

Accountable data use by Law Enforcement Agencies & Intelligence Services

Koliwe Majama

3 March 2021

Funded
by the European Union
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Why Collect Data?

Historically, gathering of communications data has been used for the investigation of crime and national intelligence purposes.

- a) Criminal investigations - Are usually targeted and intended to produce evidence in court eg. Property crimes and drug trafficking, money laundering and tax evasion.
- b) Intelligence gathering - Is mainly for the benefit of & decision making purposes by governments . wide and in some instances is in the form of mass surveillance within and without a particular country's borders
- c) National vs. regional and continental collection - Important especially for regional and international collaboration of intelligence bodies e.g. the Five Eyes comprising Australia, Canada, New Zealand, the United Kingdom, and the United States.

Frameworks for LEA Data Use in Africa



African Union Convention on
Cybersecurity
& Personal Data Protection

(2014)



ACHPR Declaration on the
Principles of Freedom of
Expression and Access to
Information

(2019)



African Declaration on
Internet Rights and
Freedoms

(2014)

International Trends

In the European Union:

The General Data Protection Regulation (2015) - does not apply to the processing of data by LEA

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

African Status

- A. African data protection laws are:
 - I. Generally broad and all encompassing and risk:
 - a) Offer too much protections
 - b) or Give wide powers to the State and LEA
 - II. Weak on limitations on investigating or processing of data excesses
- B. Some African governments rely on old or alternative legislation for collection, processing and use of data stand alone data protection law.
- C. Some African countries have Surveillance laws which undermine rights to privacy (Zimbabwe, Interception of Communications Act)

Ideals

Data protection laws should:

- Be enacted in tandem with surveillance laws that are grounded on human rights principles
- Be proportionate and just -protect targeted/marginal citizens
- Adhere to international human rights law standards/basic principles

Human Rights Based Approach

- P**articipation - Citizens actively in decision making processes
- A**ccountability - Duty bearers should be accountable and effective remedies should be available when breaches occur
- N**on discrimination & equality - LEA should not selectively apply laws to discriminate against vulnerable groups
- E**mpowerment - Citizens should be able to claim and exercise their rights
- L**egality - Laws should be in line with the constitution and international law

Necessity & Proportionality Principles

- States are failing to ensure that laws, regulations, activities, powers, and authorities related to Communications Surveillance adhere to international human rights law and standards. There are 13 principles.
- Key principles for discussion:
 1. Legitimate aim
 2. Necessity
 3. Proportionality
 4. Judicial oversight - or DPA or a human rights commission (But an independent body should be available)
 5. Transparency (post the investigative process) - reporting

Thank You

koliwe@apc.org

apc.org

africaninternetrights.org

koliwemajama.co.zw