

State of Internet Freedom in Tanzania 2019

Mapping Trends in Government Internet Controls, 1999-2019

January 2020

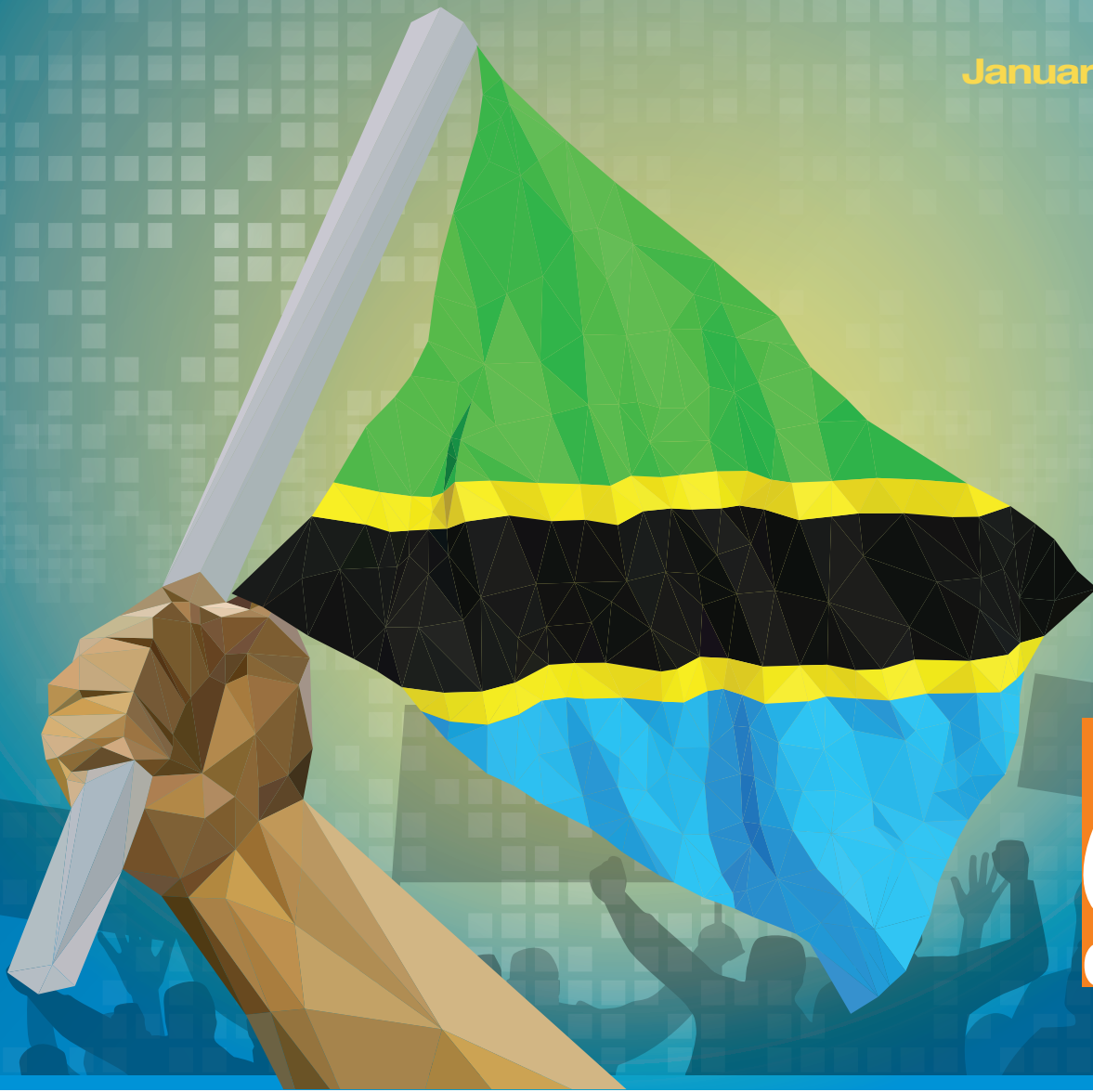


Table of Contents

1

Introduction

4

1.1 Introduction

4

1.2 Aim of the Study

5

2

Methodology

6

3

Country Context

7

3.1 ICT Status

7

3.2 Political Environment

8

3.3 Economic Status

4

Results

9

4.1 Key Trends of Internet Control Over the Last Two Decades

9

.1 Weaponising the Law to Legitimise Actions

9

.2 The Push Towards Determining Identity Amidst Poor Oversight

12

.3 Enter The Era of Social Media and Data Taxation

13

4.2 Key Positive Developments

13

.1 Robust Advocacy and Push-back by Non-State Actors

13

.2 Repeal of Repressive Legislation

14

5

Conclusion and Recommendations

15

5.1 Conclusion

15

5.2 Recommendations

16

Credits

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) with support of various partners.

