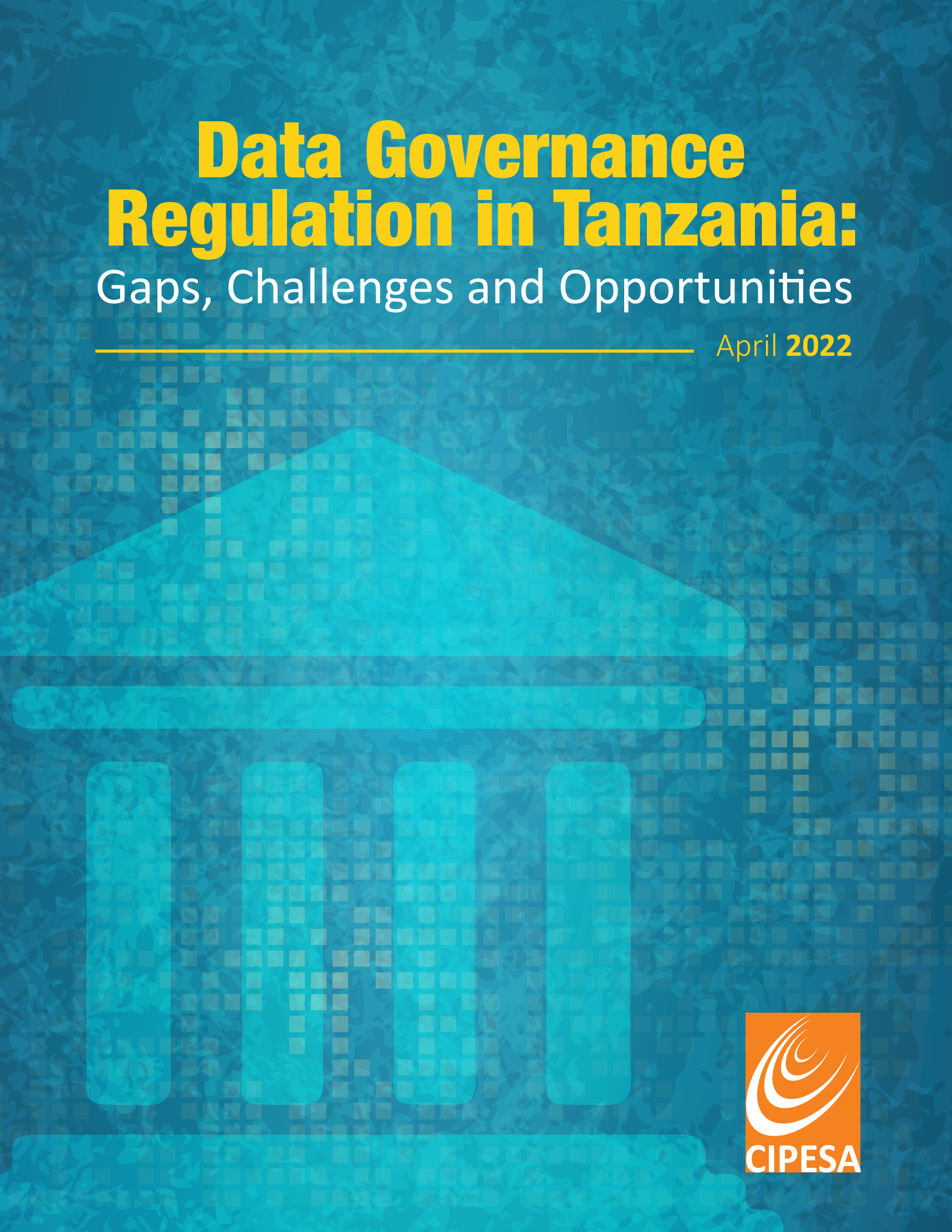
Data Governance Regulation in Tanzania:

Gaps, Challenges and Opportunities

April **2022**



CIPESA

Table of Contents

Acknowledgement:

CIPESA acknowledges the contribution of Media Convergency in the writing of this report.
The report was produced with support from the Hewlett Foundation in the context of promoting data openness among public and private actors and advancing respect for data rights towards citizens' participation and informed policy decisions in rights-respecting data-for-development initiatives. Similar reports have been produced for Ghana, Kenya, and Uganda.

