State of Internet Freedom in Africa 2018

# Privacy and Personal Data Protection in Tanzania:

## Challenges and Trends

**September** 2018

CIPESA

# Table of Contents

State of Internet Freedom in Africa 2018
**Privacy and Personal Data Protection in Tanzania: Challenges and Trends**

# 1 Introduction and Background

The right to privacy is enshrined in various international human rights instruments. However, with the advent of the digital era including the internet, the right to privacy is increasingly coming under threat. There has been an increase in the volume of data collected by both government and private bodies for various purposes. This increased data collection and processing raises questions especially on the safety personal data owing to the absence of appropriate safeguards to storage and processing of personal data.

Although Tanzania's Constitution guarantees the right to privacy, the country does not have a comprehensive law to regulate the collection, processing and sharing of personal data including safeguards against the possible violations of the personal data collected. The constitutional provision and other provisions within other existing laws are too general to address the vulnerability of the ongoing personal data collection programmes, and as such the protection of the vast amounts of data remains at risk.[1]

Since 2013, the only laws in place to provide for data protection were the Constitution of the United Republic of Tanzania, 1977, the Electronic and Postal Communications Act, 2010 and its Consumer Protection Regulations.[2] There are various laws which appear to protect privacy rights on one hand and infringe on the same rights on the other hand. These laws include: The Cybercrimes Act, 2015, the Electronic and Postal Communication Act, 2010, the Electronic Transactions Act, 2015 and the Tanzania Intelligence and Security Services Act, 1996. Other laws such as the Prevention of Terrorism Act, 2002 and the Criminal Procedure Act, 1985 allow for surveillance of personal communication and without sufficient safeguards against infringements on privacy rights. In addition, there are incidents in which the Government has been accused of conducting online surveillance and interception of communications through its security agencies in a manner that erodes privacy and data protection principles.

In 2010, Tanzania introduced mandatory SIM card registration which required all mobile subscribers to register their SIM cards by providing their personal information including copies of their identity cards. At the same time, the Tanzania Revenue Authority was issuing driving license containing biometric data such as fingerprints. In 2014, the government expanded its nationwide programme of issuing biometric National Identity Cards to its citizens and residents. In 2015, the Biometric Voters Registration System was introduced. A private company, GenKey, a Dutch company, working as a subcontractor for South Africa-based Lithotech Exports, implemented the system. The process commenced in early 2015 and registered 24 million eligible voters. While recognising the value of the biometric technology, it must be regulated and data collected only for specific purposes and use for a particular period.[3]

1 *THRDC, "The Report on the Right to Privacy in Tanzania" 2015.*

2 *Information from legal personnel at Tanzania Communications Regulatory Authority.*

3 *GenKey's biometric ID solutions deployed for voter registration in Tanzania, https://tinyurl.com/ww3urtt*

In 2015, Tanzania enacted the highly contentious Cybercrimes Act, 2015. The Act empowers police officers to demand the disclosure of personal information of internet users from internet service providers or online content providers such as bloggers and owners of online platforms.[4] In October 2015, shortly after the enactment of the law, the offices of the Tanzania Civil Society Consortium on Election Observation (TACCEO) which was monitoring the election process was raided by armed police officers. Three laptops, 24 desktop computers and 25 phones were confiscated. A total of 36 staff and volunteers were arrested but later released after long interrogation at the Central Police Station in the capital Dar es Salaam. They were arrested on suspicion of committing the offence of publishing false information contrary to Section 16 of the Cybercrime law and Election Act. The raid and arrests took place hours before the National Electoral Commission (NEC) announced the winner of the presidential election. The seized equipment and devices remained in police custody for nine months until their release on July 18, 2016. Further, no charges were preferred against the staff by the police, stating that investigations remained ongoing. To-date, there has not been any court proceedings in the case.

In 2018, the government passed new regulations which pose as a threat to the right to privacy and data protection. The Tanzania Communication Regulatory Authority demanded that all telecom operators start registering their subscribers by using biometric data (i.e. fingerprints).[5] While this may have been well-intentioned, the absence of proper safeguards means that all collected data is at risk of being abused. More importantly, the ever-increasing trend by the government to opt for biometric systems to identify its citizens in the absence of a comprehensive privacy and data protection law is worrying.

It is against this background that this study focused on the state of privacy and personal data protection in Tanzania It tracks key trends in the country over the past five years, analysing major risk factors, mapping notable developments on data protection and privacy legislation and violations, and identifying measures that can positively influence the right to privacy legislation in Tanzania. The study should inform key actors, including government, the media, academia, civil society on the current legal, institutional and practice landscape as well as opportunities for advancing the right to privacy and data protection.

**4** *See section 32 of the Cybercrimes Act, 2015.*

**5** *Why TCRA Opted for Biometric Plan" available at http://mobile.thecitizen.co.tz/news/Why-TCRA-has-now-opted-for-biometrics/2304482-4325534-format-xhtml-6kakmvz/index.html (accessed August 1, 2018).*

# 2 Methodology

The study was qualitative in nature and comprised literature review and key informant interviews. The researchers reviewed various reports relating to data protection, privacy and the internet ecosystem. Specifically, reports on the right to privacy from civil society organisations (CSOs) such as the Tanzania Human Rights Defender (THRDC) and the Legal and Human Rights Centre (LHRC) were reviewed. In addition, various articles on online data protection and privacy were reviewed. Furthermore, internet sources were reviewed to find information that was not readily available.