This research documents the trends in government internet controls, 1999-2019 in Tanzania tracking key trends in recent years, analysing the key risk factors, and mapping notable developments on data protection and privacy legislation and violations, and users' understanding of protecting their privacy online. Other country reports for Botswana, Burundi, Cameroon, Chad, the DRC, Ethiopia, Kenya, Malawi, Nigeria, Rwanda, Senegal, Uganda, and Zimbabwe. The research was conducted as part of CIPESA's OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes internet freedom in Africa.

CIPESA recognises Asha Abinallah as the main content contributors to this report.

The research was conducted with support from Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and the Federal Ministry for Economic Cooperation and Development (BMZ).

Editors

Ashnah Kalemera, Victor Kapiyo, Paul Kimumwe, Lillian Nalwoga, Juliet Nanfuka, Edrine Wanyama, Wairagala Wakabi, PhD

State of Internet Freedom in Tanzania 2019

Published by CIPESA,

www.cipesa.org

January 2020



Creative Commons Attribution 4.0 Licence
<creativecommons.org/licenses/by-nc-nd/4.0/>
Some rights reserved.

1

Introduction

1.1 Introduction

Since 2000, Tanzania has seen tremendous growth in internet connectivity that has enabled some citizens' online participation and aided the realisation of some rights and freedoms, such as the right to information and freedom of expression.¹ The Tanzania Communication Regulatory Authority (TCRA) reports that the country had 23.14 million internet users by the end of June 2019, with a penetration rate of 45%, and 43.67 million mobile phone subscribers.²

Although the internet offers opportunities to demand for human rights and good governance, it also offers the possibility for state and non-state actors to curtail citizens' rights through censorship, surveillance and interception of communications. Indeed, while the Tanzania government has been making efforts to extend internet access to rural and urban areas, it has also enacted and leveraged laws and policies that undermine internet freedom. These include the Cybercrime Act 2015, Statistical Act 2015, Access to information Act, 2016, Media Service Acts 2016, and the Electronic and Postal Communications Act (EPOCA) 2010.

These laws have been used severally to clamp down on internet freedom over the past two decades. For example, section 16 of the Cybercrime Act, 2015, which prohibits the publication of false information, has been used to charge some critical voices in Tanzania, including for allegedly "insulting" President John Pombe Magufuli on social media. Tanzania has also continued to demand cooperation from private sector actors to facilitate easy interception of communications. The government regularly makes information requests to telecommunication companies (telcos) and Internet Service Providers (ISPs) to enable the identification of users of telecom services and the monitoring of their communications.³

In February 2019, President John Pombe Magufuli ordered the creation of a task force to speed up the construction of the National Information Communication Technology Broadband Backbone (NICTBB) whose construction kicked off in 2010. The NICTBB seeks to fulfil the increasing demands of information services, strengthen competitive abilities of domestic data and voice operators and bridge the digital divide in Tanzania.^{4, 5}

¹ *Safeguarding Civil Society, Assessing Internet Freedom and Digital Resilience of Civil Society in East Africa*, <https://smallmedia.org.uk/work/safeguarding-civil-society-east-africa>

² *Tanzania mobile phone subscriptions rise to nearly 44 million* <https://www.reuters.com/article/tanzania-telecoms/tanzanias-mobile-phone-subscriptions-rise-to-nearly-44-million-idUSL3N26G26H>

³ *CIPESA, State of Internet Freedom in Africa 2017*, https://cipesa.org/?wpfb_dl=254

⁴ *About the NICTBB*, <http://www.nictbb.co.tz/about.php?in=nictbb>

⁵ *Tanzania's Cybercrime Act Makes It Dangerous to "Insult" the President on Facebook*, <https://tinyurl.com/s8pzdjv>; *Tanzania is threatening more citizens with jail for insulting the president on social media*, <https://tinyurl.com/y8n4qq36>

Given the ongoing development around digital rights and online freedoms, it is important to situate the on-going discussions around digital and internet rights by providing an in-depth analysis of how the government in Tanzania through policies, laws and practices has shaped digital rights over the last 20 years.

1.2 Aim of the Study

This study examines how the different control measures implemented by the Tanzanian government have shaped, affected and undermined digital rights. The study covers the period from 1999 to 2019. The study focuses on the proliferation of retrogressive or repressive policies and laws; surveillance and surveillance capacity of the government; digitisation programmes; censorship; and the new frontiers like the introduction of internet-related taxes. The study also identifies and recommends measures that different stakeholders – government departments, civil society, technology companies, academia, media, and researchers - can take to secure internet freedom in Tanzania.

2

Methodology

The study employed a qualitative approach including literature review, policy and legal analysis, and key informant interviews. Reports of previous studies, media reports, academic works, government documents, and other literature, were reviewed. The literature review generated an understanding of the developments in the country.