Introduction

In the last few years, the Tanzanian government has undertaken rapid data collection and digitisation initiatives, including digital identity (digital ID), biometric voters' cards, and SIM card registration. In 2014, Tanzania expanded its nationwide programme of issuing biometric National Identity Cards to its citizens and residents. And in 2015, the country introduced a Biometric Voter Registration System in preparation for the 2015 constitutional referendum, with a target of registering at least 20 million voters.[1]

In March 2018, Tanzania's communications regulator, Tanzania Communications Regulatory Authority (TRCA), in collaboration with the National Identification Authority, commenced a 30-day pilot project for biometric registration of customers of all telecommunication service providers.[2] According to the 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. After what the government claimed was a successful pilot, the exercise was rolled out nationwide.[3]

When systematically collected and processed, data becomes critical in informing decision making and policy making by both private and public bodies. Unfortunately, the on-going digitisation programmes are being carried out in the absence of a comprehensive data protection framework, which would provide safeguards against possible violations even as personal data continues to be collected and processed.

The right to privacy has been guaranteed under Tanzania's Constitution with article 16 calling for the enactment of a law that stipulates how privacy rights should be protected, pursued or interfered with by the government. However, this law has not yet been enacted. This delay in enacting a comprehensive data protection law has further increased concerns about data security and safety, and on human rights, which could undermine the efficacy of data initiatives.

In the absence of a comprehensive law, the country and citizens rely on provisions scattered in several laws, including the Electronic and Postal Communications Act, 2010 and its Consumer Protection Regulations. Other laws such as 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 contain contradictory provisions that provide for privacy rights but at the same time, permit surveillance of personal communication and without sufficient safeguards against infringements on privacy rights.[4]

1 *Biometric voter registration kicks off in Tanzania, https://www.aa.com.tr/en/politics/biometric-voter-registration-kicks-off-in-tanzania/72446*

2 *Why TCRA opted for biometric plan, https://www.thecitizen.co.tz/tanzania/news/national/why-tcra-opted-for-biometric-plan-2625236*

3 *Tanzania set to roll out biometric SIM registration, https://www.commsupdate.com/articles/2019/04/29/tanzania-set-to-roll-out-biometric-sim-registration/*

4 *State of Internet Freedom in Africa - Tanzania https://www.opennetafrica.org/?wpfb_dl=92*

There has been growing political will by the government to put in place a proper policy, legislative and institutional framework for privacy and data protection. For instance, the Ministry of Communication and Information Technology is keen on improving the technological landscape, and the government is running the Data Use Partnership which has a well-defined data management aspect to it.[5] It is important, however, that at the heart of these new initiatives are robust data governance policies and practices that harness the benefits of data through multi-stakeholder efforts which are inclusive and empowering. Further, it is crucial that such initiatives respect digital rights, including the rights to privacy and personal data protection, access to information, non-discrimination, and free expression.

Objectives of the Study

In this research brief, CIPESA assesses the state of data governance regulation in Tanzania, including the gaps, challenges, and opportunities around the protection of personal information and data collected by Tanzanian authorities and corporate entities.

Research Methodology

The study used a combination of qualitative methods, including literature review of reports as well as legal and policy analysis of relevant legal instruments including the international and regional human rights instruments. Additionally, 17 key informant interviews were conducted with purposely selected respondents including lawyers, journalists, ICT sector experts as well as law enforcement officers from the Tanzania Police Force Cyber Crimes Unit. The study also conducted a Focus Group Discussion which brought together 10 experts.

5 The Data Use Partnership (DUP) is a Tanzanian Government–led initiative that is improving the national health care system through better digital health systems and the use of health information.

Legal Framework on Data Governance

International Framework on Data Governance

Tanzania is party to various international human rights instruments which directly or indirectly protect data rights and privacy. Tanzania follows a dualistic approach in international laws, where international instruments must first be signed, ratified, and domesticated for them to apply in the country. Some of the instruments which Tanzania is party to include the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights (ICCPR), the Convention on the Rights of the Child (CRC), and the African Charter on the Rights and Welfare of the Child.

