The Right to Privacy v National Security in Africa: Towards a Legislative Framework which Guarantees Proportionality in Communications Surveillance.

By Justice Alfred Mavedzenge*

Published by *African Journal of Legal Studies* , Volume 12(3), 2020, pp 360-390. Official copy can be downloaded from https://brill.com/view/journals/ajls/12/3-4/article-p360_7.xml

1. Introduction

African states and the world over are faced with the rising challenge of organised crime and terrorism. If not effectively dealt with, these challenges may destroy states and societies. In order to deal with these challenges, many governments conduct surveillance and intercept private communications as means to gather information that is necessary to forestall attempts to commit such crimes or to identify perpetrators, for purposes of holding them accountable through the criminal justice system.

Yet, the individual has a right to privacy, including the right to the privacy of their personal communications. Although the African Charter on Human and Peoples' Rights (the African Charter)[1] does not expressly recognise the right to privacy, the obligations of governments to respect and protect certain elements of this right are inferred from other fundamental rights that are expressly guaranteed in this Charter.[2] At the national level, at least

*Justice Alfred Mavedzenge is a Senior Legal Advisor at the International Commission of Jurists and a Researcher at the Democratic Governance and Rights Unit of the University of Cape Town

[1] Of June 1981. The African Charter is the main human rights instrument on the African continent.

[2] These rights include the right to life and human dignity which is recognised in article 4 of the African Charter as follows 'Human beings are inviolable. Every human being shall be entitled to respect for his life and the integrity of his person.' One's integrity or dignity as a person is violated if their personal privacy is unlawfully interfered with. The proposition that the right to privacy is an inferred right under the African Charter has also

25 jurisdictions in Africa[3] have the right to privacy expressly guaranteed as a constitutional right. For instance in South Africa, it is guaranteed as follows: 'everyone has the right to privacy, which includes the right not to have-(a) their person or home searched, (b) their property searched, (c) their possessions seized, or the privacy of their communications infringed.'[4] Zimbabwe,[5] Namibia,[6] Malawi,[7] Kenya,[8] Tanzania,[9] Nigeria,[10] and Ethiopia[11] have similarly framed the right to privacy in their national constitutions, albeit with some slight variations.

There is apparent tension between the duty of the state to respect the right to privacy on one hand, and the obligation to protect national security on the other hand. The right to privacy includes the freedom from having one's private life and communications being pried into. However, in order to combat such vices as organised crime and terrorism, governments may have to conduct investigations which involve spying into the private affairs and communications of certain persons in order to obtain information that is necessary to prevent the crime from being committed or to hold the perpetrators accountable. Such investigations are conducted through electronic surveillance and interception of private communications. At

been made by the African Commission on Human and Peoples' Rights in 'Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa' (2015) at p 36.

[3] These include Zimbabwe, South Africa, Namibia, Botswana, Zambia, Nigeria, Liberia, Cote d'Ivoire, Kenya, Guinea, Gambia, Senegal, Togo, Niger, Benin, Guinea-Bissau, Ghana, Tanzania, Uganda, Ethiopia, Rwanda, Somalia, Lesotho, and Burundi.

[4] See s 14 of the Constitution of the Republic of South Africa, 1996.

[5] See s 57 of the Constitution of Zimbabwe, 2013.

[6] See art 13 of the Constitution of Namibia, 1990.

[7] See art 21 of the Constitution of Malawi, 1994.

[8] See art 31 of the Constitution of Kenya, 2010.

[9] See art 16 of the Constitution of Tanzania, 1977.

[10] See art 22 (1) of the Federal Constitution of Nigeria.

[11] See art 26 of the Federal Constitution of Ethiopia.

least 13 African countries[12] have enacted legislation to empower government to conduct electronic surveillance and intercept private communications. Some countries have enacted legislation to specifically regulate interception of private communications, while in some countries, such authority is provided for and regulated through counter-terrorism legislation.[13] The power to conduct surveillance and intercept private communications is necessary and justified in circumstances where the state needs to combat organised crime, terrorism and similar vices.[14] However, serious concerns have also been raised regarding how governments conduct such investigations in a manner that excessively undermine the enjoyment of individual privacy.[15]

Concerns have also been raised regarding how governments abuse surveillance powers to spy into the private affairs of their opponents in order to gather information which is then used to suppress and stifle legitimate, democratic political activity.[16] Thus, although surveillance and interception of communications are indeed necessary for defending and protecting fundamental rights (from the siege of terrorism and organised crimes), these investigative methods can also be a serious threat to the enjoyment of the same rights,

[12] These include Zimbabwe, South Africa, Namibia, Botswana, Zambia, Nigeria, Kenya, Guinea, Gambia, Ghana, Tanzania, Malawi, and Seychelles.

