CIPESA

Privacy and Data Protection in the Digital Era : Challenges and Trends in Africa

December 2018

ICTs, Privacy and Data Protection in Africa

The use of Information and Communications Technology (ICT) in Africa is fast growing among individuals, enterprises and governments departments. However, there are several challenges associated with ICT use in Africa that undermine freedom of expression, free flow of information privacy and data protection.

At the end of 2017, Sub-Saharan Africa had over 444 million mobile subscribers with an equivalent penetration rate of 44%, which is still well below the global average of 66%. But with an annual growth rate of 4.4% expected between 2017 and 2020, a subscriber growth rate will be more than double the global growth rate over the same period.[1]

The mobile money industry in Africa is also growing exponentially. According to the GSMA, the mobile money industry registered 690 million accounts worldwide in 2017, and processed a billion dollars a day, generating direct revenues of over USD 2.4 billion. Of these accounts, 338 million were in Sub-Saharan Africa and processed $19.9 billion in 1.2 billion transactions in 2017.[2]

Consequently, the growth in mobile subscriptions, increased use of smartphones, enhanced collection of biometric data, and digitisation of more sectors of the economy and public services have resulted in increased collection, processing and sharing of personal data.

Unfortunately, many internet users are not aware of the implications of their use of the web and how their rights are compromised by their internet usage or how their data is automatically gathered or processed without their knowledge and sold or linked with third parties. This could be due to the absence of a direct translation or equivalent term for the word “privacy” in many African languages.

Legal Frameworks for Privacy and Data Protection

The right to privacy is enshrined in various international human rights instruments. These include the Universal Declaration of Human Rights (UDHR); International Covenant on Civil and Political Rights (ICCPR); UN Convention on the Rights of the Child (UNCRC); and the United Nations Convention on Migrant Workers (CMW). These instruments adopt the same language and definition of privacy.

Article 12 of the UDHR and Article 17 of the ICCPR provides that: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”[3]

In June 2014, African Union (AU) member states adopted the African Union Convention on Cybersecurity and Personal Data Protection (also referred to as the Malabo Convention), making it the first pan-African instrument on privacy and personal data protection.[4] Unfortunately, since its adoption in June 2014, only 10 of the AU’s 55 member states have signed the convention: Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe, and Zambia. So far, only Mauritius and Senegal have ratified it, meaning the convention is unenforceable since it requires a minimum of 15 ratifications in order to enter into force.

By the end of December 2018, only 23 African countries had enacted comprehensive personal data protection legislation, namely; Angola, Benin, Botswana, Burkina Faso, Chad, Cape Verde, Côte d’Ivoire, Equatorial Guinea, Gabon, Ghana, Lesotho, Madagascar, Mali, Mauritius, Mauritania, Morocco, Senegal, Seychelles, South Africa, Tunisia, Uganda, Zambia, and Zimbabwe.[5]

Legal Provisions Compelling Telecom Companies to Cooperate on Surveillance

Several African countries have legal provisions that require the cooperation and compliance of service providers to state information requests or surveillance assistance. This cooperation includes the requirement to install technical surveillance capability, to actively enable communications monitoring, and to hand over data when asked.

In Uganda, Section 8 of the Uganda Communications Act, 2010 requires service providers to among others, technically assist government to intercept communications by ensuring systems are technically capable of supporting lawful interceptions at all times; installing hardware and software facilities and devices to enable interception.

Ethiopia’s Proclamation 804 of 2013 Re-establishing National Intelligence and Security Service (NISS) requires all persons to cooperate with NISS by providing information. Similarly, Rwanda’s interception law provides in Article 3, that the interception of communications shall be considered lawful where it is done in the interest of national security and in accordance with this law.

Similar requirements are contained in Tanzania Prevention of Terrorism Act and Tanzania Intelligence and Security Service Act and Kenya’s Security Laws (Amendment) Act (2014), which amends the Prevention of Terrorism Act.

1 *GSMA, The Mobile economy in Sub-Saharan Africa 2018, https://bit.ly/2KgUlEJ*
2 *2017 State of the Industry Report on Mobile Money, GSMA, https://bit.ly/2KRjQcq*
3 *UDHR, http://www.un.org/en/universal-declaration-human-rights/*
4 *AUCC, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection*
5 *Deloitte, Privacy is Paramount Personal Data Protection in Africa, https://bit.ly/2IdfBrI*

Permitted Interception and Surveillance

Laws in several African countries stipulate the procedures for conducting surveillance and making information requests to intermediaries such as telecom companies. These laws apply generally to communication and information within the countries and are not limited to the nationality of the individual whose information is sought.