Article 17 of the ICCPR states that, "no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence nor to unlawful attacks on their honor and reputation". The United Nations Human Rights Committee has expounded article 17 by stating that the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. States must take effective measures to ensure that information concerning a person's private life does not fall into the hands of persons who are not authorised by law to receive, process, and use the information in a way incompatible with the ICCPR.[6]

In June 2014, African Union (AU) member states adopted the African Union Convention on Cybersecurity and Personal Data Protection (also referred to as the Malabo Convention), making it the first pan-African instrument on privacy and personal data protection.[7] In particular, article 8 of the convention calls upon states parties to commit to establish a "legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data." The convention also outlines internationally recognised principles in personal data collection, storage, and processing. Unfortunately, by the end of March 2022, Tanzania had not signed the convention.[8]

6 *CCPR General Comment No. 16 of 1988, https://www.refworld.org/docid/453883f922.html*

7 *AUCC, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection*

8 *https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf*

National Legal Framework on Data Governance in Tanzania

There is no specific law on data protection and governance in Tanzania. The Data Protection Bill[9] that was first introduced in 2014 is yet to be enacted. Nevertheless, there are some laws with provisions which relate to data protection and governance, though they do not offer sufficient protection.

The Constitution of United Republic of Tanzania of 1977

The Constitution of the United Republic of Tanzania supersedes all other laws which derive validity from it. Article 16 of the Constitution specifically provides for the right to privacy, respect and protection of a person's privacy, matrimonial life, respect and protection of a person's residence and private communications. This article can be interpreted as also offering protection to personal data in a digital environment. The article specifically provides that "Every person is entitled to respect and protection of his person, the privacy of his own person, his family and of matrimonial life, and respect and protection of his residence and private communications". Nevertheless, the Constitution in Article 30 provides for general limitations to the enjoyment of the right to privacy, and state authorities may access personal data under specified circumstances.

The Electronic and Postal Communications Act, 2010

The Electronic and Postal Communications Act (EPOCA)[10] provides for the regulation of postal and electronic communications. The EPOCA, under section 3, defines electronic communication to mean the communication of information in the form of speech or other sound, data, text, or images by means of guided and unguided electromagnetic energy. Under section 98, the Act protects data by imposing the duty of confidentiality on licensees[11] of network services or their agents who may encounter personal information of the customers.

On a positive note, section 120 of the Act prohibits unlawful interception of communication of any person. It also prohibits disclosure to an unauthorised third party or use or attempt to use information which is known to be unlawfully intercepted.

However, the law provides for mechanisms in which licensees are allowed to intercept information in the course of their normal work routine, including for mechanical or service quality checkups, except for random interception. Furthermore, under section 84 of the Act, there is a mandatory requirement for the TCRA to establish and maintain a Central Equipment Identification Register (CEIR) which contains information of all devices collected by licensees from their subscribers, including mobile numbers and special International Mobile Equipment Identity (IMEI) number. Licensees are required to maintain sub-registers that contain all information submitted to CEIR and to submit the same to the TCRA every month. Similarly, section 89 requires all subscriber information as well as the subscriber database under section 91 to be kept within the Authority. These provisions potentially create room for easy monitoring and surveillance of individuals' communications, hence violating their privacy.

9 *https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=2615&file=EnglishTranslation*

10 *Tanzania Electronic and Postal Communications Act, 2010, https://www.tcra.go.tz/en_documents/17*

11 *As per the Act, licensees are those persons who have obtained Network Facilities License, Network Services License, Application Services License or Content Services License.*

The Cybercrimes Act, 2015

The Cybercrimes Act was enacted in 2015 amidst wide criticism. The law protects personal data and information by prescribing offenses related to use of computer systems and information and communication technologies and imposing heavy penalties on those who commit such offenses. The Act also provides for investigation, collection, and use of electronic evidence. The law extends to Tanzanian nationals residing in foreign countries where the offense committed is an offense in both Tanzania and in the foreign land. The Act also applies to foreigners where the offense is committed using a computer system, device or data located in Tanzania.