The legal and policy analysis included a review of relevant laws, policies and practices. Such laws and policies include those that govern the telecoms sector, the media, social media use, access to information, interception of communications, security and intelligence agencies, and security enforcement in general.

Key informant interviews were conducted with purposely selected respondents. These included staff of telecom companies and ISPs, government institutions, media houses, social media users, human rights defenders and activists, academics, and lawyers. The interviews were conducted through phone calls and one-on-one interviews.

3

Country Context

3.1 ICT Status

The telecommunications industry in Tanzania is regulated by the Tanzania Communications Regulatory Authority (TCRA), a body set up by the Tanzania Communications Regulatory Act (2003). Although the internet has been available in Tanzania since the late 1990s, only two percent of Tanzanian households had a computer with an internet connection in 2005.⁶ According to statistics from the industry regulator TCRA, there were 43.92 million mobile and fixed telephone subscribers as of March 2019, while the number of internet users had increased from 19.9 million internet in 2016 to 23.14 million in 2019, representing a penetration rate of 45%.

The telecoms market in Tanzania has seven mobile operators, namely Tigo (with a 28% market share), TTCL (2%), Zantel (3%), Airtel (26%), Halotel (9%), Vodacom (32%) and Smart (0.3%). According to the Tanzania Internet Service Providers Association (TISPA), there are 29 registered ISPs. However, high data costs remain a hindrance to internet use. For example, on Halotel, a 1.5 GB per month bundle costs USD 5 while one of 25 GB costs USD 25.

3.2 Political Environment

Tanzania's ruling party Chama Cha Mapinduzi (CCM) continues to dominate the political scene, as it has won all presidential elections conducted since 1995 after the introduction of a multiparty system. However, Tanzania's transition to a true multiparty democracy has been frustrated by institutional weaknesses, weak party structures and processes, and dwindling tolerance to multi-party politics.⁷ In October 2015, President Magufuli came to power in what some observers considered "the most fierce" election the ruling party had faced after 54 years in power.⁸ His government has been criticised for routinely intimidating, harassing and attacking human rights defenders (HRDs), journalists, bloggers, and opposition members and their supporters. According to various human rights organisations, since 2015, Tanzania has implemented recently-enacted draconian legislation and applied legal and extra-judicial methods to harass HRDs, silence independent journalism and blogging, and restrict freedoms of expression, peaceful assembly, and association.⁹

⁶ http://ictexport.govmu.org/English/Documents/Market%20Intelligence/Africa_IO/Tanzania/ICT%20in%20Tanzania%20-%20recent.pdf

⁷ State of Politics in Tanzania, https://www.kas.de/c/document_library/get_file?uuid=5255a2d1-92dd-75e9-92ce-0bc85a47f08c&groupId=252038

⁸ Tanzania poll: John Magufuli of CCM defeats Edward Lowassa, <https://www.bbc.com/news/world-africa-34669468>

⁹ DefendDefenders, HRC39: Address crackdown on civic space in Tanzania, <https://defenddefenders.org/hrc39-address-crackdown-on-civic-space-in-tanzania/>

In order to stem the declining public support ahead of the 2020 elections, the crackdown on human rights, political dissent, criticism and opposition seems to have gone a notch higher. There have also been suspicious defections of opposition leaders to CCM, with those crossing-over including Magufuli's main challenger in the 2015 election, Edward Lowassa.¹⁰ There were also reports that 13 leaders from the opposition party Chama cha Demokrasia na Maendeleo (CHADEMA) in Hai District had defected to CCM after claiming that they were satisfied by Magufuli's performance yet conflicts in the main opposition party had hindered development in their home regions.¹¹ Analysts said the timing of Lowassa's defection pointed to Magufuli's quest to galvanise his support base ahead of the 2020 poll when he will be seeking re-election for a second and final term.¹²

3.3 Economic Status

Since the early 2000s, Tanzania has seen remarkable economic growth and strong resilience to external shocks. Until 2007, the poverty rate in Tanzania remained stagnant at around 34% despite a robust growth in the Gross Domestic Product of approximately 7% annually.¹³ Over the past few years, the National Strategy for Growth and Reduction of Poverty (MKUKUTA) has given high priority as the blueprint to eradicate extreme poverty and promote broad-based growth.¹⁴

Key economic development challenges include slow progress towards inclusive growth, infrastructure bottlenecks, and vulnerability to climate change. Infrastructure bottlenecks are most notable in the transport and energy sectors. Poverty and income inequality remain high, while reliance on rain-fed agriculture has exposed farmers to income shocks. One of the development challenges on the social front is youth unemployment, which increased to 7.3% in 2016, compared with 5.7% in 2012.¹⁵

Foreign direct investment has declined from high levels five years ago (about 5% of GDP in 2014), and export growth has stagnated.¹⁶ The medium-term outlook is positive, however, with growth projected at 6.6% in 2019 and 2020, supported by large infrastructure spending.

