DIGITAL SURVEILLANCE IN THE KENYAN COUNTERTERRORISM DISCOURSE:THE CLASH BETWEEN THE RIGHT TO PRIVACY AND THE RIGHT TO SECURITY

CPRSOUTH 2017 **POLICY BRIEF**

Digital surveillance encompasses a broad range of activities conducted with the intent of gathering intelligence. These activities include audiovisual observations to the interception of electronic communications, the collection, processing, storage or transfer of data to third parties. In the wake of advanced technology, the use of the cyber space by criminals to promulgate crimes and the use of internet for terrorist purposes has necessitated the use of digital surveillance to counter crimes. The use of digital surveillance has resulted in infringing privacy right of particular individuals due to its intrusive nature of surveillance on personal lives online. This right to privacy is a fundamental human right that protects the privacy of individuals from unwanted intrusions by the State or any other private actor. Using Kenya as a case study, this brief explores the use of digital surveillance in countering cyber terrorism in relation to the infringement or privacy rights. The country grapples with the threat of terrorism with new waves of online propaganda and recruitment by terrorist organizations such as the al-Shabaab and the ISIS, which had necessitated digital surveillance as means to counter terrorism. This brief expounds on the complexities of balancing the two rights: the right to security and the right to privacy. The clashing of the two rights have been at the epitome in discussions centered on digital surveillance in the counter terrorism discourse. For, various counter-terrorism strategies online, necessitates the encroaching into the privacy context of particular individuals, raising various criticisms from human right organizations, on human rights violations mainly with regard to the right to privacy.

SUMMARY OF FINDINGS

First and foremost, policy makers in Kenya need to understand the balancing of the two rights: the right to privacy and the right to security in the digital surveillance discourse, wherein counter terrorism needs to be conducted in a fast paced technologically driven world. Here, the right to privacy too needs to be considered.

The need to upheld privacy right and the consistency on internet privacy protection in Kenya and other African states are important. This necessitates states on agreeing privacy or data protection laws that could be applied across the Internet. Two guidelines that have shaped the privacy discourse online: Organization for Economic Co-operation and Development Privacy Guidelines in 2013 and the International Principles on the Application of Human Rights to Communication Surveillance of 2013.

Consistency in balancing the two rights have not always been followed or have been relaxed in contexts such as terrorism, where information needs to be gathered quickly with regard to national security. In these contexts, law enforcement officials have been reluctant to follow such guidelines and in some aspects mandated by national laws (in Kenya, such laws include the Prevention of the Terrorism Act of 2012 in Kenya and the Security Amendment Act 2014), evading privacy rights due to the need base timings and specificities of terrorism associated cases.

There is an inverse relationship on the two aspects, if surveillance increases, other rights such as privacy decreases. A main factor in this clash, is the aspect of the right to privacy and other rights associated to the right to privacy itself. For, privacy acts as a basis for other rights such as the freedom of association, freedom of expression and freedom of movement.

The right to freedom of association and assembly are often threatened by the use of surveillance, as an increase in surveillance powers could lead to a 'function creep' (Scheinin, 2013:14) due to the labeling of particular groups or organizations as terrorist organizations as a political campaign tool, where the government use surveillance powers which was initially given only to fight terrorism. Digital surveillance in counter terrorism should be justified when prescribed by law, with a legitimate aim, with proportionality of the aim in regard to the degree of the probability and seriousness of the threat of terrorism in Kenya.

In an attempt to balance the two rights, the policy maker or legislator should utilize empirical evidence in achieving national security. Balancing requires the need to 'justify the derogation of human rights by reference to a demonstrated link between the means (which derogates from the human right) and the end (community safety or national security)' (Brown & Korff, 2009:1). This may require attempting the pros and cons in terms of implications of their proposed decision.

The successful implementation of digital surveillance should be empirically driven with effective public participation in surveillance policy making.