[13] For example, in Zimbabwe the government has enacted the Interception of Communications Act [Chapter 11:20] while in Uganda, the authority to intercept private communications is also provided for in the Anti - Terrorism Act of 2002.

[14] See African Commission on Human and Peoples' Rights, 'Principles and Guidelines on Human and Peoples Rights while Countering Terrorism in Africa' (2015) 12-13.

[15] See Arthur Gwagwa and others, 'Protecting the Right to Privacy in Africa in the Digital Age' (2014) *Privacy International* 2.

[16] These concerns have led the United Nations to adopt Resolution 68/167: *The Right to Privacy in the Digital Age*, in December 2013. Also see United Nations Special Rapporteur, 'The Right to Privacy in the Digital Age' A/HRC/27/37 (2014) para 14 where the Rapporteur noted that 'There are credible indications to suggest that digital technologies have been used to gather information that has then led to torture and other ill-treatment.'

especially the right to privacy.[17] As Badala Balule rightly observes, surveillance can result in the collection and storage of 'personal data and private information which can be aggregated to provide intimate and detailed profiles of the targeted individuals, resulting in an invasion of the concerned individuals' right to privacy.'[18] This has led to efforts by the international community to develop a set of principles and guidelines to regulate communications surveillance.[19] One of these principles is proportionality.[20]

2. Understanding the proportionality test

Where communication surveillance is necessary, it must be conducted in accordance with the law and in a proportionate manner.[21] Guidelines and principles developed by experts are generally not regarded as binding international or domestic law, unless where such principles have evolved to become part of the rules of customary international law or are part of an international treaty that has been signed and ratified by governments. Therefore, one of

[17] For instance, see Privacy International, 'State of Privacy Uganda' (2018) <https://privacyinternational.org/state-privacy/1013/state-privacy-uganda#commssurveillance> accessed on 4 February 2019. It is noted that 'In late 2011, officials of the Chieftaincy of Military Intelligence (CMI) and Uganda Police Force (UPF), acting on presidential orders, used an intrusion malware, short for malicious software, to infect the communications devices of key opposition leaders, media, and establishment insiders.'

[18] Badala Tachilisa Balule and Bojosi Otlhogile, 'Balancing the Right to Privacy and the Public Interest: Surveillance by the State of Private Communications for Law Enforcement in Botswana' (2015) 37(1) Statute Law Review 19–32.

[19] See United Nations Special Rapporteur, 'Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism' U.N. Doc. A/69/397 (2014) at para 51. Also see United Nations Special Rapporteur, 'Promotion and Protection of all Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development' A/HRC/34/60 (2017) paras 30-39. Also see African Commission on Human and Peoples' Rights, 'Principles and Guidelines on Human and Peoples Rights while Countering Terrorism in Africa' (2015).

[20] Ibid.

[21] See 'International Principles on the Application of Human Rights to Communications Surveillance' officially launched in September 2013 during the session of the UN Human Rights Council in Geneva, available at https://necessaryandproportionate.org/about [Accessed on 4 February 2019].

the challenges to the application of the proportionality principle could be that it is a guideline which governments are not legally bound to adhere to, especially when confronted with problems as serious as those which threaten national security. However, this argument should not hold much water especially in jurisdictions that are bound by the International Covenant on Civil and Political Rights (ICCPR)[22] because the Human Rights Committee has interpreted article 17 of the ICCPR to impose a duty on state parties to ensure that, 'any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case'.[23]

Furthermore, the principle of proportionality is not peculiar to the regulation of communication surveillance and the right to privacy. This principle is also recognised under the limitation clauses in the Bill of Rights of some of the African state constitutions, especially those with English common law background.[24] The principle of proportionality is applied to assess the constitutionality of conduct or measures which limit fundamental rights.[25] Thus, although proportionality of communication surveillance may be regarded as one of the international principles developed with a specific interest to strike a balance between the enjoyment of such rights as privacy and the need to protect national security, it ought to be appreciated that this principle already exist as part of the domestic constitutional law for most

[22] Of 16 December 1966.

