of the police or an authorised law enforcement officer may apply to a designated judge who may issue a decryption direction. Nigeria's Lawful Interception of Communication Regulations have similar provisions in rule 9(1), which states that where communication intercepted is encrypted, the communications service provider will be required by the regulator to provide the key, code or access to the encrypted communication.

Tunisia's Electronic Signatures Act grants police wide search powers under sections 86 and 87 including access to computerised data such as passwords, encryption or decryption codes, and any other means required to enable the comprehension of computerised data.[7]

Compelled assistance is quite worrisome as governments and their agencies usually have unfettered access to individuals' private data beyond prescribed limits. Yet governments and agencies should use compelled provider assistance to facilitate law enforcement access but only with clear rules as to where and to what extent compelled service provider assistance is applicable under the legal framework. Requests for compelled provider assistance must be targeted and limited to a particular case which expressly require such actions.[8]

Mandatory SIM Card Registration

In virtually all African countries, there is mandatory SIM card registration, during which a horde of identifying data is collected. While the surge in cyber crimes prompted SIM registration, the data requirements for registration are huge yet the data protection practices are poor with no specific data protection laws. Even in countries with data protection laws, implementation is often poor and many laws fall short of established human rights standards.

Moreover, the trends in data collection seem to be changing with several countries increasingly pegging service delivery to data which is collected and stored in various databases. Of itself, SIM registration in effect *eradicates* the ability of mobile phone users to communicate anonymously and facilitates mass surveillance, making tracking and monitoring of all users easier for law enforcement and security agencies.

Data Localisation Concerns

Data portability is a growing concern across the continent with laws prescribing that personal data should be stored locally. Where cross-border data transfers are necessary, then the country to which such data is to be transferred must have similar protection measures to those of the originating country, and in most instances under authorisation of data protection authorities. In Kenya, Malawi, Nigeria, Tunisia, Uganda, Zambia and Zimbabwe data transfers must be authorised.

However, hosting data locally could grant state surveillance apparatus in some countries in the region easier access to data for decryption and surveillance purposes with or without compelled assistance, as they would not need to go through foreign countries' or intermediaries' data management protocols to access this data.[9] Governments should *minimise data localisation requirements* for law enforcement access. The data localisation measures in various African countries appear to go against the Africa Declaration, which forbids states from adopting data localisation requirements unless they are justifiable and compatible with international human rights law and standards.

7 *Section 86 provides for search by a warrant issued by a Magistrate, while Section 87 provides for search and seizure without a warrant to a police officer, not below the rank of Inspector.*

8 *EastWest Institute, Encryption Policy in Democratic Regimes Finding Convergent Paths and Balanced Solutions*

9 *Cory Farmer and Judson L. Jeffries, How Surveillance, Collection of Biometric Data and Limitation of Encryption are Undermining Privacy Rights in Africa*

Illustrative Cases

Rwanda

In some countries, if the private communications of human rights defenders and opposition politicians fall into the hands of state agencies, the consequences can be dire. In April 2014, private WhatsApp and Skype messages that Rwandan musician Kizito Mihigo purportedly exchanged with government opponents living in exile were used as evidence in his trial for conspiring to overthrow the government.[10] In 2015 he was sentenced to 10 years in prison, although three years later he was pardoned by the president. Mihigo was re-arrested in February 2020 while allegedly trying to flee to neighbouring Burundi; he *died* in a police cell four days later. In a separate case of "inciting insurrection" against renowned Rwandan government critic Diane Rwigara, prosecutors presented audio messages they said were obtained from the defendant's phone when state agents seized it. The prosecution lost the case in 2018 due to insufficient evidence.[11] The trial of army officers Colonel Tom Byabagamba and retired Brigadier Frank Rusagara, who were convicted in 2016 and handed lengthy jail terms, also heard evidence from their private communications.[12]

Uganda

In July 2018, Uganda introduced a daily tax on access to Over-The-Top (OTT) services under which up to 50 social media sites could not be accessed before paying the tax.[13] It also ordered internet service providers to block access to several Virtual Private Networks (VPNs). This move increased the potential of the Ugandan state to spy on its citizens and further clamp down on free speech beyond enforcing tax compliance.[14] During an internet disruption in the 2021 general elections, the government warned Ugandans against using VPN, threatening that it would hunt down and arrest those who had installed VPN on their devices.[15] The use of VPN had grown popular in Uganda when the government ordered two internet shutdowns in 2016, forcing citizens to seek alternative means to stay online while protecting their identities. A list of upto 100 VPNs was issued for blockage by the telecoms regulator during the 2021 internet disruption.