¹⁰ Veteran Tanzanian politician Edward Lowassa returns to CCM, <https://www.theeastafrican.co.ke/news/ea/Veteran-Tanzanian-politician-Edward-Lowassa-returns-to-CCM/4552908-5005600-10br1dqz/index.html>

¹¹ Chadema leaders defect to CCM, <https://www.thecitizen.co.tz/news/Chadema-leaders-defect-to-CCM/1840340-5078702-p7aj44/index.html>

¹² Veteran Tanzanian politician Edward Lowassa returns to CCM, <https://www.theeastafrican.co.ke/news/ea/Veteran-Tanzanian-politician-Edward-Lowassa-returns-to-CCM/4552908-5005600-10br1dqz/index.html>

¹³ Tanzania Poverty Assessment, <https://openknowledge.worldbank.org/handle/10986/21871>

¹⁴ Ibid

¹⁵ https://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/2019AEO/AEO_2019-EN.pdf

¹⁶ World Bank, Tanzania Overview, <https://www.worldbank.org/en/country/tanzania/overview>

4

Results

This section presents the internet control measures in Tanzania since 1999. It also examines the intervening political and socio-economic considerations behind the different control measures as introduced and applied by different governments.

4.1 Key Trends of Internet Control Over the Last Two Decades

4.1.1 Weaponising the Law to Legitimise Actions

The Tanzanian government has been enacting laws and adopting policies that provide for a more restrictive environment to digital rights. Some of them were introduced under the pretext of ensuring national security and fighting terrorism and cybercrime. However, they were mainly characterised by the criminalisation of free speech and silencing dissent and criticism.

Legalising Surveillance and Interception of Communication

Over the years, Tanzania has adopted legislation to legitimise the country's surveillance practices through legalising interception by state agencies supported by communication intermediaries. Interception of communications is explicitly provided for under the Prevention of Terrorism Act, 2002 and the Intelligence and Security Service Act, 1996.

Under Section 31 of the 2002 Prevention of Terrorism Act, “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.” Section 31 of Subsection 4 of this Act allows for any communications intercepted, including from outside of the country, to be admissible in proceedings for any offence under the Act.

Additionally, the Cybercrime Act, 2015 gives extensive surveillance powers to the police, including in the use of intrusive surveillance methods such as keylogging devices or software that records every keyboard stroke of personal computers in real time, without strictly requiring judicial prior authorisation or oversight.¹⁷ Sections 39-44 of the Act place legal liability on communication service providers to monitor communications, remove information, terminate or suspend services, and notify law enforcement agencies of any alleged illegal activity, giving the ISP the full discretion to determine what constitutes an illegal activity.¹⁸

¹⁷ *Right to Privacy in the United Republic of Tanzania*, https://privacyinternational.org/sites/default/files/2017-12/privacy_tanzania.pdf

¹⁸ *Ibid*

On the other hand, the Tanzania Intelligence and Security Service Act of 1996, which established the Tanzania Intelligence and Security Service (TISS) as a department in the Office of the President, also provides for surveillance powers.¹⁹ Section 5(2) notes that the TISS shall not institute surveillance of any person or category of persons by reason only of his or their involvement in lawful protest, or dissent in respect of any matter affecting the Constitution, the laws or the Government of Tanzania.

The Build-Up of the State's Surveillance Capacity

Tanzania's interest in advancing its surveillance capacity was revealed in a Wikileaks report in July 2015 that revealed communication between a Tanzania State House official, Eliezer Mabula, and Emad Shehata, a key account manager at the Hacking Team, and their planning of a visit to the Hacking Team offices in Milan, Italy.²⁰ Hacking Team sells offensive intrusion and surveillance capabilities to governments, law enforcement agencies and corporations.²¹

In April 2017, Tanzania signed an agreement with South Korea to enhance Tanzania's cyber capabilities. Under the five-year Memorandum of Understanding (MoU), the Korea Internet and Security Agency (KISA) would offer Tanzania expertise and monitor the security of the cyber infrastructure.²² In March 2018, Israel and Tanzania entered into a military training and intelligence gathering and sharing agreement. The countries agreed to intensify their collaboration in key defense and security matters, particularly in troops training, cyber and inter-territorial security as well as improved military technology.²³

Whereas surveillance activity is conducted with utter lack of transparency, there is occasional evidence that state agencies are intercepting communications. For example, following the political clash between high-ranking officials within Tanzania's ruling party CCM in 2019, audio recordings of phone conversations between senior government officials in which they discussed private matters and purportedly insulted the president were leaked and spread on social networks. The source of the leak remains unknown but there were hallmarks of government surveillance activity over the leaks. The president has said he “forgave” the officials who he claims “insulted” him in the audio recording.²⁴