[23] See *Toonan v Australia* Communication No. 488/1992 at para. 8.3 and *Antonius Cornelis Van Hulst v. Netherlands*, Communication No. 903/1999 at para 7.3. Also see *M.G v Germany*, Communications No. 1482/2006 at paras10.1 and 10.2.

[24] For example, see the national constitutions of Zimbabwe (section 86), South Africa (section 36) and Kenya (section 24), Malawi (Section 44).

[25] George Barrie, 'The Application of the Doctrine of Proportionality in South African Courts' (2013) 28 *South African Journal of Public Law*, p 40.

African states. In that sense, the principle that communication surveillance must be proportionate is part of municipal law and is enforceable in most jurisdictions on the continent.

South Africa, which is one of the leading constitutional democracies on the continent, has a rich jurisprudence on the application of the principle of proportionality in the context of fundamental rights limitation. The courts have taken the view that the principle of proportionality in its broad sense:

> '..is a safeguard for the individual, over and above traditional methods of controlling the state's administration. It involves a balancing act between the competing interests and objectives of the state… Proportionality demands that when an individual's rights are affected or threatened by state action, only such action shall be countenanced which is suitable, necessary and not out of proportion to the gains to the community.'[26]

In respect of communication surveillance, a committee of experts has noted that:

> '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.'[27]

The African Court of Human and Peoples' Rights seems to have not yet pronounced itself on this subject, but elsewhere, the European Court of Human Rights has made a similar

[26] George Barrie, 'The Application of the Doctrine of Proportionality in South African Courts' (2013) 28 *South African Journal of Public Law*, p40.

[27] See 'International Principles on the Application of Human Rights to Communications Surveillance' officially launched in September 2013 during the session of the UN Human Rights Council in Geneva, available at https://necessaryandproportionate.org/about [Accessed on 4 February 2019].

interpretation as quoted above.[28] But how is this proportionality test applied in practice, when making decisions regarding communication surveillance?

It seems that the proportionality test is a two-stage inquiry. First, is the inquiry into the necessity of communication surveillance. Here, the question is not whether surveillance is desirable or convenient. Rather the question is whether, given the circumstances of the case, there is a pressing need to conduct surveillance in order to protect a legitimate interest or purpose?[29] If the answer to this question is in the affirmative, then the inquiry will progress to the second stage where the agency must determine (in light of the circumstances) the appropriate terms and conditions of surveillance. Crucially, the terms and conditions must stipulate the nature and scope of communications or information to be intercepted, the target persons, the equipment to be used, and the period for surveillance as well as mechanisms for monitoring, to ensure that the surveillance is conducted in accordance with the terms and conditions. These terms and conditions should be proportionate in the sense that they should not subject the targeted person to surveillance whose nature, extent, and scope is more than what is necessary to achieve the purpose for which the surveillance has been authorised. In particular, the terms of the warrant for surveillance must ensure that:

> 'information accessed will be confined to that [which is] reasonably relevant to the crime alleged and any excess information collected will be promptly destroyed or

[28] *S and Marper v United Kingdom* (2009) 48 EHRR 50 at para 118. Also see *Gillan and Quinton v United Kingdom* (2010) 50 EHRR 45 at para 56.

[29] This may entail an inquiry into whether 'there is a high degree of probability that a serious crime has been or will be committed; evidence of such a crime would be obtained by accessing the protected information sought; other available less invasive investigative techniques [are unavailable or] have been exhausted.' See International Principles on the Application of Human Rights to Communications Surveillance available on https://necessaryandproportionate.org/principles [accessed on 4 September 2018].

returned; and information is accessed only by the specified authority and used for the purpose for which authorisation was given.'[30]

Contemporary discussions are focused on identifying mechanisms which should be established in communication surveillance regulatory frameworks (such as legislation) in order to ensure that these principles are adhered to and given effect to at national levels.[31] This paper seeks to contribute to these conversations, particularly by suggesting and discussing the nature of regulatory authorities or agencies which ought to be mandated by surveillance laws to adjudicate over applications or requests for warrants of communications surveillance. Thus, the central question to be discussed in this paper is: what sort of regulatory authorities should be entrusted with the power to authorise communications surveillance, if the principle of proportionality is be achieved, and what is the role of the judiciary?