To complement the desk review, key informant interviews were conducted with select respondents. The respondents were chosen basing on their conversance with the issues informing the study. The respondents were selected from private legal practitioners in law firms, Higher Learning Institutions (e.g. Schools of Law), civil society organisations dealing with promotion and protection of human rights, telecom companies, internet service providers, and the Tanzania Communication Regulatory Authority (TCRA). Others included journalists, bloggers, online content providers and platforms such as JamiiForums and Fikra Pevu. A total of 20 respondents were interviewed.

# 3 Country context

This section provides an overview of the country context in terms of the political economy, the status of Information and Communications Technology (ICT) in the country, and the political environment.

## 3.1 Political Economy

Tanzania's population is estimated at 56.9 million. A World Bank report on the state of the Tanzania economy shows that more than 50% of Tanzanians are living below the poverty line, with income of Tanzania Shillings 1,300 ($ 0.57) per day.[6] Further, the country ranks at a low position of 151 out of 189 countries, under the UNDP Human Development Indicator ranking of 2016.[7] According to official statistics from the 2012 census, the literacy rate stands at 67.8% of the total population.[8]

## 3.2 ICT Status

According to statistics from the Tanzania Communications Regulatory Authority (TCRA), as of December 2017, there were 40.08 million mobile and fixed telephone subscribers with a penetration rate of 78%.[9] This was a slight decrease compared to 40.17 million subscribers and a penetration rate of 80% recorded at the same period in 2016. Further, there are 22.99 million internet users and a penetration rate of 45%, according to the same report.

There are seven licensed telecoms operators in the country - Airtel, Zantel, Halotel, Vodacom, Tigo, TTCL and Smart (rebranded from Benson). Vodacom has the largest number of mobile subscribers at 12,866,059, followed by Tigo (11,062,852), and Airtel (10,855,955), while Zantel, Halotel, TTCL and Smart are the small players in the segment.[10] In addition, there are up to 20 Internet Services Providers registered with the Tanzania Internet Services Providers Association (TISPA).

The price of internet data bundles, inaccessibility to telecommunication facilities and low literacy rates affect the ability of several Tanzanians to access ICT. The cost of internet services is relatively high, averaging Tshs 250 (USD 0.11) per 50 megabytes. Some of the companies charge up to TShs. 30,000 (USD 13) for a monthly 2GB internet bundle. Internet cafés charge approximately TShs 1,000 (USD 0.43) per hour. Further, a wide section of the populace does not have access to smartphones, laptops, tablets and computers.

6 *Wachumi: Ni bajeti chungu kwa makabwela, http://mTanzania.co.tz/?p=14926*

7 *UNDP, International Human Development Indicators, http://hdr.undp.org/sites/default/files/rankings.pdf*

8 *UNICEF, Tanzania Country Info, http://www.unicef.org/infobycountry/Tanzania_statistics.html*

9 *TCRA, Quarterly Statistics Report of December 2017, https://www.tcra.go.tz/index.php/quarterly-telecommunications-statistics#2017-quarterly-statistics-reports*

10 *Ibid.*

## 3.3 Political Environment

Tanzania has held regular multiparty elections since its transition from a one-party state in the early 1990s, but the opposition remains relatively weak, and the ruling party, Chama Cha Mapinduzi (CCM), has retained power for over half a century.[11] Since the election of President John Magufuli in 2015, the government has cracked down with growing severity on its critics in the political opposition, the press, and civil society.[12] The government has been implementing the restrictive Cybercrimes Act, 2015 and the Media Services Act, 2016; suspended critical newspapers such as Mawio and Mwanahalisi for two years;[13] arrested a local rapper, Ney wa Mitego over a song critical of the President;[14] prosecuted social media users for insulting the president;[15] and arrested and prosecuted the founders of JamiiForums.[16] Azory Gwanda, a journalist who reported on killings of police and CCM members in Kibiti-District has been missing for nearly a year without a trace.[17] Also, in August 2018, several police officers were caught on camera brutally beating a journalist who was under their custody at the National Stadium.[18]

In March 2018, the government introduced a new regulation[19] which requires online content creators[20] to pay application fees of TZS 100,000 (USD 43.7), initial three-year license fees of TZS 1,000,000 (USD 437) and renewal fees of a similar amount. The penalty for non-compliance is a fine of TZS 5,000,000 (USD 2,186). The regulations further require persons to furnish ownership details in order to obtain an operating licence. In May 2018, human rights activists obtained an injunction halting the application of the regulations citing them as an affront to free speech.[21] The injunction was overturned in May 2018.[22] The implementation of the regulations halted the operations of some bloggers, including popular online platform JamiiForums which ceased operations for some time in order to avoid the punitive actions under the law.[23] Tanzania subsequently published a list of 148 licensed online content services providers, who included Jamii Forums.[24]

11 *Freedom House; Freedom in the World Report 2019/Tanzania available at; https://freedomhouse.org/report/freedom-world/2019/tanzania*

12 *Ibid*

13 *Tanzanian newspaper suspended for 'insulting president', https://tinyurl.com/vft5toh*

14 *Tanzanian rapper held for 'insulting' President Magufuli in song, https://tinyurl.com/qvzcldt*

15 *Five charged with "insulting Magufuli" on social media, https://tinyurl.com/wxuxh25*

16 *Tanzanian police charge Jamii Forums founder, https://tinyurl.com/swde69g ; Tanzanian Court Acquits Jamii Forums Founders on One of Three Charges, https://tinyurl.com/rf79ldq; Freedom House, Freedom of the world, Freedom House, https://tinyurl.com/w8mccxx*