In 2017, Tanzania's Deputy Minister for Transport and Communications, Edwin Ngonyani, appeared to confirm that the country was building up its capacity to conduct surveillance. While making the case for controlling social media and raising the country's cyber capabilities, the minister was quoted as having said: "Our Chinese friends have managed to block such media in their country and replaced them with their homegrown sites that are safe, constructive and popular. We aren't there yet, but while we are still using these platforms we should guard against their misuse".²⁵

In 2019, the verified Twitter account of a vocal Tanzanian opposition leader Zitto Kabwe was compromised, and several tweets posted from the account pledging Zitto's support to President Magufuli. However, his wife immediately clarified that her husband had no access to his laptop or mobile phone, which was then confirmed by Kabwe himself later the same day.²⁶ Although no one took credit for the hack, it shows possible pro-government hacking capacity.

¹⁹ CIPESA et al (2015), *The Right to Privacy in the United Republic of Tanzania: Stakeholder Report Universal Periodic Review 25th Session – Tanzania*

²⁰ See the leaked communications here: <https://wikileaks.org/hackingteam/emails/emailid/16764>

²¹ Hacking Team https://en.wikipedia.org/wiki/Hacking_Team; @Hackingteam <https://twitter.com/hackingteam?lang=en>

²² Dar, Seoul team up against rising cases of cybercrimes, <https://www.dailynews.co.tz/news/dar-seoul-team-up-against-rising-cases-of-cybercrimes.aspx>

²³ Tanzania And Israel Sign Military Training And Intelligence Gathering-Sharing Agreement, <https://intelligencebriefs.com/tanzania-and-israel-sign-military-training-and-intelligence-gathering-sharing-agreement/>

²⁴ President Magufuli says he forgave January Makamba and William Ngeleja, <https://www.thecitizen.co.tz/news/1840340-5260274-9btpfa/index.html>

²⁵ Tanzania: Govt Seeks Chinese Help in Social Media, <https://www.theeastafrican.co.ke/news/Tanzania-seeks-Chinese-help-in-social-media/2558-4041306-d66m76z/index.html>

²⁶ @BwanaAnna on Twitter <https://twitter.com/bwanaanna/status/1144168848926621696>

Silencing Dissent and Criticism through Criminalising Free Speech

Section 16 of the Cybercrime Act, 2015 makes it an offence to publish information, data or facts presented in a picture, text, symbol or any other form in a computer system, where such information, data or fact is false, deceptive, misleading or inaccurate. While the political opposition, national and international human rights groups challenged the constitutionality of the law, the Chief Justice, Mohamed Chande Othman, defended the law as having been enacted in good faith to safeguard the right to privacy of Tanzanians.²⁷

Several people have been arrested in Tanzania in the name of Cybercrime Act. The law authorises law enforcement authorities to jail those who publish “offensive” content or “false” information online. In November 2015, four Tanzanians, Leila Sinare, Godfrey Soka, Deo Soka, and Monica Gaspary Soka were charged under Section 16 of Cybercrime Act, 2015 for publishing false election related information on the social messaging platform WhatsApp.²⁸ Other cases under this law include the arrest and prosecution of Sospiter Jonas in Dodoma in October 2015 for “misuse of the internet” after posting on Facebook that Tanzanian Prime Minister Mizengo Pinda “will only become a gospel preacher.”²⁹ Rights groups and activists believe the law was partly aimed at silencing popular online Swahili based internet forum, JamiiForums, which has increasingly suffered the wrath of the authorities. Digital rights activist and JamiiForums proprietor, Maxence Melo, tasted the acrid side of the law when he was jailed for failure to disclose JamiiForums user data.³⁰ In April 2016, Tanzanian netizen Isaac Habakuk Emily, appeared in court on charges of “insulting” the country's president, John Magufuli, contrary to Section 16 of Tanzania's Cybercrime Act No. 14 of 2015.³¹

In 2018, two foreign journalists working with a journalists’ freedom organisation, the Committee to Protect Journalists (CPJ) were arrested and questioned on grounds that they were engaged in activities contrary to their visas.³² The two journalists, Angela Quintal and Muthoki Mumo were in Tanzania “... to understand the challenges facing the Tanzanian press and to inform the global public.”³³ They were later freed without any charge. Similarly, a Ugandan digital rights advocate and Executive Director of the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), Dr. Wairagala Wakabi who was to speak at the annual Tanzania Human Rights Defenders’ Day hosted by Tanzania Human Rights Defenders Coalition was briefly detained, interrogated and deported to Uganda on grounds of national interest.³⁴ In April 2019. During the several hours of Interrogation, he was denied access to a lawyer.³⁵

²⁷ Why cybercrime act is not easy to defend and justify, <https://www.thecitizen.co.tz/oped/Why-cybercrime-act-is-not-easy-to-defend-and-justify/1840568-3206562-sp7m5f/index.html>