Admittedly this question has been discussed elsewhere and recommendations have been made[32], albeit without addressing in greater detail certain points *in limine*-questions relating to contextual realities of the different jurisdictions and conceptual hesitations about the right to privacy. These include questions which challenge the legitimacy and relevance of the proportionality principle itself. Policy reform on this subject cannot be achieved without first responding to the following question: Why should governments (in the first place) be concerned about protecting the right to privacy, which is sometimes viewed as an individual

[30] See International Principles on the Application of Human Rights to Communications Surveillance available on https://necessaryandproportionate.org/principles [accessed on 4 September 2018].

[31] See Gwagwa (n 15) 1-13. Also see Privacy International, 'Guide to International Law and Surveillance' (2017) *Privacy International,* p 12-26. Also see Amie Stepanovich and Drew Mitnick, 'Universal Implementation Guide for the International Principles on the Application of Human Rights to Communication surveillance' (2015) *Access,* p 16-22.

[32] See for instance See Gwagwa (n 15) Also see Stepanovich and Mitnick (n 31).

luxury when they are faced with challenges such as organised crime and terrorism, which pose existential threats to states and society? This question must be answered in order to justify why the right to privacy should not be disproportionately limited when the state fulfils its duties towards protecting national security.

3. The significance of the right to privacy

The origins of the right to privacy is a highly contested subject. Some scholars and jurists[33] regard this right as having originated from the English common law, while others, such as John Thauberger, forcefully reject this and instead argue that the right to privacy 'is purely an American development.'[34] It can also be argued that certain elements of the right to privacy were already recognised in the African indigenous law long before the advent of the English law on the continent.[35] The debate regarding where the idea of a right to privacy was originally conceptualised is therefore something that will continue to rage amongst scholars. However, what is important at this juncture is to analyse what the right to privacy means in order to establish what this right entails, which in turn makes it so significant to the extent that there is

[33] Such as Judge Clooney. See Thomas Cooley, *Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* (2nd ed, Callaghan, 1879) p 29. Also see Iain Currie and Johan De Waal, *The Bill of Rights Handbook* (5th ed, Juta, 2005) p 316.

[34] See John Thauberger, 'Right to Privacy' (1965) Vol. 30 (3) *Saskatchewan Bar Review*, p 167-168.

[35] For instance as a rule of custom, there are certain places such as the bedroom and possessions [for example personal clothes] which are treated with utmost respect to the extent that they should not be invaded or seized. In some African cultures, this principle is respected even when a person is deceased, to the extent that the deceased's personal possessions cannot be tampered with until certain rituals have been conducted.

need to ensure proportionate balance between the obligation to respect individual privacy and the duty to protect national security, when authorising communications surveillance.

The African Charter, as indicated above, is silent on the right to privacy and there is therefore nothing in its provisions which identifies the obligations created by this right. Even though in some African jurisdictions the law identifies elements of this right (such as freedom from having one's home searched) these elements are only cited as examples of what this right entails. They are not by themselves an exhaustive enumeration of what the right to privacy entails. Thus, we have to go beyond the legal texts in order to interpret what the right to privacy really mean.

In this connection, some of the prominent scholars on this subject have provided useful views on what they think the right to privacy entails. Judge Clooney described it as the right to be let alone.[36] Samuel Warren[37] argues that it is the right to determine to what extent one's thoughts, sentiments, and emotions should be communicated to others. Allan Westin[38] defines it as the right of an individual to determine 'what information about himself or herself should be known to others.' He also defines it as the freedom from being observed by others.[39] Lloyd Weinreb[40] says it entails the right to conceal or withhold from others certain information. Ian

[36] See Thomas Cooley, *Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* (2nd ed, Callaghan, 1879) p 29. Also see William Prosser, 'Privacy'(1960) Vol 48 (3) *California Law Review*, at p 389.

[37] See 'Right to Privacy.' (1890) Vol 4 (5) *Harvard Law Review*, p 198. He borrowed these views from Yates J, who in *Millar v Taylor* 4 Burr 2303, 2379 (1769) said 'certain every man has a right to keep his own sentiments, if he pleases. He has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends.'