17 *Read about the incident at https://www.bbc.com/swahili/habari-42263687.*

18 *https://www.jamiiforums.com/threads/afrika-hoyee-mwanahabari-alipokezwa-kichapo-cha-mbwa-na-mapolisi-Tanzania.1466588/.*

19 *The Electronic and Postal Communications (Online Content) Regulations 2018, https://tinyurl.com/yyke73sw*

20 *The law applies to bloggers, internet cafes, online content hosts, online forums, online radio or television, social media and subscribers and users of the internet.*

21 *Reuters, Tanzania bloggers win temporary court order against state crackdown, https://tinyurl.com/ujtst5a*

22 *Tanzania government wins court case to impose online regulations, https://tinyurl.com/rfl76ph*

23 *The Great Silencing, or why I stopped blogging, https://tinyurl.com/wea92f4; Tanzania: Jamii Forum Founder Speaks Out On Decision to Close Site, https://allafrica.com/stories/201806120534.html*

24 *TCRA, Online content services licences by 31st July 2018, https://tinyurl.com/u8qchh8*

.

# 4 Laws and Policies Affecting Privacy and Personal Data Protection

This section gives an overview of the legal and policy framework on privacy and data protection in Tanzania. It also highlights the international and regional framework and its implications on privacy and data protection in the country.

## 4.1 International Framework on the Protection of Privacy

Tanzania is party to International human rights instrument that protect the right to privacy. These include the Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR), Convention on the Rights of the Child (CRC) and the African Charter on the Rights and Welfare of the Child.[25]

For instance, article 17 of the ICCPR provides unequivocally that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, nor to unlawful attacks on their honour and reputation. The United Nations Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."[26]

## 4.2 The Constitution

The Constitution of the United Republic of Tanzania provides for the right of privacy under article 16, which arguably protects data and personal information. It provides, in article 16(1), that every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications.

However, this right is not absolute and the government is required, under article 16(2), to pass the necessary legal procedures under which the enjoyment of the right may be limited, stating that, "For the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of person, his property and residence may be encroached upon without prejudice to the provisions of this Article."

Article 18(c) of Constitution also provides for the rights to freedom of expression and protection from interference stating thus: "Every person - (c) has the freedom to communicate and a freedom with protection from interference from his communication."

25 *International Instruments Ratified by Tanzania, https://tinyurl.com/t5t7rlx*

26 *General Comment No. 16 (1988), para. 1*

## 4.3 Recognition of Privacy and Personal Data Protection in Statutes

Despite the Constitutional provisions on privacy, Tanzania is yet to enact a comprehensive law on data protection. There are nonetheless some national laws with provisions on protection of the right to privacy and data protection in Tanzania. However, some laws like the Prevention of Terrorism Act, 2002, the Tanzania Intelligence and Security Services Act, 1996 and the Electronic and Postal Communication Act, 2010 have contentious provisions that potentially limit the right to privacy including by allowing surveillance and monitoring of digital communications and other online activity of citizens.

### 4.3.1 Prevention of Terrorism Act 2002

The Prevention of Terrorism Act 2002 provides for the interception of communication and admissibility as evidence of intercepted communication in courts law. Section 31 provides that "a police officer may for the purpose of obtaining evidence of the commission of an offence under this Act, apply, ex parte, to the Court, for an interception of communications order." While section 31(4) of the same Act allows the admissibility as evidence of any communications intercepted, including from outside of the country, in proceedings for any offence under the Act. The law places some degree of responsibility on the courts to determine the merits of the interception before granting an order to the officer.

### 4.3.2 Tanzania Intelligence & Security Services Act 1996

The Tanzania Intelligence & Security Services Act, 1996 mandates the Tanzania Intelligence & Security Service (TISS) with the duty to collect information through investigations or otherwise, to the extent that it is strictly necessary. Section 14 of the Act gives the TISS powers to collect, "analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting a threat to the security of the United Republic or any part of it".

Under Section 18, TISS can as well enter into arrangements with any person, local government or other authority, any police force or other policing organisations as well as government of foreign states or an international organisation of states or its institutions for purposes of performing its functions. However, this must be done with the approval of the Minister of Foreign Affairs.

In exercising such power, TISS can intercept any communication on the basis of national security under section 5(2). However, TISS is barred from instituting surveillance of any person or category of persons by reason only of their involvement in lawful protest, or dissent in respect of any matter affecting the Constitution, laws or the Government of Tanzania. This means that they can institute surveillance for other grounds such as national security.[27]

27 *See section 5(2) of the Tanzania Intelligence and Security Services Act, 1996.*

### 4.3.3 Electronic and Postal Communication Act, 2010

The Electronic and Postal Communication Act, 2010 does not expressly provide for the interception of communication. However, the existence of interception powers can be implied from section 120 of the Act, which states that "no person, without lawful authority under the Act or any other written law, can intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept any communications." In order to intercept communication, there must be an application. The application must be made under "any other law" to the Director of Public Prosecutions (DPP) for authorisation to intercept or listen to any customer communication transmitted or received. However, it is only public officers, or an officer appointed by the Tanzania Telecommunications Regulatory Authority (TCRA), who is duly authorised by the Ministry of Science & Technology, as well as the Ministry of Home Affairs, who may be permitted to intercept such communications.

