

A PERCEPTION SURVEY ON COMMUNICATION SURVEILLANCE AND PRIVACY OF HUMAN RIGHTS DEFENDERS IN KENYA

FACT SHEET

National Coalition of Human Rights Defenders - Kenya

INTRODUCTION

The right to privacy is a fundamental right protected in law across the world including Kenya as stipulated in the Bill of Rights in the 2010 Constitution. It is essential to the protection of human dignity and serves as the foundation upon which many other rights are built. Privacy denotes "that area of individual autonomy in which human beings strive to achieve self realization ... alone or together with others."

Human rights work demands use of communication tools ranging from face-to-face, telephones and e-mails and short message services (SMS). All these provide varied degrees of risk, which are also specific to the work the HRDs are engaged in, as well as contexts. Numerous Kenyan HRDs have raised concerns about their mobile phones being tapped and their communication intercepted. These experiences have implications for HRDs and, therefore, it is essential to ensure that HRDs are not the subject of unlawful surveillance practices and that they are able to do their work without fear of snooping by anyone.

This report analyses the needs, concerns and areas of interest for HRDs in relation to privacy, data protection and communications surveillance. It also establishes how surveillance impacts HRDs work and their role as actors of change in society. Examining the risk levels based on these specifics as well as finding the best-suited measures will be important for continued HRDs protection.

This survey set out to:

- Assess HRDs' level of exposure, understanding, and perception of communication surveillance;
- Document HRDs' current strategies for mitigating, perceived or actual communication surveillance.

This study utilized a mixed methodology, combining qualitative and quantitative approaches. A total of 49 respondents from 15 counties were reached. The quantitative component of the survey targeted 30 HRD respondents while an additional 19 were interviewed as key informants. The survey was guided by the following broad research questions:

1. What are the main norms and legal frameworks being used to govern the right to privacy
2. What are the emerging patterns of how State (i.e. county or national government officials, police, justice system operators) use these laws and how do they affect HRDs and their work
3. What is the level of HRDs' exposure, understanding, and perception of communication surveillance
4. What strategies do HRD's use for mitigating communication surveillance

National Coalition of Human Rights Defenders - Kenya

FINDINGS

Existing framework for the protection of information and Communication in Kenya

Kenya is party to regional and international treaties and conventions that have protections on the right to privacy. As provided in Article 2(5) of the Constitution, general rules of international law and any treaty or convention ratified by Kenya shall form part of the law of Kenya. This means that the international laws and principles directly apply in Kenya to the extent that they are not in contravention of the Constitution.

The Universal Declaration of Human Rights (UDHR), in Article 12, provides for the protection against arbitrary or unlawful interference with privacy, family, home or correspondence as well as against unlawful attacks on honor and reputation. The UDHR provisions are echoed in other international treaties that Kenya has ratified. These include the International Covenant on Civil and Political Rights (ICCPR) which protects the right to privacy in Article 17. It places an obligation on Kenya to adopt legislative and other measures to give effect to the prohibition against such interferences as well as to the protection of the right to privacy. Article 17 envisions that surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping, and recording of conversations should be not be undertaken if inconsistent with Article 17

While it has not yet come into force, the African Union Convention on Cyber Security and Personal Data Protection 2014 is the first regional treaty seeking to advance data protection. In draft Article 8, it provides that each State Party shall commit itself 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." It is important to note that there have been strong criticisms against the Convention, and its implications for human rights.

In Kenya, numerous mechanisms are in place to guarantee the protection of the right to privacy. In 2010, the right was constitutionally entrenched in Article 31 which upholds that: "Every person has the right to privacy, which includes the right not to have (a) their person, home or property searched; (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed, or d) the privacy of their communications infringed." The Constitution also provides that any limitation of the right to privacy should be provided by law, and only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality, and freedom. It is thus not enough for the limitations to be provided in legislation, but they are also obligated to prove that such limitation meets this constitutional threshold.

Judicial pronouncements on the right to privacy and lawful surveillance in Kenya

The constitution guarantees protection of private communications in Kenya. As such lawful surveillance must meet minimum standards provided in law -- necessary in a democratic society to achieve a legitimate aim. It requires that individuals are protected against arbitrary interference with their right to communicate privately.

- CORD v Attorney General (supra) it was held that surveillance and intercepting of communication interferes with the right to privacy, adding that "…surveillance in terms of intercepting communication impacts upon the privacy of a person by leaving the individual open to the threat of constant exposure. This infringes on the privacy of the person by allowing others to intrude on his or her personal space and exposing his private zone."

- *Kenya Human Rights Commission v CAK*[1] , the court found that the DMS did not meet the constitutional test in article 24 requiring limitations of the right to privacy to be proportional

1 Kenya Human Rights Commission v Communications Authority of Kenya & 4 others [2018] Constitutional Petition No. 86 of 2017, eKLR 13

and lawful. It held that it lacked proportionality as there were less restrictive means available to achieve the intended purpose of combating use of illegal devices through the work of the police, the Kenya Revenue Authority, and the Kenya Bureau of standards, which are legally mandated to prevent the importation and use of counterfeit and illegal devices. It further found that DMS was unlawful since the mandate of combating illegal devices does not fall within the statutory mandate of CAK.