²⁸ Four Tanzanians charged for publishing political information on whatsapp <https://advox.globalvoices.org/2015/11/11/four-tanzanians-charged-for-publishing-political-information-on-whatsapp/>

²⁹ Two Tanzanians accused of False Information Face Charges under new Cyber Crimes Law, <https://tinyurl.com/y9oe6n2z>

³⁰ CIPESA, UPDATE: Maxence Melo Charged with Obstruction of Investigations and Operating a Domain Not Registered in Tanzania, <https://tinyurl.com/y7yowhmp>

³¹ Tanzania cybercrime act makes it dangerous to insult the president on facebook <https://advox.globalvoices.org/2016/04/18/tanzanias-cybercrime-act-makes-it-dangerous-to-insult-the-president-on-facebook/>

³² Freed journalists have safely left Tanzania-CPJ <https://www.nation.co.ke/news/africa/Why-Tanzania-detained-CPJ-staff/1066-4843448-n11o6q/index.html>

³³ Ibid

³⁴ CIPESA, “CIPESA Executive Director Detained At Tanzania Airport – UPDATE”, April 25, 2019, available at <https://cipesa.org/2019/04/cipesa-executive-director-detained-at-tanzania-airport/>

³⁵ Nwachukwu Egbunike, “Tanzanian authorities detain and deport Ugandan human rights leader,” Advox, April 26, 2019, available at <https://advox.globalvoices.org/2019/04/26/tanzanian-authorities-detain-and-deport-ugandan-human-rights-leader/>

4.1.2 The Push Towards Determining Identity Amidst Poor Oversight

The question of determining the identity of telecommunication services users with precision has pushed governments to introduce measures such as mandatory SIM card registration as well as biometric data collection. Between 2012 and 2019, the Tanzania government upped up its ante in collecting and processing users' personal data by launching three major data collection programmes. These were the National Identity card registration by the Tanzania National Identification Authority (NIDA) which began registering citizens' information to facilitate issuance of national identification cards (NIDs) in February 2012. By March 2015, NIDA had registered more than 6.1 million citizens; 1.7 million had received NIDs. Secondly, in March 2018, the TCRA launched a pilot project to register SIM cards using biometric technology. TCRA said in a statement that all SIM cards had to be registered through biometric technology, using NIDA IDs or at least a NIDA registration number from May 1, 2019.³⁶ Thirdly, the government officially commissioned Tanzania's new electronic passport that will have biometric particulars of the bearer, making it virtually impossible to forge or duplicate.

SIM Card Registration

In Tanzania, SIM card registration was started in 2009 under an administrative order of TCRA mainly to address Know Your Customer (KYC) issues.³⁷ In 2010 SIM Registration was backed by the Electronic and Postal Communication Act of 2010 where to use or cause to be used, a SIM card without registration is criminalized.³⁸ 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.³⁹

In March 2018, the Tanzania Communications Regulatory Authority (TCRA) launched a project to register the owners of 43.2 million active SIM cards using biometric technology.⁴⁰ Following this, all SIM cards have to be registered through biometric technology - namely, capture of users' fingerprints alongside scans of their national identity cards or National Identity registration number from May 1, 2019. The exercise, which had earlier been expected to be completed by December 2019, was pushed to January 30, 2020. After this date, the TCRA said it might switch off up to 15 million SIM cards of users who failed to register their mobile phone lines biometrically.⁴¹

Adoption of Biometric Data Collection

In February 2012, the Tanzania National Identification Authority (NIDA) began registering citizens for national identification cards (NIDs) issuance. In October 2015, Tanzania introduced a decentralised Biometric Voter Registration (BVR) process, coupled with the issuance of a voter's card.⁴² The system enabled data collectors to determine the eligibility of citizens in minutes, record their data (photo, fingerprints, signature) and immediately issue a secure voter card. The electronic identification cards were introduced to curb electoral fraud ahead of the 2015 general elections. The process saw the detection of 231,955 cases of multiple registrations.

³⁶ <https://www.thecitizen.co.tz/news/1840340-5075938-89eetq/index.html>

³⁷ Regulatory Collaboration In Ensuring Digital Financial Inclusion In Tanzania https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/Events2019/Togo/Ses3.1_%20Nkya_collaboration.pdf

³⁸ *Ibid*

³⁹ CIPESA (2018) State of Internet Freedom in Tanzania https://cipesa.org/?wpfb_dl=313

⁴⁰ Biometric Sim listing set to start <https://www.thecitizen.co.tz/news/1840340-5075938-89eetq/index.html>

⁴¹ Tanzania says may switch off 15 mln SIM cards in biometric registration, <https://tinyurl.com/yahtax5p>

⁴² Instant Issuance of 24 Million Voters Cards in Tanzania, https://www.evolis.com/sites/default/files/atoms/files/evolis_success_story_tanzania_votercards-en_web_1.pdf

In January 2018, Tanzania commissioned a new electronic East African Community passport to replace the existing passport, set to be phased out by January 2020. The e-passport contains the holder's biometric information on a tamper-proof page, to curb fraud and ease clearance at immigration. The move followed a directive from the 35th EAC Council of Ministers meeting in April 2017 for member states to issue e-passports by January 2018.