Additionally, the Electronic and Postal Communications (Online Content) Regulations, 2018the new Online Content Regulations, 2018 contain provisions which compel the online content providers and users to identify the sources of their information or content. This is provided for under regulation 5(1)(e). This means that in some instances, online content providers may be ordered to disclose the identity of their source of content or information. This may jeopardise the privacy of the persons who wish to contribute or share content anonymously.

### 4.3.4 Tanzania Passport and Travel Documents Act, 2002

This Act provides for the regulation of information which should be contained in documents such as passports. This provision is under section 7 and the First Schedule to the Act which inter alia, requires that passports contain the following information: full names of the holder, nationality of the holder, sex of the holder, date and place of birth of the holder, photograph of the holder, signature of the holder, profession/occupation, height, colour eyes, special peculiarities and permanent address.

Each applicant for a passport must provide this information to the issuing authority. However, in practice, some of the information is not included in the passport, such as height, eye colours, peculiarities and profession. Unfortunately, the Act is silent on protection of the collected data.

### 4.3.5 Registration and Identification of Persons Act, 1986

This Act in section 7 makes it compulsory for any person above the age of 18 years to register for a national identity card. During registration, the person is required to disclose all the information outlined in section 9(b) of the Act. This includes: full names, business and residential address, nationality, place of birth, age and sex, marital status, profession, trade or occupation and any other particulars as may be prescribed by the Minister through the government gazette.

Under section 19, the Act prohibits the Registrar and any registration officer from disclosing photographs and fingerprints, or any immigration officer performing functions under the Act from producing for inspection, or supplying a copy of, the photograph of any person registered under this Act or his fingerprints, or disclosing or supplying a copy of the particulars furnished under section 7 or 9, except with the written permission of the Minister.

### 4.3.6 Road Traffic Act, 1973.[28]

Driving licenses are issued by the Tanzania Revenue Authority (TRA) in collaboration with the Police. The Act is silent on the kind of information which an applicant is required to provide. However, since the license the issued together with the Taxpayer Identification Number (TIN), TRA has been collecting information such as full names, date and place of birth, business and residential address, occupation, business and fingerprints.[29]

28 *Road Traffic Act, https://moj.gov.jm/sites/default/files/laws/Road%20Traffic%20Act_1.pdf*

29 *Information obtained through interview with Human Rights Lawyer at Victory Attorneys & Consultants.*

# 5 Results: Status, Trends and Challenges

This chapter details the emerging trends and key challenges to privacy and personal data protection in Tanzania, citing various examples and incidents.

## 5.1 Limited Understanding of Privacy

Privacy and data protection are quite new concepts to many Tanzanians. This is largely attributed to the low level of ICT literacy.[30] Majority of internet users do not know or understand the risks they face when they post their information online.[31] They do not fear that the information shared in various online platforms may be used without their consent.[32]

In addition, few persons seem to understand the implications of unregulated collection and processing of their personal data through the on-going registration for National Identification cards, SIM card registration and processing of drivers' licences. The is a low level of awareness of the laws and citizens' right to privacy, hence most cannot question the nature and scope of personal data collected from them.[33]

## 5.2 Fragmented Oversight Over Privacy and Data Protection

Despite the on-going data collection programs in the country, Tanzania has no specific body mandated to regulate privacy and data protection. The mandate is scattered among different agencies. For example, TCRA has been regulating the communication sector to ensure that subscriber data is protected. TCRA enforces the Electronic and Postal Communication (Consumer Protection) Regulations, 2011 which aim to protect consumer information. Rule 6 (2) (e) of the Regulations prohibits a licensee or operators who have collected information from improper or accidental disclosure. As the sector regulator, TCRA has been keen on ensuring that privacy and data of consumers in the sector are protected.

Additionally, the collection of personal data in Tanzania is not only limited to the communication sector. Mobile operators and banks have been collecting information from their customers for the purpose of registration for both

30 *In 2015, it was reported that the illiteracy rate in Tanzania had gone up to 78%from 77%in 2012, available at https://allafrica.com/stories/201609080940.html*

31 *Information supplied by the mobile-telecom operators who opted to remain anonymous.*

32 *Information obtained through interview with various respondents.*

33 *Ibid.*

the traditional banking services and the modern digital transactions such as the use of mobile apps to enable individuals open banks accounts and effect transaction remotely.[34]

Therefore, in the absence of a comprehensive data protection law and an oversight body, risks of customers' information being misused or leaked to third parties are significant.[35]

## 5.3 Weak Policy and Legal Frameworks

This section presents an analysis of the weaknesses of the existing policy and legal frameworks in Tanzania.

### 5.3.1 Absence of Comprehensive Data Protection Frameworks

Currently Tanzania lacks a comprehensive privacy and data protection law. However, there is a draft bill that has been in development since 2014 by the Ministry of Communications, Science and Technology as part of its cyber security initiative. However, the constitution does not provide a clear definition of what amounts to personal data. This limits the scope within which personal data is recognised.