Section 4 of the Act prohibits illegal access to data, and illegally accessing or causing a computer system to be accessed. Illegal interception of communication is also prohibited under section 6 of the Act, as is interfering with data by damaging, altering, deleting, obstructing, and interrupting it.

On the negative side, the Act empowers police officers to demand disclosure of personal information of internet users from online service providers for purposes of investigations. Section 39 of the Act provides that the Minister will make procedures for service providers to avail authorities with such information, but such procedures have not been made. This opens a loophole for such power to be arbitrarily used.

The Electronic and Postal Communications (Consumer Protection) Regulations, 2018

These regulations were made pursuant to the Electronic and Postal Communications Act, 2010 (EPOCA) with the aim of protecting consumers in dealings with service providers. Regulation 6 protects the privacy of the consumer's information that is collected and maintained by service providers.

The regulations further provide that information of consumers must be fairly and lawfully collected and processed. It must be accurate, processed for identified purposes, and in accordance with other rights of the consumer. Where there is a personal data breach, service providers and their agents shall be liable.

The Electronic and Postal Communications (Online Content) Regulations, 2020

This is another regulation made under EPOCA with the aim of regulating online content service providers, internet service providers, application services licensees and online content users. The law prohibits publication of content which infringes personal privacy and integrity under regulation 16. These regulations exclusively deal with digital data on online platforms and impose a duty on licensees or online content providers to regulate and install mechanisms/firewalls to filter the content published, in order to conform with what is permissible by the regulations and other laws.

Nevertheless, the regulations are widely criticised as having an adverse impact on the right to privacy. For instance, regulation 9 requires online content providers to have surveillance systems in place to identify the source of information or content while regulation 13 provides for the installation of cameras in internet cafes and the storage of recorded images for at least 12 months. The regulations further provide for the assignment of static public Internet Protocol (IP) addresses to computers in cafes, which potentially discourages usage of circumvention tools, such as Virtual Private Networks (VPN), which enable users to bypass network restrictions and to enhance their anonymity.[12]

12 Edrine Wanyama, Tanzania Entrenches Digital Rights Repression Amidst Covid-19 Denialism and a Looming Election, https://cipesa.org/2020/08/tanzania-entrenches-digital-rights-repression-amidst-covid-19-denialism-and-a-looming-election/

The Electronic and Postal Communications (Radio Communication and Frequency Spectrum) Regulations, 2018

These regulations protect against data violation by providing under Regulation 6(1) that a person shall not intercept or acquaint themselves with the contents of any radio communications other than those transmitted for general information or for the information of licensees belonging to the same licensed network. The regulation also prohibits those who have access to radio communication or wireless network from disclosing the content of the communication except to persons authorised or to a court of law. They are prohibited from using that communication in a way not authorised by the TCRA.

The Electronic and Postal Communications (SIM Card Registration) Regulations, 2020

The regulations provide for SIM cards registration by use of biometric data. It should be noted that collected biometric information can be mishandled and misused if not accorded relevant protection and thereby end in the hands of scammers and other unscrupulous individuals.

Under Regulation 20, licensees, dealers, and their agents are prohibited from all acts of misuse of data and information. In case of misuse, the regulations impose a penalty of not less than five million Tanzania Shillings (USD 2,150) or imprisonment for a term not less than 12 months or both.

The Electronic Transactions Act, 2015

The Electronic Transactions Act, 2015 provides for the protection of electronic transactions in the country. It also makes records of electronic transactions admissible as evidence in courts of law. The law does not expressly govern data or privacy of information but to some extent it addresses issues of data governance.

Section 32(1)(a) prohibits the sending of an unsolicited commercial communication unless the consumer has provided prior consent to it. Also, section 32(1)(b) provides that at the outset of the communication, the sender must reveal their identity for the purpose of the communication. The law also requires the communication to have opt-out options and the consumer to have an opportunity to review the transaction before placing an order for goods or services. Further, suppliers are prohibited from interfering with an individual's privacy. Where a person is found guilty of violating one of these requirements, they are liable for a punishment of a fine of not less than 10 million Tanzanian Shillings or imprisonment for not less than one year, or both.