4.1.3 Enter The Era of Social Media and Data Taxation

Tanzania adopted the Electronic and Postal Communications (Online Content) Regulations in March 2018 making it compulsory for bloggers and owners of other online forums such as discussion forums and online television and radio streaming services to register with the regulator.⁴³ Online content creators⁴⁴ are to pay application fees of USD 43.7, an initial three-year license fees of USD 437 and renewal fees of a similar amount. The penalty for non-compliance is a fine of USD 2,186. and pay up to USD 900 for a license. Anyone convicted under the regulations faces a fine of at least 5 million shillings (USD 2,200), imprisonment for a minimum 12 months, or both.⁴⁵ Subsequently, the TCRA warned that it would take legal action against all unlicensed websites if they did not comply with the law by June 15, 2018. The move led to the immediate suspension of all unregistered bloggers and online forums for fear of criminal prosecution.⁴⁶

4.2 Key Positive Developments

Despite the negative trends witnessed in Tanzania over the last two decades, there were notable developments that were indeed positive and that support the enjoyment of internet freedom. The country has undergone a digital transformation, reflected by the growing number of people connected to communications and internet services. Mobile internet penetration has nearly quadrupled since 2010 to 18.5%, with more than 8 million new mobile internet subscribers added over that period.⁴⁷ The development is championed by the investment of the government and private sector. The other critical developments have included the growths of robust advocacy and push-back by non-state actors against the regulatory measures adopted by the governments that have resulted in the adoption of progressive legislation as well as the repeal of repressive legislation.

4.2.1 Robust Advocacy and Push-back by Non-State Actors

Sustained civic action appears to be a formidable driver to help counter the internet control measures introduced by governments. In September 2015, the Tanzania Human Rights Defenders Coalition (THRDC), Legal and Human Rights Center (LHRC) and other groups challenged the constitutionality of the Cybercrime Act in the High Court.⁴⁸ In December 2016, the High Court overturned only Section 50 of the law while declaring 19 of the 20 sections of the law constitutional, which decision, the organisations vowed to appeal.⁴⁹

⁴³ Tanzania issues Regressive online content regulations <https://cipesa.org/2018/04/tanzania-enacts-regressive-online-content-regulations/>

⁴⁴ 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

⁴⁵ Legal Analysis Tanzania: Electronic and Postal Communications (Online Content) Regulations 2018, <https://www.article19.org/wp-content/uploads/2018/05/Tanzania-Online-Content-Regulations-2018-Final.pdf>

⁴⁶ CIPESA (2019) Shrinking Civic Space in East Africa https://cipesa.org/?wpfb_dl=299

⁴⁷ <https://www.gsmaintelligence.com/research/?file=783bb9b0ab8e6e53361607a838d25dcb&download>
<https://www.gsmaintelligence.com/research/?file=783bb9b0ab8e6e53361607a838d25dcb&download>

⁴⁸ Parts of Cybercrime Act opposed in court, <https://www.thecitizen.co.tz/news/Parts-of-Cybercrime-Act-opposed-in-court/1840340-2867400-fds9pbz/index.html>

⁴⁹ Activists to challenge ruling on cybercrime law, <https://www.thecitizen.co.tz/news/Activists-to-challenge-ruling-on-cybercrime-law/1840340-3505144-n1il6mz/index.html>

4.2.2 Repeal of Repressive Legislation

In June 2019, following complaints by stakeholders against the Statistics Act 2018, and the blocking of a USD \$50 million fund meant for Tanzania in October by the World Bank blocked, saying it was deeply concerned about restrictions that the government had placed on freedom of speech concerning publication of statistics.⁵⁰ The government repealed a provision in the Statistics Act, 2018, which made it an offence to collect and publish statistics which contradicted those of the National Bureau of Statistics (NBS).⁵¹

⁵⁰ World Bank blocks Sh110bn over Statistics Act <https://www.thecitizen.co.tz/news/World-Bank-blocks-Sh110bn-over-Statistics-Act/1840340-4789448-1sv815/index.html>

⁵¹ It is no longer a crime to publish statistics in Tanzania <https://www.thecitizen.co.tz/news/It-is-no-longer-a-crime-to-publish-statistics-in-Tanzania-/1840340-5174870-wjidxhz/index.html>

5

Conclusion and Recommendations

5.1 Conclusion

Firstly, Tanzania has taken some positive steps that aim to enhance the enjoyment of internet freedom. However, most of the laws and regulations are oppressive and widely limit and curtail internet freedom and rights. These laws and regulations are on steady increase, from none in the beginning of 2000 to three laws in 2019. The laws pose major challenges to citizens especially by violating digital rights and freedoms such as through surveillance and interception of communications, arrests, detention and torture of activists and government critics as well as internet censorship. Similar to these challenges is the continued collection and unauthorised use of biometric data of the individual which results in violation of data protection and privacy rights.