Further, there are no regulations to provide for legal procedures, manner and circumstances under which data can be disclosed by third parties, including law enforcement agencies. Without these legal protections and procedural safeguards, the government has few restrictions on how to handle personal data collected through data processing initiatives such as the SIM card registration and the National ID registration.[36]

### 5.3.2 Use of Restrictive Laws to Undermine Privacy

In Tanzania, security agencies have on several instances demanded access to identifying details of individuals who have posted content online. Section 32 of the Cybercrimes Act, 2015 authorises the police to compel the disclosure of data for purposes of criminal investigations. This provision has been abused by police officers to infringe privacy rights. For instance, JamiiForums was in January and February 2016 issued with several letters compelling it to disclose the Internet Protocol (IP) addresses of its anonymous users or other information that would help the police to identify them.[37] When Jamii declined, its founders were arrested and charged with the offence of obstructing investigations.[38] The individuals whose information was sought had allegedly posted information on the forum about political tensions among members of the ruling party, Chama Cha Mapinduzi, and scandals in one of the country's leading banks. In addition, Jamii's founders were charged with the equally controversial offence of management of a domain not registered in Tanzania under Section 79(c) of the Electronic and Postal Communications Act (2010).[39]

34 *Ecobank and CRDB have these apps. The CRDB uses USSD codes also to allow simple opening of the bank account.*

35 *Information obtained through interview with TCRA personnel.*

36 *Right to Privacy in Tanzania; Stakeholder Report Universal Periodic Review, https://cipesa.org/?wpfb_dl=212*

37 *Tanzania Court Deals a Blow to Intermediary Liability Rules, https://www.opennetafrica.org/tanzania-court-deals-a-blow-to-intermediary-liability-rules/*

38 *BBC, Tanzania Police Charges Jamii Forums Founder, https://www.bbc.com/news/world-africa-38341151*

39 *Maxence Melo Charged with Obstruction of Investigations and Operating a Domain Not Registered in Tanzania, https://bit.ly/2OP8wA1*

Tanzania's Cybercrimes Act, which made three years in September 2018, has been used extensively to rein in voices critical of president Magufuli's government, as well as voices critical of powerful business interests. More than 15 social media users have been arrested under the Act, with many charged in court just like the JamiiForums founders.[40]

Meanwhile, there is an emerging trend in Tanzania, whereby law enforcement agencies seize phones and personal computers from individuals and hold them for several days on the pretext that they are conducting investigations. In April 2018, police briefly detained two popular musicians, Nasibu Abdul Juma (whose stage name is Diamond Platnumz) and Faustina Charles (popularly known as Nandy), after they each posted video clips on Instagram and WhatsApp respectively, which authorities deemed obscene.[41] They were released on bail without charge after questioning and two mobile phones were confiscated as part of the investigation. If charged, the two face fines of at least five million shillings (USD 2,200), a minimum prison sentence of 12 months, or both.

In November 2017, the leader of the opposition Alliance for Change and Transparency, Zitto Kabwe's phones were confiscated by police following his arrest and detention in October the same year. The politician was under investigation for uttering a seditious statement against the government, hence was held to be in violation of the Cybercrimes Act and Statistics Act.[42] In July 2018, the Home Affairs Minister had called for his arrest for incitement.

Earlier, during the October 2015 election period, police detained 40 volunteers of Tanzania's opposition party Chadema, and confiscated computers and phones they were using to tally election results.[43] The party termed the arrest a government bid to intimidate the opposition. Similarly, in October 2015, human rights defender Imelda Urio and 35 other members of the Tanzanian Civil Society Election Consortium (TACCEO) were arrested and detained over their election observation activities, which authorities said contravened section 16 of the Cybercrimes Act, which prohibits publication of false information.[44] The police confiscated the group's computers, office phones and mobile phones for nine months. No charges were preferred against the group.

### 5.3.3 Legal Provisions Compelling Telecom Companies to Cooperate on Surveillance

There are several provisions in various legislation that require disclosure of information and surveillance. These include the Cybercrimes Act, 2015, the Criminal Procedure Act, 1985, and the Electronic and Postal Communication Act, 2010. These laws may be used to compel the disclosure of information, including personal data held by third parties.

Regulation 5(1)(e) of the Electronic and Postal Communications (Online Contents) Regulations, 2018 requires content providers to have mechanisms in place in order to identify the source of their information or content. This may

40 *Five Tanzanians charged with insulting the president, https://bit.ly/2xRJzg7*

41 *Popular Tanzanian singer arrested in latest internet crackdown, https://reut.rs/2xlEvkP*

42 *Police confiscate Zitto's mobile phone, raid ACT-Wazalendo offices, https://bit.ly/2Q6CRKI*

43 *Tanzanian opposition says 40 volunteers arrested after election, https://bit.ly/2NKi03n*

44 *Tanzania: Ongoing police harassment against Imelda Urio and 35 other human rights defenders, https://tinyurl.com/w7ufbvo*

jeopardise the privacy of the persons who wish to contribute or share content anonymously. Regulation 11(1) provides that personal information obtained by the communications regulatory authority in exercise of its powers or duties under the regulations can only be disclosed if required by any law enforcement agency, court of law or other lawfully constituted tribunal. The regulations do not provide the procedure for making such requests.

Furthermore, under Section 121 of the Act, "It shall be lawful under this Act for an officer, employee or agent of any network facilities provider, network service provider, application service provider or content service provider whose facilities or services are used in communications, to intercept, disclose, or use those communications in the normal course of his employment while engaged in any activity which is a necessary incident to the performance of his facilities or services or to the protection of the rights or property of the provider of the facilities or services, but the provider shall not utilise the facilities or services for observing or random monitoring".