[38] See 'Social and Political Dimensions of Privacy' (2003) (Vol 59 (2) *Journal of Social Issues*, p 43.

[39] Ibid at p 432.

[40] See Lloyd Weinreb, 'The Right to Privacy' in Paul Frankel etal, *The Right to Privacy* (Cambridge University Press, 2000) p 26.

Currie and Johan De Waal[41] say the right to privacy is violated when there is an illegal intrusion on someone's personal privacy or when there has been an unlawful disclosure of private facts or information about a person.[42]

In their attempt to define the right to privacy, it seems different scholars have put different emphasis on different elements of privacy. Thus, the above postulations on what the right to privacy entails are useful but none of them on their own sufficiently captures and explains the full scope of this right. The right to privacy cannot be limited to information or data privacy because it also includes the right not to have one's place of abode searched or intruded.[43] Equally its scope cannot be limited to the right not to be observed by the public or the right to be let alone because the right to privacy includes certain positive obligations to promote and fulfil it. As has been rightly argued by Henry Shue[44] and other scholars,[45] every fundamental right creates at least four types of obligations namely; the duty to respect, the duty to protect, the duty to promote, and the duty to fulfil. Therefore, if the right to privacy is defined as the freedom not to be observed by others or the right to be let alone, this would give a false impression that this right creates negative obligations only and does not create positive obligations to promote and fulfil it. Certainly, the right to privacy also creates positive obligations to promote and fulfil it. For instance, government's obligations are not limited to refraining from interfering with one's personal privacy, but it could be argued that, they also

[41] See *The Bill of Rights Handbook* (5th ed, Juta, 2005) p 316.

[42] Also see UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988 at para 8.

[43] This is reflected in a number of national constitutions in Africa. See for example section 14 (a) of the Constitution of South Africa, 1996 and section 57 (a) of the Constitution of Zimbabwe, 2013. Also see Table 1 below.

[44] See *Basic Rights: Subsistence, Affluence and US Foreign Policy* (Princeton University Press, 1980) p 60.

[45] Who include Iain Currie and Johan De Waal, *The Bill of Rights Handbook* (6th ed, Juta, 2013) p 568.

include the duty to create conditions (such as housing) necessary for every person to enjoy that right. What then is the right to privacy?

It seems appropriate to define the right to privacy as the right to enjoy personal privacy. This includes freedom from having personal privacy spaces invaded or intruded by government and other persons. But what does personal privacy mean? In most African jurisdictions[46], the following have been accepted as falling within the privacy sphere: sexual intimacy, personal thoughts, places where humans live or abode, certain personal possessions such as clothing, and records containing certain personal details such as medical reports. In that sense, one's right to privacy is violated when their private information or personal data is disclosed without their consent,when their home or property is invaded by other people without their consent, when their personal possessions are seized, or when their private communications are intercepted without their consent.

However, it is important to caution that these are not the only aspects of life which are or should be considered as part of the privacy sphere. The full scope of what constitutes personal privacy ultimately depends on context, which differs from one society to the next, and even in one society, it differs from time to time. The context is influenced by a number of factors but more importantly by the society's socio-cultural values and beliefs.[47] Certain conduct is regarded as a matter of personal choice because socio-cultural values of society

[46] For example see section 31 of the Constitution of Kenya; section 21 (1) of the Constitution of Malawi; section 22 (1) of the Constitution of Nigeria and section 16 (1) of the Constitution of Tanzania. These provisions are mimicked in Constitutions across the continent. See Table 1 below.

[47] Lloyd Weinreb, 'The Right to Privacy' in Paul Frankel etal, *The Right to Privacy* (Cambridge University Press, 2000) p 30 and 42-44.

dictate so.[48] A good example is the issue of same sex marriage which is regarded in some societies as culturally acceptable, while in some, it is considered to be uncultural, and the law does not protect it under the right to privacy. For instance, in South Africa, the decision to form and consummate same sex marriage is accepted as a private decision, while in countries like Zimbabwe and Uganda, it is forbidden to form and consummate such relationships, and therefore, it is not considered to be a matter of private choice. Thus, whereas in South Africa the decision to marry a person of same sex is a privacy issue, in Zimbabwe that decision does not fall within the realm of personal privacy.