THE RESEARCH

I. DIGITAL SURVEILLANCE AND COUNTER TERRORISM IN KENYA

In Kenya, with the increased threat of terrorism and the new waves of online propaganda and recruitment, had necessitated digital surveillance as means to counter terrorism mainly from al-Shabaab and ISIS. In Kenya, contemporary counter-terrorism policies attest to the fact that public safety strategies involve a strong surveillance role as reflected in the Security Law Amendment Bill of 2014. Within this context of surveillance, the phenomena of privacy have been greatly debated. Commentators have asserted that in Kenya there is a shift in balance between state surveillance and individual privacy rights (Accessnow, 2014). Official responses were in line with public safety threats that have precipitated with an increase in surveillance activity on digital communications.

Increasingly, the adoption of electronic surveillance was to keep pace with technology and pursue crimes on a global scale across transnational linkages. The Government of Kenya employed different types of digital surveillance. In April 2014, under the Umoja Kenya Initiative, the biometric registration process did collect all data pertaining to an individual including name, age, and identities of relatives, property owned and residence. In May 2014, the government announced that the partially state-owned Kenyan communications provider Safaricom had been awarded a government tender to set up a new surveillance system on CCTV for the Kenyan Police, known as the Integrated Public Safety Communication and Surveillance System. In March 2012, the telecommunications industry regulator, the Communications Commission of Kenya (CCK), announced that it was setting up a system to allow the authorities to monitor incoming and outgoing digital communications. CCK requested that all telecommunication service providers cooperate in the installation of internet traffic monitoring equipment known as the Network Early Warning System (NEWS). The CCK cited a rise in cyber security threats as a justification for this move.

II. PRIVACY WITHIN THE DIGITAL SURVEILLANCE DISCOURSE

Certain efforts of the government have been widely criticized in terms of surveillance. Peace Brigades International (2012) stated in relation to human rights defenders (HRDs) in Kenya that incidences of surveillance by state and non-state actors have been reported. Offices have been raided or burgled and computers hacked, and several organizations suspected that their phones were being tapped. Human Rights Watch (2013) warned of the rising attacks on Human Rights Defenders. In July 2015, it was revealed that agents of the Kenyan intelligence services had contacted intrusion malware company Hacking Team to ask them to shut down a critical blog 'Kahawa Tungu' as a 'proof of concept' for their surveillance tools (Global Privacy Network, 2016).

The combination of these trends raises serious concerns about the government's potential use of surveillance tools to further repress on civil society and human rights activists, especially in the context of the 'war on terror,' which the government has used as a legitimizing narrative to justify serious human rights violations. In some cases the legitimacy and proportionality in digital surveillances been questioned, lacking empirical evidence in decision-making. The timeliness of the need for such surveillance with regard to national security being used as an argument for the need for prompt interventions in mitigating the threat of terrorism.

METHODOLOGY

The study is based on the author's experience of working in research related to countering violent extremism in Kenya. The study incorporates primary data from the author's PhD study and other secondary researched materials.

SOURCES

Accessnow. (2014). Surveillance in a legal vacuum: Kenya considers massive new spying system. Available at: https://www.accessnow.org/surveillance-in-a-legal-vacuum-kenya-considers-massive-new-spying-system/ (Accessed on 12 November 2016)

Brown, I. & Korff, D. (2009). Terrorism and the proportionality on internet surveillance, European Journal of Criminology, 6(2):1.

Global Privacy Network. (2016). State of Surveillance: Kenya. Available at: https://www.privacyinternational.org/node/735 (Accessed on 12 November 2016)

Human Rights Watch (2013) Human Rights Watch. 2014. Kenya: Security Bill Tramples Basic Rights: Law makers should reject amendments. Available at: https://www.hrw.org/news/2014/12/13/kenya-security-bill-tramples-basic-rights (Accessed on 20 November 2016)

Peace Brigade International (2012). An assessment of the feasibility and effectiveness of protective accompaniment in Kenya. London: Peace Brigade International. (accessed 11 June 2017)

Sheinin, M. (2013). LIBI Committee Inquiry on Electronic mass surveillance of EU citizens. Available at: https://iow.eui.eu/wp-content/uploads/sites/19/2015/04/141013-LIBE-Scheinin-Supporting-Docs.pdf (accessed 11 June 2017)

AUTHOR

Fathima Azmiya Badurdeen, Department of Social Sciences, Technical University of Mombasa, P.O. Box 90420 – 80100, Kenya, Tel +254 713838765, fazmiya@tum.ac.ke, www.tum.ac.ke