Whereas section 39 of the Cybercrime Act mandates the Minister to prescribe procedures for service providers to avail competent authorities with some information, the procedures have not been developed. As a result, law enforcement agencies may interpret the law partially or to the best of their interests or to the interests of some people such as tycoons.[45] Through these laws, law enforcement agencies may approach and compel any person who holds certain information to disclose that information in the pretext of conducting investigations. Unfortunately, what is worrying is the fact that these laws do not provide adequate safeguards on data processing and use by third parties. In addition, there are also fears over increased surveillance of social media platforms by law enforcement agencies.[46]

### 5.3.4 Unreasonable Search and Seizure Practices

Although the cybercrimes law requires law enforcement agencies to follow the prescribed procedures prior to obtaining information, there have been some instances where law enforcement agencies have been forcing persons to provide personal data without following the established procedures. In 2016, the police demanded Jamii Forums to disclose information and IP addresses of their users. When directors of the Jamii Media refused, the police threatened to prosecute them. The police eventually charged Maxence Mello, Director of Jamii Forums, with obstructing an investigation following refusal to hand over details of people who had posted on their site.[47]

More recently, there has been an increasing trend of law enforcement agencies seizing phones and personal computers from individuals for days in the pretext of conducting investigations. In November 2017, Zitto Kabwe, an opposition leader's phones were confiscated by the Police to allegedly help in ongoing investigation.[48] It is not clear what kind of information the police were looking for in the phones. However, it was later revealed that he had been accused of uttering seditious statements against the government contrary to the Cybercrime Act and Statistics Act.

45 *Interview with Jamii Media.*

46 *Jamii Media Limited v. Attorney General Miscellaneous Application No.9 of 2016, High Court of Tanzania at Dar es Salaam.*

47 *Tanzanian police charge Jamii Forums founder, https://www.bbc.com/news/world-africa-38341151*

48 *Police confiscate Zitto's mobile phone, raid ACT-Wazalendo offices, https://tinyurl.com/s8emaw4*

## 5.4 Data Collection Programmes by Governments

### 5.4.1 Mandatory Data Collection

In 2014, Tanzania expanded its nationwide programme of issuing National Identity Cards to its citizens and residents through a biometric system. In 2015, the country introduced a Biometric Voter Registration System with a private Dutch company, GenKey, working as a subcontractor for South Africa-based Lithotech Exports, contracted to implement the system through which 24 million eligible voters were registered.[49] The Tanzania Revenue Authority also collects biometric data prior to the issuance of driving licenses. The country has no law in place to provide safeguards against possible violations even as personal data continues to be collected en masse.

In March 2018, TRCA, in collaboration with the National Identification Authority, commenced a 30-day pilot project for biometric registration of customers of all telecommunication service providers.[50] According to TCRA, the provision of fingerprints would establish proof of identity, seal existing loopholes, and prevent criminal activities such as fraud, verbal abuse and threats, and collect correct subscription statistics from the telecom sector. Operators Tigo and Zantel hailed the initiative as necessary to discourage misuse of mobile phones, abusive language, fraud, and said it would reduce customer complaints. As of December 2017, TCRA had collected information from 40,080,594 persons through the SIM card registration process.[51]

### 5.4.2 Scaling up Digitisation Programmes

In recent years, there has been an increase in collection of data by government bodies using digital and biometric systems for various purposes. For instance, since 2015, the Government through the National Electoral Commission has been registering voters through a biometric voter registration system and collected vast information regarding voters. Also, the National Identification Authority (NIDA) has been collecting biometric data for the purpose of issuing National IDs since 2012.[52] The TRA has also been collecting biometric information in order to issue driving licenses and TIN numbers.

Recently, TRCA instructed mobile operators to start registering their subscribers by using biometrics such as fingerprints. The Electronic and Postal Communication Act, 2010 (EPOCA) requires the registration of SIM card owners. Section 93 of the Act provides that "Every person who owns or intends to use detachable SIM card or built-in SIM card mobile telephone shall be obliged to register SIM card or built in SIM card mobile telephone". Subsections (2) and (3) outline the information that must be registered for natural and legal persons respectively. Failure on the part of the operator to register a subscriber and a user's use of an unregistered SIM card equally qualifies them for fines and imprisonment upon conviction.

49 *THRDC." Report on the Right to Privacy in Tanzania", 2015. pg 8.*

50 *Why TCRA opted for biometric plan, https://bit.ly/2zsmVND*

51 *TCRA Quarterly Statistics Report of December 2017.*

52 *Information obtained through interview with legal consultant at Victory Attorneys.*

Further, the Act mandates the Communication Regulatory Authority to maintain a database of all subscribers' information. Service providers are required under section 91 to submit all subscriber information to the TCRA every month. It has been argued that mandatory SIM card registration eradicates the potential for anonymity of communications, enables location-tracking and simplifying communications surveillance and interception and thereby interferes with the right to privacy. [53]

Maintenance of the data base is an ongoing process and applies to both new and already registered subscribers. Mobile operators have been sending short messages to their subscribers requiring them to visit their offices to complete registration. More recently, telecom operators such as Vodacom, Tigo and Airtel have started using biometric data in verifying or identifying their customers under instruction of TCRA. What is worrying, however, is that there is no known mechanism in place to guarantee the safety of the biometric data captured.

Unfortunately, in the implementation of these programmes data protection is not provided for. This subjects personal data to unlawful practices in storage and processing. As such, personal data can be used as a tool for surveillance, enable profiling, and may be subjected to further analysis through data mining techniques thus creating a significant privacy vulnerability.[54]

## 5.5 Enhanced State Surveillance Capacity

### 5.5.1 Permitted Interception and Surveillance

Section 31 of Tanzania's Prevention of Terrorism Act provides that "a police officer may for the purpose of obtaining evidence of the commission of an offence under this Act, apply, ex parte, to the Court, for an interception of communications order."[55] Section 14 of the Tanzania Intelligence and Security Services Act, 1996[56] 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.[57] However, section 5(2) of this law bars TISS from instituting surveillance of any person or category of persons by reason only of their involvement in lawful protest, or dissent in respect of any matter affecting the constitution, the laws or the Government of Tanzania."[58] Similarly, Section 120 of Tanzania's Electronic and Postal Communication Act, 2010 prohibits the interception of any communication, disclosure of content of communication, or use of the content of intercepted communications without lawful authority.[59] It provides a penalty of five million Tanzanian shillings (USD 2,191) or to imprisonment for a term not less than 12 months, or both.