The context (which determines whether something is within the realm of privacy or not) is also influenced by society's political philosophy which in turn determines the system of governance.[49] In societies based on authoritarian government systems, where the state is keen to control human behaviour, there is little room for individual autonomy from society and the state, and the scope of the privacy sphere is usually narrower than in those societies that are based on liberal democratic ethos. Thus, in liberal democratic societies, where individuals are autonomous, the realm of personal privacy is wide, and consequently, the right to privacy may be claimed in respect of numerous interests or things.

It must be noted, however, that society's political philosophy and socio-cultural values are not static. They are a subject of intergenerational and intra-generational negotiations, and consequently, they are constantly changing. As a result, the realm of what is considered as 'private sphere' keeps changing from time to time, even in one society. Thus, the scope of the

[48] See Allan Westin, 'Social and Political Dimensions of Privacy'(2003) Vol 59 (2) *Journal of Social Issues*, p 433.

[49] Ibid at p 432.

right to privacy is constantly changing and 'debates over privacy are never-ending, for they are tied to changes in the norms of society as to what kinds of personal conduct are regarded as beneficial, neutral, or harmful to the public good.'[50] However, What can be said with certainty is that the right to privacy entails the right to enjoy personal privacy, which includes freedom from unlawful surveillance of the person and their relationships or their personal communications.[51]

Having examined what the right to privacy means, I now turn to analysing why this right deserves protection to the extent that it should not be disproportionately limited when governments seek to address national security challenges which pose an existential threat to society and the state.

Certain theoretical or ideological assumptions and peculiar contextual realities have led to the perception that, the right to privacy does not deserve protection when the country is faced with more serious and imminent challenges which threaten national security.[52] This stems from the idea that individual rights are subservient to collective rights and interests. By its nature, the right to privacy is an individual right[53], whereas protection of national security is a public interest. In that sense, some may argue that when a conflict arises between the right to privacy

[50] Ibid at p 433.

[51] See note 42 above.

[52] This view is well captured and reflected in the presentation by the former UK Foreign Secretary, William Hague at the Info-security Europe conference in 2016 where he said 'The answer [to the question regarding what is more important between privacy and national security] will come through public debate, through unfortunate cases and a new batch of laws. And I can only see that ending up in one place; because seeing what I have [seen] on security and how unacceptable it is in a modern society for the security of the mass of the population to be jeopardised.' For an in-depth critique of this speech see Danny Palmer, 'Security versus privacy: There's only going to be one winner' *ZDNet* (London, 9 June 2016) Available at: https://www.zdnet.com/article/security-versus-privacy-theres-only-going-to-be-one-winner/ [Accessed on 4 September 2018].

[53] Although it can also be claimed by a group of people.

and the need to protect national security, the former must give in to the demands of the latter. For that reason, when surveillance legislation is drafted and enacted, more emphasis is put on giving the state adequate powers to conduct surveillance to protect national security and very little attention is paid towards creating strong mechanisms which ensure that the right to privacy is not disproportionately limited. Checks and balances in the process of securing warrants for surveillance may be viewed as unnecessary inconveniences. In fact, it is sometimes argued that if one does not have anything wrong or criminal which they have done (to undermine national security) then there is nothing to hide and there is no need to worry about the impact of surveillance on their privacy.[54] These counter arguments against the proportional limitation of the right to privacy are based on poor understanding of the purpose served by the right to privacy.

The right to privacy is guaranteed in order to protect human dignity.[55] Human dignity is a multi-faceted concept. At its core, however, is the understanding that a human being has intrinsic or inherent worthiness, and therefore, is worthy to be treated with a certain measure of respect and concern by the society and other human beings.[56] Privacy is constitutionally guaranteed as part of the respect that is due to the human being. But more importantly, the

[54] For a comprehensive discussion and critique of this argument, see Daniel Solove, 'Nothing to Hide: The False Trade-off between Privacy and Security' in Daniel Solove (ed) *Nothing to Hide: The False Trade-off Between Privacy and Security* (Yale University Press, 2011).

[55] See Luciano Floridi, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) *Springer Science + Business Media Dordrecht*, p 308. Also see Report of the United Nations Special Rapporteur on the Right to Privacy, 'Promotion and Protection of all Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development' A/HRC/34/60 (2017) para 29. Also see *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6; 1998 (12) BCLR 1517 at para 30.

