Mandate of the Special Rapporteur on the right to privacy

REFERENCE:
OL KEN 8/2017

12 May 2017

Excellency,

I have the honour to address you in my capacity as Special Rapporteur on the right to privacy, pursuant to Human Rights Council resolution 28/16.

In this connection, I would like to bring to the attention of your Excellency's Government information I have received concerning **the Kenyan Security Laws (Amendment) Act 2014 and the National Intelligence Service which raise concerns about potential interference with the exercise of the right to privacy**.

According to the information received, the interception of communications in Kenya is currently governed by multiple instruments and presents the following concerns:

Article 42 of the National Intelligence Service Act (2012) establishes the authority of the Director-General to intercept individual communications when she or he "has reasonable grounds to believe that a covert operation is necessary to enable the Service to investigate or deal with any threat to national security or to perform any of its functions." The Article also establishes that these operations "shall be specific and accompanied by a warrant from the High Court."

Article 36 of the Prevention of Terrorism Act (2012) also grants police officers above the rank of a Chief Inspector the power to request an interception of communications order from the High Court. Still according to the same article 36,3,b), the Court may "make an order "authorizing the police officer to enter any premises and to install on such premises, any device for the interception and retention of a specified communication and to remove and retain such device."

The Prevention of Terrorism Act (2012) was amended by the adoption of the **Kenyan Security Laws (Amendment) Act 2014**. **Article 69** inserts "the following new section immediately after section 36- 36A. (1) The National Security Organs may intercept communication for the purposes of detecting, deterring and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary. (2) The Cabinet Secretary shall make regulations to give effect to subsection (1), and such regulations shall only take effect upon approval by the National Assembly. (3) The right to privacy under Article 31 of the Constitution shall be limited under this section for the purpose of intercepting communication directly relevant in the detecting, deterring and disrupting terrorism."

The 2014 amendments also altered the National Intelligence Service Act. **Article 56** introduces a specific section on "Special Operations" related to the National Intelligence Service. This article establishes that: "Where the Director-General has reasonable grounds to believe that a covert operation is necessary to enable the Service to investigate or deal with any threat to national security or to perform any of its functions, the Director-General may, subject to guidelines approved by the Council, issue written authorization to an officer of the Service to undertake such operation."

According to allegations, due to the lack of clarity of the existing framework, the National Intelligence Service often intercepts communication content and acquires call data records to gather intelligence and prevent crimes without court warrants. In occasions the NIS shares with the police the information generated through its interceptions and the police obtain the judicial clearance to monitor the same target again to gather evidence admissible in court.

Section 13 of the Registration of Subscribers of Telecommunications Services Regulations (2014) of the Kenya Information and Communications Act (1998) requires operators to provide the Communication Authority "access to access to its systems, premises, facilities, files, records and other data to enable the Commission inspect." According to allegations received there is lack of clarity with regard to limitations to the data that the operator is to provide and with regard to the authority of the National Intelligence Services while requesting private data (as the 1998 Act was only explicitly with regard to criminal investigations). In this context, it was further alleged that the NIS has direct access to telecommunications network today and are capable to obtain digital content and data without prior notice or judicial authorization. It was also reported that law enforcement agents are present in telecommunications operators facilities and NIS are also informally present.

The NIS reportedly also possesses devices that allow an agent of the small NIS technical unit to geolocate a target through his/her mobile phone. Allegations also indicate that the NIS and Military Intelligence have equipment capable to perform the functions of an IMSI catcher. Allegedly, intelligence gained by intercepting phone communications, primarily by the NIS, is provided regularly to units of the police to carry out counterterrorism operations.

Finally, it was reported that the NIS is meant to be subjected by parliamentary oversight, presumably the Intelligence and Security Committee, although this is not clear based on the wording of the National Intelligence Service Act (2012). Similar the Act establishes an Intelligence Service Complaints Board (see sections 66 and 67.) The Board is limited to making recommendations to the President or Cabinet Secretary. Further, it is alleged that very little information is publicly available about the Board and its investigations, if it has engaged in any.

