FACTSHEET: TANZANIA

Last updated: 31 March 2020
Prepared by Justin Bryant
Revised by Tshepiso Hadebe

FAST FACTS

Population: 59,204,794
Capital: Dodoma
President: John Magufuli
2020 Freedom House Score: 40/100
Data protection law? No

LAW

While the Constitution of the United Republic of Tanzania guarantees the right to privacy, the Tanzanian context is particularly challenging because provisions in certain laws that grant individuals a small degree of data privacy exist among other provisions that bolster the government's surveillance powers with few institutional checks.

There have been two notable failed attempts to pass comprehensive data protection laws in Tanzania; the 2006 Freedom of Information Draft Bill failed to define key terms and was derided by journalists as curtailing freedom of information, and the Draft Data Protection Bill 2014—which was supposedly based on the EU Directive and the SADC Model Law—omitted consent as a condition for processing, and has been criticised as effectively inoperable despite its similarities to data protection legislation in other countries.

In 2010, Tanzania implemented the Electronic and Postal Communications Act (EPOCA). When it was being drafted, civil society expressed concern over provisions which would threaten privacy rights—such as the establishment of the Central Equipment and Identification Register (CEIR) and a mandatory SIM registration requirement. Before EPOCA, subscribers could communicate anonymously, now every SIM registration has become a personal identifier. SIM registration has allegedly led to wide communication surveillance, location monitoring, and personal data processing for purposes unknown and uncommunicated to data subjects. Police and security agencies are alleged to store communication details using the CEIR.

The fact that there is no requirement of judicial authorisation for interception of communications is problematic. In 2015, the President signed the Tanzanian Cybercrimes Act. After vocal criticism from within and outside Tanzania, the government said that the Act would be reviewed before the end of the parliamentary session. It nonetheless went into effect with changes to only one section. The Act is being challenged in domestic courts on the grounds that several provisions allow law enforcement to search and seize computer systems, data, and information without a court order, eroding the constitutional right to privacy. The Act also permits the police to use invasive surveillance methods such as keylogging devices or software that records keystrokes in real time, without judicial authorisation or oversight.

PERSONAL DATA

EPOCA guards against the violation of any person's entitlement to respect and protection of person, the privacy of their own person, their family and matrimonial life, and respect and protection of their residence and private communications.

COLLECTION AND PROCESSING

The Consumer Protection Regulations provide that a licensee may collect and maintain consumers' or subscribers' information where it is reasonably required for business purposes.

The Cybercrimes Act prohibits operators and other service providers from monitoring activities or data being transmitted in their system, and as such, these providers are shielded from being held liable for illegal activity that takes place within their networks or systems through the actions of third parties. It is, however, lawful for officers, employees, or agents of these providers to intercept, disclose, or use communications transmitted while engaged in any activity necessary to the performance of services or to protect the rights or property of the provider.

REGISTRATION AND ENFORCEMENT

There are no laws currently pertaining to data controllers or their registration.

CROSS-BORDER TRANSFER

There are no laws currently governing the extraterritorial transfer or sale of personal data.

In terms of SIM card data, EPOCA prohibits network service agents from disclosing information unless the information is required by law enforcement, a court of law, or other lawfully constituted tribunal.

The Registration and Identification of Persons Act requires written permission for the disclosure or supply of copies of photos, fingerprints, or particulars furnished under the Act.

SECURITY AND BREACH PROTOCOL

Under the Cybercrimes Act, accessing or causing a computer system to be accessed without permission is an offence punishable by at least one year of imprisonment, a fine of at least three million Tanzanian Shillings, or both. Similarly, to intentionally and unlawfully remain in a computer system or to continue to use a computer system after the expiration of the time which one was allowed is punishable by at least one year of imprisonment, a fine of at least one million Tanzanian Shillings, or both.

Intercepting personal communications and interfering with data by damaging, deleting, altering, obstructing and interrupting it is punishable by a fine of at least ten million Tanzanian Shillings, or three times the value of the undue advantage received by the offender, whichever is greater, or at least three years in prison.

Read the legal notice and terms of use for this factsheet.