[56] Laurie Ackermann, *Human Dignity: Lodestar for Equality in South Africa*. (Juta, 2013) p 56. This view was also echoed in *S* v *Makwanyane* [1995] 1995 (6) BCLR 665 at para 328 where Justice O'regan said 'The importance of dignity as a founding value of the new Constitution cannot be overemphasised. Recognising a right to dignity is an acknowledgement of the intrinsic worth of human beings: human beings are entitled to be treated as worthy of respect and concern.'

human being is understood to have inherent capabilities, which amongst others,[57] include: the capability to exercise his or her own judgement, be autonomous from society, develop and assert their own personality, to form relationships, and to actively influence how his or her society should be shaped.[58]

There seems to be consensus amongst a number of scholars[59] that the right to privacy is based on the philosophical understanding that, although a person lives in a community with others (the public sphere), he or she is nevertheless an autonomous individual who requires personal space (private sphere) which is insulated from the rest of the community. This view has also been endorsed by courts of law[60] and by the United Nations human rights bodies.[61] The personal space is a necessity for every human being because that is the space where the human being can organise his or her personal thoughts, keep certain information about himself or herself which he or she desires to remain private, and form as well as consummate intimate relationships. In a world that is increasingly harsh, it is also a space where the human being

[57] Such as to have self-awareness and a sense of self-worth, to develop personalities, to strive for self-fulfilment in life and to enter into meaningful relationships with others. See Laurie Ackermann, Supra note 56.

[58] Laurie Ackermann, *Human Dignity: Lodestar for Equality in South Africa*. (Juta, 2013) p 23-24. Also see Sandra Liebenberg, 'The Value of Human Dignity in Interpreting Socio-economic Rights' (2005) *South African Journal on Human Rights*, p 7.

[59] See Lloyd Weinreb, 'The Right to Privacy' in Paul Frankel etal, *The Right to Privacy* (Cambridge University Press, 2000) p 25.

[60] For example, in *Bernstein* v *Bester* 1996 (4) BCLR 449 (CC); 1996 (2) SA 751 (CC) at paras 65 and 67 where Justice Ackermann said 'rights, like the right to privacy, are not based on a notion of the unencumbered self, but on the notion of what is necessary to have one's autonomous identity . . . In the context of privacy this means that it is . . . the inner sanctum of the person such as his or her family life, sexual preference and home environment which is shielded from erosion by conflicting rights of the community.' Also see *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6; 1998 (12) BCLR 1517 at para 32 and 117.

[61] See Report of the United Nations Special Rapporteur, 'Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism' (2009) A/HRC/17/34.

retreats from the public sphere to rest and regenerate self before relaunching themselves into the public sphere.

Furthermore, as part of his autonomy from society, the human being should also be allowed to be different from others, especially as he develops his own personality. Such autonomy entails that the human being should enjoy some discretion to make certain choices in his life because a human being is not an object but has agency and has preferences that are unique and different from others and those must be respected by society.[62] Such preferences may include: decisions on family planning, sexual relations or preferences, hairstyles, and dressing.[63] Decisions or choices on such issues are usually regarded as private to the individual and therefore part of the right to privacy. In that sense, the right to privacy is one of the rights which are guaranteed in order to secure the human being's freedom to exercise and enjoy autonomy by choosing to live life in a manner that is different from others. Therefore, when human beings are deprived of privacy, they are in reality deprived of their right to be autonomous from society and that undermines their ability to develop their own peculiar personalities.

Forming and consummating relationships as well as organising personal thoughts are amongst the basic capabilities of a human being as indicated above[64], and these capabilities

---

[62] *National Coalition for Gay and Lesbian Equality* v *Minister of Justice* 1999 (1) SA 6; 1998 (12) BCLR 1517 at para 117.

[63] Ibid at paras 30 and 32 where Justice Ackermann said 'Privacy recognises that we all have a right to a sphere of private intimacy and autonomy which allows us to establish and nurture human relationships without interference from the outside community. The way in which we give expression to our sexuality is at the core of this area of private intimacy. If, in expressing our sexuality, we act consensually and without harming one another, invasion of that precinct will be a breach of our privacy.'