- *Okiya Omtata v CAK*[2] and 8 others , the court found that the introduction of DMS failed to meet the public participation requirements, holding that "the public whose data is held…and whose constitutional right to privacy is at risk in the event of breach must as of necessity be involved in the engagements. Thus, the process must be subjected to adequate public participation wide enough to cover a reasonably high percentage of the affected population in the country."

Key findings of the survey

- Human Rights Defenders exhibited varying degrees of apprehensions on possible personal information breaches but there are gaps between concerns about online surveillance and the actual practice of information sharing.

- The increased use of digital-based media and online interactions has enabled expansion and new forms of surveillance. The findings indicate that HRDs are exercising some caution in terms of what they share. However, this still exposes them to the risk of surveillance.

- HRDs use diverse tools to communication is perceived as the most secure in the survey. However, interviews revealed that there are still concerns in interpersonal engagements. Calling the landline, using mobile chats and sending text messages were also perceived as relatively secure even if this is not technically accurate. Posting on social media and sending email without encryption are perceived as least secure.

- HRDs have adopted practices that improve communication security and privacy. The most common is the use of passwords to lock personal gadgets, customizing privacy settings to limit views on social media, a regular check of information to be collected and use of different communication tools. Reluctance to accept phones and computer donations, securing and disguising online footprints were also rated highly.

- HRDs value privacy more than convenience in internet use. When they sense they are being monitored, some HRDs change their behavior in varying degrees including by protecting private information, their perception of privacy and protecting browsing habits.

- Majority of the respondents reported that they have experienced security breaches that include unlawful access to their social media and email accounts as well as phone tapping.

- On interpersonal, relational and physical dimensions of communication surveillance, the two levels of HRDs work -national and county -have provided newer dimensions of surveillance. HRDs touching on violations at the county level are more vulnerable to surveillance because of their proximity to those they monitor. Infiltration by individuals masquerading as HRDs was also reported.

- HRDs working in or sympathetic to minority rights particularly SOGIE issues face more risks of surveillance. Those that use media for advocacy work at the county level also face challenges.

- Many HRDs are equipped to handle issues of preparedness, individual organizational safety,

2 Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others [2018] Constitutional Petition No. 53 of 2017, eKLR

responding, rescuing, and attendant policies and protocols. However, they are not adequately prepared on communication surveillance policies and data protection.

- The levels of knowledge of communication surveillance and information security vary greatly. Beyond policies and skills, there is not much investment in physical resources needed to secure information. Some organizations have adopted protective measures that include installing alarm systems, CCTV cameras and backing up data to ensure that it cannot be completely lost.

Key Recommendations

A number of recommendations are made from this research, which can help to improve and ensure sufficient safeguards whenever there is the collection and processing personal information for whatever legitimate reasons and ultimately, the work of HRDs in advocating a just society.

For Government:

- Ensure an inclusive process for the development and enactment of the proposed Data Protection Bill that conforms to the Constitution of Kenya, 2010 and international standards and best practices on the protection of privacy.
- Ensure that the Computer Misuse and Cybercrimes Act, 2018 conforms with the Constitution of Kenya and international standards of protecting freedom of expression.

For the Private Sector:

- To ensure meaningful access, opt-out, and other rights, there must be a way to provide people with notice about all of the companies collecting their information.
- Be transparent about their business models as well as how personal data obtained as a result of the use of their services is being processed.

For the Kenya National Commission on National Human Rights:

- Call for an independent authority to investigate communications surveillance programs conducted by the Kenyan government and ensure that these practices respect Kenya's national and international obligations to protect the privacy of its citizens and their personal data.
- Investigate all reported cases of unlawful surveillance of human rights defenders and ensure redress mechanisms are available should these lead to the identification of violations of the right to privacy.

For National, Local, and International CSOs and HRDs:

- Advocate for the enactment of a Data Protection Act that conforms to the Constitution and international privacy standards.
- Advocate for the review of the Computer Misuse and Cybercrimes Act, 2018 to conform with the Constitution and international standards of protecting freedom of expression.

For Donors:

- Provide necessary resources, financial and technical, HRDs and CSOs to build secure systems, and develop plans and policies that can improve implementation of secure communication policies and practices.
- Provide funding to rural-based CSOs to work on issues of privacy and surveillance.

For Policy Makers and Law Enforcers:

- Ensure open, inclusive legislative process when adopting a Data Protection Bill which must conform to the Constitution and Kenya's international human rights obligations, and in particular the right to privacy.
- Review and reform existing policies and laws and adopt new legislation that provides an environment for defenders to work freely and safely without communication surveillance.