Zimbabwe

In September 2011, the Zimbabwean regulator, the Postal & Telecommunications Regulatory Authority (POTRAZ), barred telecom operator Econet Wireless from introducing the Blackberry Messenger service, which provided encrypted messaging services.[16] The regulator reasoned that, in enabling users to send encrypted messages that Zimbabwean authorities could not intercept, the Blackberry service contravened the southern African country's Interception of Communications Act (2007). The act allows the state to intercept and monitor communications in the course of their transmission through a telecommunication, postal or any other related service or system in Zimbabwe. While this law does not outrightly ban the use of encryption technology, the fact that the regulator used a requirement in this legislation that stipulates that all services must have "the capability to be intercepted" to ban the Blackberry services means that the law still holds wide scope for being used to undermine encryption while enabling state surveillance. The said provision, Section 12(1)(a), states that notwithstanding any other law, a telecommunication service provider shall "provide a telecommunication service which has the capability to be intercepted."

Mauritius

Mauritius is one of the more progressive African countries. Nonetheless, in early 2021 it attempted to introduce brazenly retrogressive regulation to undermine encryption. Claiming that it was faced with a problem of fake news and fake profiles on social media platforms, the Mauritius ICT Authority (ICTA) in April 2021 initiated a public consultation about introducing a lawful interception mechanism that would decrypt and re-encrypt social media traffic. In the proposal,

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

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

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

13 *Social Media, VPNs, App stores, and YouTube indefinitely banned in Uganda*

14 *How Undermining Encryption threatens Online User Security in Africa*

15 *Government threatens to arrest VPN users*

16 *Econet BlackBerry service 'banned'; Blackberry Messenger a dream*

ICTA sought to set up a National Digital Ethics Committee (NDEC) with an enforcement unit empowered to take down and censor social media posts. To make its plan work, it proposed setting up a proxy "to segregate from all incoming and outgoing internet traffic in Mauritius, social media traffic, which will then need to be decrypted, re-encrypted and archived for inspection purposes as and when required". This meant that information of all social media users pertaining to device specifics, content type, location, among others, would be readily available to the authorities.[17] The proposals faced a huge national and international backlash[18] and appear to have been dropped.

Further, Section 12(c) of the Computer Misuse and Cybercrime Act 2003, allows investigatory authorities such as the police, for matters related to a criminal investigation or the prosecution of an offence, to get a court order for disclosure of an electronic key that enables access to or the interpretation of data.

Ethiopia

In 2014, the 2009 Anti-Terrorism Proclamation was used to arrest and detain six members of the Zone 9 bloggers - a collective of of activists regularly blogging and campaigning on human and democratic rights. The bloggers were *accused* of working with foreign organisations and rights activists by "using social media to destabilise the country" and using digital encryption to communicate, which the prosecution claimed was proof of their alleged conspiracy to commit terrorism. In 2018, prosecutors in Ethiopia dropped all charges against the last members of the collective that still faced prosecution. Some of the collective's members spent 15-18 months in incarceration. The proclamation on telecom fraud offences (proclamation no 761/2012) bans the use of encryption tools by individual users.[19] Indeed, for a long time, encryption has been branded and demonized as a tool for supporting terrorists and terroism.[20]

Recommendations

The high-handed regulation of encryption and restrictions placed on its use fundamentally undermine the enjoyment of the right to privacy and puts at risk the safety of users of digital technologies. Moreover, it shows a lack of commitment by states to regional and international human rights obligations. It is therefore imperative that:

- All laws that place undue restrictions on the use of encryption tools are repealed. In the alternative, all regressive provisions should be amended to remove the restrictions.
- While governments often require surveillance to curb crime, laws should be crafted in a manner that does not outrightly prohibit and/or criminalise the use of encryption technologies.
- States should cease blanket compelled service provider assistance and provide for clear and activity-bound assistance.
- States should enact specific data protection and privacy laws to provide for robust protection of privacy of the individual so as to prevent blanket interferences.

17 *Mauritius' Social Media Regulation Proposal Centres State-Led Censorship*

18 *Mozilla, Google Ask Mauritius Gov't To Abandon Its Plan To Intercept, Decrypt All Social Media Traffic Originating In The Country*

19 *Sarah Clarke, Mass surveillance and online censorship—the PEN International perspective*

20 *Kimberly Carlson, Ethiopia's New Cybercrime Law Allows for More Efficient and Systematic Prosecution of Online Speech, Electronic Frontier Foundation, June 9, 2016*