The Banking and Financial Institutions Act, 2006

The Banking and Financial Institutions Act is the main law that regulates the banking and financial sector. The Act regulates and supervises banks and financial institutions for the purpose of maintaining stability, soundness, and safety of the financial system in the country.

Personal data and privacy go hand-to-hand with banking and financial activities, and the financial status of a person is considered as one of the protected data. The Act provides in its section 32 that publication of financial statements of individuals is prohibited unless there is consent to it. Also, as per provisions of section 48, the Bank of Tanzania is not required to divulge information concerning banks or its customers unless there is a requirement by law or by customary practices.

Further, section 48(2) of the Act compels Directors, officers, auditors, and employees of financial institutions to sign fidelity and secrecy agreements before assuming office to ensure the confidentiality of information.

The Registration and Identification of Persons Act, 1986

Section 7 of the Registration and Identification of Persons Act 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 gender, 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. It also prohibits immigration officers performing functions under the Act from producing for inspection, or supplying a copy of, the photograph of any person registered under this Act or their fingerprints or disclosing other personal information by an individual, except with the written permission of the Minister.

The Tanzania Passport and Travel Documents Act, 2002

This Act provides for the regulation of information which should be contained in travel documents such as passports. The First Schedule, under section 7 of the Act, provides for the information that applicants are supposed to provide when applying for travel documents. This includes the full names, nationality, gender, date and place of birth, photograph, signature, profession/occupation, height, color of eyes, and permanent address of the applicant.

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, for example the height, eye color, and profession. Unfortunately, the Act is silent on protection of the collected data.

Regulatory Framework

Tanzania has no specific institution mandated to manage or regulate personal data and privacy. However, as highlighted in the above discussion, management of data is fragmented across sectors.

The Tanzania Communications Regulatory Authority

Majority of data governance laws are within the telecommunications sector where the Tanzania Communications Regulatory Authority (TCRA) is the primary regulator and therefore in charge of all issues relating to data governance. The TCRA is a quasi-independent government body vested with functions of regulating the communications and broadcasting sectors. The Authority was established under the Tanzania Communications Regulatory Authority Act, 2003 with the aim of regulating electronic communications, postal services, and management of the national frequency spectrum. Before establishment of TCRA, there were two commissions which are now defunct dealing with communications and broadcasting services, that is, Tanzania Communications Commission and Tanzania Broadcasting Communications.[13]

The functions and duties of TCRA are laid down in section 5 and include to promote effective competition and economic efficiency; protect the interests of consumers; promote the availability of regulated services to all consumers including low income, rural and disadvantaged consumers; and enhance public knowledge, awareness and understanding of the regulated sectors.

Institutional Framework

Content Committee

This Committee is established under Section 26 of the Tanzania Communications Regulatory Authority Act with the powers and functions of advising the sector minister on broadcasting policy, monitoring and regulating broadcast content, handling complaints from operators and consumers and monitoring broadcasting ethics compliance, along with other functions assigned to it by TCRA.

Regarding data governance, the Committee is responsible for handling consumer complaints which may include data or privacy infringement committed by content service providers or any other actors. The procedure for filing a complaint to the Committee is provided for under Regulation 20 of the EPOCA (Online Content) Regulations, 2020. A person may file a complaint to the content service provider concerning prohibited content, and the provider shall, within 12 hours, resolve the complaint. When the content service provider fails to resolve the complaint within the specified time, the aggrieved person may, within 30 days from the date of filing the complaint, refer the complaint to the TCRA.

The Tanzania Police Force

The Tanzania Police Force (TPF) is the state body with the mandate to protect citizens and their properties. The TPF has a specialised "Cybercrimes Unit" which was inaugurated in 2006 in the Police Force Forensic Laboratory, and it solely deals with computer-related crimes. This unit of the TPF is the main organ dealing with offenses established by the Cybercrimes Act, 2015.

Nevertheless, the powers of the police are quite broad. Although there are written limits on what police can do during the process of arrest and investigation, these are not always adhered to by all police officers.

