Necessity, Proportionality and Accountability in Law Enforcement Use of Personal Data

Workshop no. 5 on Data Protection, 2021

By

Justice Alfred Mavedzenge; Twitter @Dr_JAMavedzenge

Legitimate Purposes for surveillance of electronic and other communications by law enforcement agencies?

- Preventing the commission of serious crimes
- Investigating serious, organised crimes including terrorism, drug trafficking and human trafficking.

Some reasons why surveillance is discouraged

- Violates right to privacy
- Undermine human dignity

Protecting National Security v Privacy: How do we balance between the legitimate competing interests?

- Lawfulness
- Necessity
- Proportionality

What Lawfulness entails

- Decision to conduct surveillance must be provided for by law
- Surveillance powers must be exercised only by persons who are authorised/mandated by law to do so. Such powers CANNOT be delegated unless permitted by the law.
- All the prescribed procedures must be followed both when making the decision and when implementing the decision to conduct surveillance
- Surveillance must be limited to the authorised scope ie. Tools/Equipment to be used, target(s), timeframe, nature of information
- Surveillance must be done strictly for the legitimate purposes prescribed/recognised by the law.

Necessity: What does it entail?

- Surveillance may be authorised ONLY if it is STRICTLY necessarily to achieve the intended purpose ie. There must be no other way of collecting the information to achieve the intended legitimate purpose.
- Surveillance must NOT be conducted because it is the easiest or desirable way of collecting the information/evidence.

Proportionality test

European Court of Human Rights in *S and Marper v United Kingdom (2009)* 48 EHRR 50 at para 118, and in *Gillan and Quinton v United Kingdom (2010)* 50 EHRR 45 at para 56.

"Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy."

So, what does proportionality entail?

- The terms and conditions of the surveillance should be proportionate in the sense that they should not subject the targeted person (s) to surveillance whose nature, extent, and scope is more than what is necessary to achieve the LEGITMATE purpose for which the surveillance has been authorised.

Terms & Conditions for surveillance

To ensure proportionality, a surveillance warrant should be issued subject to defined terms and conditions that are reasonable/proportionate. Amongst other requirements, the terms of the warrant for surveillance must ensure that:

- The equipment to be used does not intrude on privacy more than is necessary
- The scope of information to be collected is limited to what is strictly necessary
- The timeframe for the surveillance is reasonable given the circumstances of the case. It must be limited to what is necessary & cannot be open ended.

Accountability in surveillance

Some existing models for Accountability: Executive approach

The law gives a member of the executive the power to receive applications and decide whether or not to authorise surveillance. For example, see:

- section 5 of the Interception of Communications Act of Zimbabwe;
- Section 64(2)Telecommunication Regulation Law of 2003 of Egypt
- Section 46 of The Anti-Terror Law of 2015 of Egypt

Some existing models for Accountability: The Judicial approach

The request for permission to intercept private communications is made by authorised persons in the executive branch of government. It is then adjudicated over by an independent judge who must consider a set of factors to evaluate lawfulness, necessity and proportionality.

However, in circumstances of an emergency, where there is IMMINENT danger to human life & it is not practically possible to secure judicial authorisation, a law enforcement agent can intercept private communications without a warrant, but he or she must submit a report to the designated judge as soon as possible. Examples include:

- Section 16 of Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) 2002 of South Africa.
- Section 37 of Prevention and Combating of Terrorist and Proliferation Activities Act of 2012 of Namibia
- Section 29 of The Terrorism (Prevention) (Amendment) Act 2013 of Nigeria
- Section 36(1) of The Prevention of Terrorism Act 2012 of Kenya

Some existing models for Accountability: Hybrid Approach

Some countries apply a hybrid of executive and judicial approaches in the sense that they prescribe the judicial approach in interception of communication legislation but prescribe the executive approach in counter-terrorism legislation.

- For instance, in Uganda authorisation to intercept communications can be made either in terms of the Regulation of Interception of Communication Act or the Anti-Terrorism Act. In terms of the *Regulation of Interception of Communication Act*, authorisation for communication surveillance is given by a judge while an application made in terms of Anti-Terrorism Act is adjudicated by a Minister.
- Other countries with hybrid models are Ghana, Democratic Republic of Congo and Tanzania.

Some recommendations for strengthening accountability

- Adjudication of applications for warrant of surveillance must be done by an independent, impartial, and technically competent authority
- There is a need to ensure oversight on the way in which an agency is adjudicating over applications for surveillance. Once a warrant has been issued, it must be submitted to an independent authority for scrutiny & approval (e.g Information Regulator)
- Alternatively, regular audits of the decisions made by the agency when adjudicating over application for warrants of surveillance, should be conducted and reports of such audits should be discussed by Parliament, in camera if neccessary.
- Implementation/execution of surveillance warrants must be monitored by a competent, well resourced and independent authority (e.g Information Regulator)
- It is also important to ensure that victims of arbitrary surveillance have access to effective remedies