53 *Privacy International, 101: SIM Card Registration, https://tinyurl.com/w6cboxy*

54 *ibid.*

55 *Prevention of Terrorism Act, https://bit.ly/2Dsgdul*

56 *Tanzania Intelligence & Security Service Act, https://bit.ly/2NDlbtn*

57 *Tanzania Intelligence & Security Services Act,https://tinyurl.com/wzmjgzp*

58 *See section 5(2) of the Tanzania Intelligence and Security Services Act, 1996.*

59 *Text of the Act, https://tinyurl.com/ucmnxhe*

### 5.5.2 State Acquisition and Deployment of Surveillance Technologies

There are emerging technologies that are a threat to privacy and yet reported to have been adopted by the government. In July 2015, WikiLeaks released emails from the Italian surveillance malware vendor Hacking Team, revealing an exchange between a representative from the Tanzanian President's Office and Hacking Team. An email from the government representative expressed interest in visiting Hacking Team's office with the view to purchase its Galileo surveillance system. This surveillance technology has the ability to bypass encryption, take control of a user's device and monitor all activities conducted on the device.[60] There is no official information regarding the deployment of the system.

## 5.6 Privacy Breaches by Business Entities

Generally, recourse and remedies for violation of the constitutional right to privacy are available from courts which can offer various reliefs, including declarations, judicial review, injunctions, or even awards of compensation to aggrieved parties. Some of these courses of action are contained either in the constitution or acts of parliament.

### 5.6.1 Legal Responsibility of Business Entities

Despite the lack of a comprehensive data protection law, the country has several polices whose provisions offer safeguards to clients' personal data and communication by requiring telecom service providers and other agencies collecting personal data to ensure the safety of such information.

Tanzania's Electronic and Postal Communication Act, 2010 protects customers' data from unwanted disclosure.[61] In addition, the Electronic and Postal Communications (Consumer Protection) Regulations, 2018 require the protection of information collected by mobile operators, such as SIM card registration information, against improper or accidental disclosure.[62] The provision thus restricts disclosure to third parties.

Moreover, section 8(1) of the Cybercrimes Act, 2015 makes it a punishable offence to "obtain computer data protected against unauthorised access without permission". It also states that "without prejudice to the National Security Act, a person shall not obtain computer data protected against unauthorised access without permission". Whereas this provision protects personal data, it allows access for national security reasons.

### 5.6.2 Targeted and Indiscriminate Communication

In the past two years mobile operators used to send bulk messages to their subscribers before TCRA issued a warning against the practice. Whereas this practice has decreased,[63] action needs to be taken to stem mobile phone fraud. Mobile operators used to facilitate the sending of Geo Poll SMS to their subscribers persuading them to participate in

60 *Ibid.*

61 *See regulation 6(2) (e) of the Electronic and Postal Communication (Consumer Protection) Regulations, 2018.*

62 *See Regulation 6(2) (e) of the said Regulations.*

63 *Information obtained through interviews with different respondents*

surveys in exchange for free air time. In some of these surveys, persons may be required to disclose personal information such as age and family economic status. It is not clear how such clients' personal information was managed, protected and used.[64]

There have also been reports of increased mobile money fraud in the country. The manner of execution of fraud includes sending short messages to selected numbers, providing numbers purported to belong to mobile money agents and requesting their targets to send money upon citing fake yet convincing reasons. Other fraudsters send messages pretending to be traditional healers.[65] The magnitude of these incidents raises questions as to the safety or privacy of the personal data such as mobile numbers of the mobile subscribers. It further raises questions as to the means by which fraudsters obtain numbers of their targets, including their personal details such as names.[66]

## 5.7 Dispute Resolution and Remedies

Like other actors in society, business enterprises should respect individuals' privacy and other human rights. Many private enterprises play a key role in the design, development, and dissemination of technologies; provision of communications; and some of them facilitate state surveillance activities. In the digital economy, there is increased concern about business models that threaten privacy rights. The integration of platforms and services, data sharing between organisations, cross-border data flows, business models reliant on data, data analytics, can all be a threat to the privacy and personal data, if not well managed.

### 5.7.1 Existing Frameworks for Remedies

Tanzania's Electronic and Postal Communications (Online Content) Regulations provide for a complaints procedure. Rule 16 requires aggrieved persons to file complaints to the online content providers on prohibited content. The content providers are required to resolve the complaints filed within 12 hours, and if they fail, the aggrieved person may refer the complaint to TCRA. The TCRA shall then handle the complaint through the Content Committee procedures.

### 5.7.2 Notable Judicial Decisions

There haven't been many cases on privacy in the country. However, in the case of Jamii Media Ltd v. Attorney General,[67] the Court ordered that the Government puts in place procedures to be used by the Police when requesting for information under the Cybercrimes Act, 2015 instead of relying on the general provisions which may be used to infringe the right to privacy. The court ruled that under section 32 (4)[68] of the Cyber Crime Act, police were not allowed to take items but rather to take the evidence needed by way of a printed form. The court emphasised the importance of police seeking the court's intervention in circumstances where the police failed to secure data or information under the provision.