13 https://www.commonwealthofnations.org/partner/tanzania_communications_regulatory_authority/

Gaps, Challenges and Risks
Facing Data Governance in Tanzania

Lack of a dedicated data protection law and regulator

As noted in the preceding sections, Tanzania does not have a comprehensive stand-alone law on personal data protection. The provisions on data protection are scattered in various laws and do not provide sufficient guidance on good data protection practices. Further, there are no existing regulations to provide for legal procedures, manners, and circumstances under which data can be disclosed by third parties, including law enforcement agencies. Without these legal protections and procedural safeguards in place, the government has few restrictions on how to handle personal data collected through data processing initiatives such as the SIM card registration as well as the National ID registration.[14]

Fragmented Oversight over Privacy and Personal Data

Despite the on-going data collection programmes in the country, Tanzania has no specific body mandated to regulate privacy and data protection. The mandate is scattered among different agencies. For example, the TCRA has been regulating the communication sector to ensure that subscriber data is protected. The 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.

Yet the collection of personal data in Tanzania is not limited to the communication sector. Mobile operators and banks have been collecting information from their customers for the purpose of registration for the traditional banking services and the modern digital transactions such as the use of mobile apps to enable individuals to open bank accounts and effect transactions from wherever they are. Organisations such as mobile operators and banks therefore need to be more accountable for data or information obtained and disclosed by their employees to third parties in contravention of the privacy and confidentiality regulations. Therefore, in the absence of a comprehensive data protection law and an oversight body, risks to the information and data of customers being misused or leaked to third parties are significant.

14 Right to Privacy in Tanzania, https://cipesa.org/?wpfb_dl=212

Claw-back clauses

There are several provisions in various legislation that require disclosure of information and support to state 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 to identify the source of their information or content. This may jeopardise the privacy of the persons who wish to contribute or share content anonymously.

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 information, these procedures have not been published. 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.

Limited capacity of law enforcement agencies

Protection of data in the digital environment requires advanced technology to track data breaches and offenders. This, in turn, requires that law enforcement agencies have the capacity and the tools to investigate and prosecute data privacy breaches and related cybercrimes. In Tanzania such capacity is lacking even as the Cybercrimes Unit of the Police Force, which has one office in the capital Dar es Salaam, plans to establish more cybercrime units in different zones in the Tanzania mainland and Zanzibar. Having one unit makes it hard to conduct thorough and timely investigations.

Poor knowledge and awareness among internet users

Whereas more Tanzanians are getting online, the growth in users of digital technologies is not matched by a corresponding increase in awareness by users about cyber risks. Many internet users are not aware of cybercrime, or of why they need to secure the privacy of their data. Even for those that may be aware of the need to protect their privacy, knowledge of how to do so is in short supply.

On the other hand, many victims of personal data breaches do not report to authorities. The reasons for this include not knowing where to seek remedial measures, fear of being the subject of public ridicule, and having little confidence that relevant authorities would take action against the perpetrators.

Recommendations

- Tanzania should urgently enact a Data Protection Act that fulfills international human rights best practices. Before the law is enacted, the government should consult stakeholders like civil society, academia and the private sector for their inputs.
- Under the prospective Data Protection law, Tanzania should establish an independent Data Protection Authority that is not answerable to another statutory body and whose leaders are appointed through a transparent and competitive process.
- The government should review existing laws, policies and practices on surveillance, biometric data collection, encryption, and data localisation to ensure they comply with the data protection principles in the GDPR and guidelines by the African Union Convention on Cyber Security and Personal Data Protection.
- Civil Society actors should advocate for the promotion and protection of the right to privacy and data protection, by sensitising the public on their rights to privacy and the need for personal data protection including through use of encryption, circumvention and anonymisation tools.
- Civil society actors should continuously document violations of the right to privacy and use them for awareness creation and advocacy for progressive data governance practices.
- The media should regularly report on privacy and data rights violations as a means to create awareness among users and to ensure perpetrators of personal data breaches are brought to book.
- Technology companies and other data controllers should implement privacy and data protection policies and best practices in their handling of customer data.

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