I would like to share the concern that the current legal and institutional framework governing intelligence and law enforcement surveillance activities imposes undue restrictions on the right to privacy in Kenya.

I am particularly concerned by the alleged lack of clarity on the routine requirement of a prior judicial authorization by a judicial authority. The amendments made in 2014 appear to have significantly expanded the already large scope for interfering in communications. The introduction of a section of "Special Operations" by article 56 is particularly problematic, as the "guidelines approved by the Council" that would regulate some of these initiatives was not developed. I am further concerned by the reported broad access authorities have to telecommunications network and their capacity to obtain data, including by placing officials permanently within facilities of providers, disproportionately limiting the capacity of providers to ensure the protection of communications information. The concerns relating to the existing norms in Kenya are furthered by reports that information collected without any prior judicial authorization by the National Intelligence Service is being shared with law enforcement authorities and counter-terrorism operations, resulting also in serious human rights violations. Finally, at the same time that NIS capacity to interfere in communications was significantly expanded by new norms and new technology the oversight mechanisms which would be crucial to increase protection against abuses of surveillance operations do not seem to be capable to fulfil their role.

In this context, I would like to draw the attention of your Excellency's Government to the obligations regarding the right to privacy, established by the International Covenant on Civil and Political Rights (ICCPR), which Kenya ratified in 1972. Article 17(1) of the ICCPR provides for the rights of individuals to be protected, inter alia, against arbitrary or unlawful interference with their privacy and correspondence and provides that everyone has the right to the protection of the law against such interference.

With regard to permissible restrictions to the right to privacy, I would like to refer to the general comment No. 31 of the Human Rights Committee on the nature of the general legal obligation on States parties to the ICCPR establishes that and that "any restrictions on any of [those] rights must be permissible under the relevant provisions of the Covenant. Where such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights."[1] The Human Rights Committee has later specified that States must ensure that any interference with the right to privacy, should be authorized by laws"(a) publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the

1 CCPR/C/21/Rev.1/Adad. 13, para 6.

limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse." [2]

Furthermore, I would also like to call your Government attention to General Assembly resolution A/RES/71/199 where States note that "while concerns about public security may justify the gathering and protection of certain sensitive information, States must ensure full compliance with their obligations under international human rights law." In particular, the resolution calls States "3 (c) to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law" and d) "to establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data." Similar recommendations are contained in the Human Rights Council Resolution on the right to privacy in the digital age, adopted in March 2017 (A/HRC/RES/34/7).

As it is my responsibility, under the mandate provided to me by the Human Rights Council, to seek to clarify all cases brought to my attention, I would therefore be grateful for your observations on the following matters:

1. Please provide any additional information and/or comment(s) you may have on the above-mentioned allegations.

2. Please indicate how the existing legal framework reflects international human rights norms with regard to the right to privacy. In particular, please clarify the status of the regulation foreseen for Special Operations under the Kenyan Security Laws (Amendment) Act 2014. What safeguards, if any, are in place to ensure interception and access to communications is limited by judicial or other independent authorizations?

3. Please indicate the existing mechanisms overseeing the surveillance activities conducted by the National Intelligence Services and the main results of their work, including public reports.

4. Please indicate whether any investigations have been carried out into the allegations of improper use of intercepted communications by Kenyan law enforcement and counter-terrorism agencies, and if so, what were the results of such investigations.

5. Please inform if IMSI catchers and similar technologies are utilized by NIS or any other Kenyan public entity; on the laws and regulations, if any, to limit their use; and on the safeguards to ensure the adherence to human

2 CCPR /C/USA/CO/4, para 22.

rights standards in the gathering and use of intelligence obtained through these technologies.

I would appreciate receiving a response within 60 days.

Your Excellency's Government's response will be made available in a report to be presented to the Human Rights Council for its consideration.

Please accept, Excellency, the assurances of my highest consideration.

Joseph Cannataci
Special Rapporteur on the right to privacy