64 *Ibid.*

65 *Alfred Zacharia, Caution as the Mobile Money Theft Rises, https://tinyurl.com/vsl47ah*

66 *Mobile phone operators warned against unsolicited text messages, https://tinyurl.com/rehwjbu*

67 *Miscellaneous Application No.9 of 2016, High Court of Tanzania at Dar es Salaam.*

68 *Section 32(4) states that; Where any material to which an investigation relates consists of data stored in a computer system or device, the request shall be deemed to require the person to produce or give access to it in a form in which it is legible and can be taken away.*

# 6 Conclusion and Recommendations

## 6.1 Conclusion

Tanzania lacks a specific data protection law, a fact that puts the right to privacy in jeopardy. However, there are safeguards in the constitution and some laws which can be used to protect data and privacy although within legal limitations. Within the country there are three main risk factors on privacy and data protection. These are: the lack of specific data protection law; laws which compel the disclosure of information without proper safeguards; and lastly, the increasing surveillance by the law enforcement agencies, which threatens the safety of the information of online users and activists.

In the past five years, the country has embarked on projects and developed laws which threaten data protection and privacy. These include introduction of compulsory registration of SIM cards in 2013; the collection of biometric information for issuance of national IDs in 2015; and the registration of voters in 2015. The Cybercrimes Act, 2015 is a draconian piece of legislation that has been used repeatedly to violate citizens' privacy and other digital rights. More recently in 2018, the government issued online content regulations which jeopardize the right to privacy, as well as citizens right to freedom of expression.

## 6.2 Recommendations

**The government** should:

- Expedite the process of enacting a privacy and data protection law that will regulate the collection, storage and processing of personal data.
- Consider amending provisions of the existing laws and policies that infringe on people's right to privacy and data protection and ensure that they conform to international human rights laws and standards on the right to privacy.
- Facilitate inclusive public discussions on the right to privacy and its implications and establish appropriate measures that protect individuals' data, including biometric data.
- Ensure that all activities of interception are only carried out on the basis of judicial authorisation.
  Establish publicly accessible legal frameworks governing intelligence sharing, and further, grant oversight bodies more powers to ensure that intelligence sharing arrangements comply with international and domestic law.[69]
- Provide a framework to govern how individuals can find out which companies hold what kinds of data about them. Profiling generates highly sensitive inferences and predictions about people's personality, behaviour or beliefs. Individuals should be able to access these inferences and predictions about them, in order to effectively challenge them, or to ask for profiles to be deleted.[70]

69 *Privacy International, Communications Surveillance, https://tinyurl.com/sbsv3c5*

70 *ibid*

**Privacy Companies/businesses** should;

- Be transparent about the information requests they receive from government and how they handle personal data.
- Take responsibility to protect human rights throughout their operations in accordance with the United Nations Guiding Principles on Business and Human Rights, including the right to privacy in the digital age. This responsibility should be independent of whether a State meets its own human rights obligations and should extend to their supply chain e.g. third party suppliers, sub-contractors or vendors.[71]
- Take all necessary and lawful measures to ensure that they do not cause, contribute to or become complicit in human rights abuses. This includes commitment to push back on illegal information requests, resisting being compelled or encouraged to sell, build or integrate surveillance capabilities into their systems and to not abuse users' data for commercial gain.
- Provide redress mechanisms and support for all their customers and users to help them protect their privacy, manage and control the use of their personal data;
- Protect the security of personal data in their custody, including through the enhancing security measures and the conduct of privacy risk audits.
- Develop internal principles and policies on privacy and data collection in accordance with local constitutional and international human rights standards and inform users of their privacy rights before commencing collection of data or use of their services

**The technical community** should;

- Develop or strengthen the avenues through which privacy breaches can be reported.
- Develop technology with privacy principles integrated as part of the general design and applied as the default settings. A useful step is the adoption of the seven principles of the concept of 'privacy by design' to serve as a foundation for privacy and data protection.
- Increase their involvement in processes that seek to influence the development and implementation of data protection laws.
- Offer useful solutions to lawmakers who are often not well-versed with the technicalities surrounding the implementation and impact of technologies on human rights.

70 *See: https://www.business-humanrights.org/en/un-guiding-principles*

**Civil Society** should:

- Advocate for the enactment of a data protection law as well as amendment of the existing laws to strengthen the protection of data and ensure privacy.
- Continue to litigate against infringement of the right to privacy and seek progressive judicial interpretations through strategic impact litigation.
- Conduct studies and research to identify gaps in the management of personal data by private and public bodies.
- Undertake awareness raising campaigns amongst the public.

**The media** should:

- Create more awareness and civic education on the importance of the right to privacy while highlighting issues concerning the right, including through the provision of information in the public interest through news stories to erode the state culture of secrecy.
- Continue to expose and investigate breaches of data protection and privacy by custodians of data.

**Academia** should;

- Support civil society to lobby Governments for the development of data protection and privacy policies and enforcement of those policies through provision of sound, evidence-based research.
- Provide intellectual leadership and guidance in society through research and outreach, and highlight concerns on the right to privacy to key stakeholders, including policy makers.


Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 6 Semawata Place, Ntinda, P.O Box 4365 Kampala, Uganda.
Tel: +256 414 289 502| Mobile: +256 790 860 084, +256 712 204 335
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org