The second issue is the state initiated surveillance capability in Tanzania. There is evidence that suggests the government is expanding its surveillance capabilities. For example, the bilateral agreement with Israel and South Korea to improve the country's cyber abilities as well as leaked information that government officials set up a meeting with The Hacking Team, Italian based cyber security firm. The capability of the government to snoop on large volumes of citizen data (without proper legal tools such as search warrants) brings about challenges of privacy and data protection. The major implication of these issues is interference with individuals' privacy which both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization.

Censorship is the third issue. The report shows indications of censorship such as of websites censored due to different reasons. The censorship trends bring about challenges to the Internet infrastructure industry that is experiencing business and operational impacts, as well as the public who otherwise had exercised their right to information from the censored content. The major implication of this issue is restricting citizens' information acquisition and changing their beliefs and attitudes.

The fourth issue discovered was the big data collection programs such as digital IDs and the collection of biometric data (national ID, passport, driver's license, and voters' card) in Tanzania. Over the years, Tanzania has introduced SIM card registration, Voters ID registration, National Identification (NIDA) as well as new passports all using biometric data from the citizens. The practice is cumbersome to citizens because one ID depends on the other and those who have been registered are required by law to do so again.

5.2 Recommendations

All stakeholders including the government, CSOs, media houses, academia, technical communities, companies and lastly ordinary citizens need joint involvement in order to realise internet freedom. From the study findings, the following emerged as key recommendations.

Government of the United Republic of Tanzania

- Amend all laws that limit freedom of expression and facilitate an aggressive internet governance framework such as the Electronic and Postal Communications Act (2010) and Cybercrimes Act (2015) amendment to ensure that citizens' digital rights are not curtailed in the name of national security concerns.
- Respect and comply with international and regional human rights instruments in respect to internet freedoms like data protection, privacy, online freedom of expression etc.
- Enact a law on data protection and privacy to guarantee individual data privacy and autonomy and ensure compliance with data protection principles in data collection, storage and processing.

Civil Society Organizations (CSOs)

- Raise awareness of citizens on digital rights and internet freedom to enable them understand their rights, duties and obligations for enhanced protection, promotion, enforcement and realisation.

Media Houses

- Play a watchdog role over the government and its actions to ensure protection and respect for internet freedom by the government.
- Inform, educate and mobilize the public to practice and demand their right to Internet freedom.
- Observe ethics, professionalism and self-determination since some of them show contents which aren't appropriate sometimes such as contents about violence against women etc. which in return backfires when the respective digital laws applied

Academia

- Publically speak against unlawful interference with internet freedom and associated rights like freedom of expression and access to information.
- Comprehensively conduct evidence based research and teach students and the general public on internet freedoms, the associated barriers and how to overcome the barriers to ensure full protection and enjoyment.

Technical Communities:

- Advance indigenous technology to improve and develop more home-based interactive platform like Jamii Forums, Fix-chap⁵² etc. so that more users can engage online in expressing themselves and utilising the myriad of opportunities enabled by technology.
- Conduct cybersecurity trainings to citizens so they can be aware of circumvention tools for surveillance and censorship such as email encryptions, virtual private networks (VPN), anonymous browsing, basic computer security i.e. concept of malwares, spams, secured cloud computing, safe URLs, deleting cookies, proper use of social media etc.
- Play a cooperative and necessary leading role in analysing bills, laws and regulation governing and affecting the space with the aim of identifying existing gaps and providing solutions that could potentially better internet rights and freedoms.

Companies

- Respect customers by ensuring data protection and privacy of information and not giving third parties clients' information out without prior consent.. Shun all third party organs or government authorities moves for censorship and surveillance.
- Manufacturers and the support ecosystem around software and hardware tools that produce dual-use technologies that can be used for law enforcement should design their deployment in a transparent way, especially on how their products are used, and should also proactively verify if the purchase objectives are matched in practice. To the extent possible, the sale and utilisation of technologies that can be repurposed for mass surveillance and censorship should be vetted with wider public participation.

Ordinary Citizens

- Citizens have to work closely with all the key and concerned stakeholders including the government in order to get engaged and support themselves in realising and enjoying internet freedom.



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](https://twitter.com/cipesaug)

Facebook: facebook.com/cipesaug

www.cipesa.org