In Kenya, section 42 of the National Intelligence Service (NIS) Act specifies the procedures.[6] In Burundi, the procedure is provided under the Ministerial Law No 540/356 of March 17, 2016 and in Article 92 of the Law No. 1/10 of 3 April 2013 on the reform of the Code of Criminal Procedure. Ethiopia's Computer Crimes Proclamation, under Article 25(1), authorises the regulatory organ to intercept in real time or conduct surveillance on computer data, internet and other communications of persons suspected of computer crimes upon obtaining a court warrant.[7]

Section 14 of the Tanzania Intelligence and Security Services Act, 1996[8] empowers the Tanzania Intelligence & Security Service (TISS) to collect, analyse and retain information and intelligence regarding activities that may on reasonable grounds be suspected of constituting a threat to the security of the country.[9]

Under Article 126 of Rwanda's Law No. 24 of 2016 governing ICT, the Minister in charge of ICT is empowered to interrupt or cause to be interrupted, any private communication that appears detrimental to the national sovereignty. Ghana's Anti-Terrorism Act, 2008 allows a senior police officer (not below the rank of an Assistant Commissioner of Police) with the written consent of the Attorney-General (AG) and the Minister of Justice to apply to a court for an order to require the interception of communications.

Mandatory SIM Card Registration

Several African countries are increasingly adopting mandatory SIM card registration with official documentation. Typically, the data required for registration includes names, addresses, gender and national identification numbers the latter of which is reliant on additional personal information.

Ethio Telecom has a mandatory SIM card registration system where users are obliged to produce an identification card and to register their names and addresses in order to get a SIM card. Ethio Telecom uses the national Equipment Identity Registration System (EIRS), which enables it to automatically register every device that uses a SIM card on its network. In September 2018, the Communications Authority of Kenya directed mobile operators to switch off all unregistered SIM cards on their networks, following a forensic audits that showed gaps in identity verifications by subscribers during registration.[10]

In Burundi, the Ministerial Order Number 01 of 2014 requires that before a mobile phone subscriber gets a SIM card, they have to provide personal data such as names, address, birth date, passport photographs, copy of identity card or passport, and the serial number of their phone.[11] Other countries that have embarked on mandatory SIM Card registration include; Malawi, Zambia, Zimbabwe, the Democratic Republic of Congo, Nigeria, and Uganda.

State Acquisition and Deployment of Surveillance Technologies

Technology advancement and increased digitisation have reduced the logistical barriers to accessing information and grown to an unprecedented scale the means through which personal data can be acquired, stored, or processed. Across the continent, different technologies have been acquired by states, handing them the capacity to enhance their surveillance capabilities.

In Malawi, MACRA procured the Consolidated ICT Regulatory Management System (CIRMS) in 2011 to enable the regulator monitor service providers for quality of service and fair pricing.[12] In April 2017, ZICTA Zambia's regulatory body claimed that it had the capacity to disable any communication devices and read personal messages.[13] Other countries reported to have acquired surveillance technologies include Uganda, Ethiopia, and Kenya.

Conclusion

The right to privacy can only be adequately guaranteed when states adopt policy, legal, and institutional frameworks that meet international human rights standards. But despite international and regional human rights laws and instruments providing a robust and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance; practices in many countries revealed a lack of adequate national legislation and enforcement, weak procedural safeguards and ineffective oversight, which has contributed to widespread impunity for arbitrary or unlawful interference with the right to privacy

6 *Section 42 National Intelligence Service Act*
7 *Computer Crime Proclamation, Proclamation No.958/2016, https://bit.ly/2QXdCvF*
8 *Tanzania Intelligence & Security Service Act, https://bit.ly/2NDlbtn*
9 *Tanzania Intelligence & Security Services Act, https://bit.ly/2NDlbtn*
10 *Press statement on findings of the forensic audit on registration of SIM cards, https://bit.ly/2RwWkq1*
11 *http://www.arct.gov.bi/images/circulaires/circulaire2.pdf*
12 *'Spy machine' roll out in September, says Malawi regulator, https://bit.ly/2R1toWo*
13 *ZICTA claims they can read your WhatsApp Messages and Disable any Communication Device, https://bit.ly/2XBIrMq*