[64] See Laurie Ackermann, *Human Dignity: Lodestar for Equality in South Africa*. (Juta, 2013) p 56 and Mary Gregor (ed), *Immanuel Kant: Practical Philosophy* (Cambridge University Press, 1996) at p 557.

must be allowed to develop and flourish if the human being is to realise his or her full potential. For instance, every human being needs companionship, which can take various forms including family, friendships, and other social relationships. Those relationships are necessary pillars of support for the human being, especially when he or she goes through a crisis in life. But even during moments when he or she celebrates life, the human being often needs the company of his companions. Thus, if the human being is deprived of those social relationships, he is also deprived of the ability to function, flourish, and to exist as a human being. More often, the human being requires privacy in order to form, consummate, nurture, and sustain those relationships, and in that sense, the enjoyment of privacy is a necessary condition which every individual requires in order to be able to function and live as a human being.

Human beings have the capability to actively participate in public life, contributing towards the shaping of the state or their society.[65] The enjoyment of privacy is also a necessary condition for the human being to participate actively in public life. Human beings need a tranquil personal space within which they can formulate and organise their thoughts. For instance, in small private groups or as individuals in their private spaces, citizens form and exchange ideas on how they should react to a government policy or how they should lobby government to adopt a certain policy. Therefore, if the human being is deprived of privacy, they are also deprived of the space to plan on how they should interact with the state and society in the public sphere of life. They are also deprived of the space within which they recoup from the exhaustion and rigours of participating in public life. This undermines the human being's ability to relaunch themselves into the public sphere and continue to contribute towards shaping society. Thus, the right to privacy should be preserved as a utility right, which is meant to protect that space which the human being requires in order for him or her to continue to exist

[65] Ibid.

as an individual as well as to develop his or her potential to make an impact on how the state and society should be shaped. In that sense, the obligation to respect and protect the right to privacy cannot be viewed as being of a lesser value, and which should be ignored when it comes into conflict with the duty to protect national security. The right to privacy is at the core of human dignity and human existence, and for that reason, a proportionate balance ought to be struck between the duty of the state to respect personal privacy and the obligation of the state to protect national security.

What the foregoing discussion also reveals and underscores is that, the enjoyment of the right to privacy is necessary for the enjoyment of other rights.[66] For instance, the enjoyment of free expression depends on whether one enjoys a privacy sphere where they develop thoughts and formulate opinions which they want to express in the public sphere. The right to freedom of association, the right to self-determination, and political participation are other examples of rights which also depend on the enjoyment of individual privacy because 'they require people to be able to communicate free from the chilling effect of government surveillance.'[67] Even rights of socio-economic nature are affected when people are deprived of their privacy. For instance, individuals may be constrained from seeking or communicating sensitive health-related information for fear that their anonymity may be compromised.[68] Therefore, when the right to privacy is taken away, the consequences are that the individual is deprived of a raft of other important rights, and this threatens both the socio-economic wellbeing of the people and the democratic foundation of the state. Thus, notwithstanding its

[66] See United Nations General Assembly Resolution 68/167: *The Right to Privacy in the Digital Age*, December 2013 at para 14.

[67] See note 30 above.

[68] See note 66 above.

efforts and duty to protect national security, the state must ensure that the right to privacy is not disproportionately limited because the enjoyment of many other rights depends on it.

Having dealt with some of the conceptual misgivings against the protection of privacy in the face of threats against national security, it is also necessary to engage with some of the practical arguments that have been advanced against privacy on this subject.

It is argued[69] that the socio-political realities of each jurisdiction should dictate the degree of protection to be afforded to individual privacy, especially where the right conflicts with the demands of national security. In that sense, it is argued that where a state is frequently experiencing terrorist attacks or a civil war or has just emerged from a catastrophic experience of such a nature, emphasis should be more on giving the government widespread authority to conduct surveillance in order to combat the threats to national security rather than bothering with the need to protect individual privacy. Perhaps, this explains why in the aftermath of terror attacks, countries such as Kenya,[70] Uganda,[71] and Egypt[72] have responded by enacting

[69] As is revealed in the presentation by the former UK Foreign Secretary, William Hague at the Info-security Europe conference in 2016. See Danny Palmer, 'Security versus privacy: There's only going to be one winner' *ZDNet* (London, 9 June 2016) Available at: https://www.zdnet.com/article/security-versus-privacy-theres-only-going-to-be-one-winner/ [Accessed on 4 September 2018].

[70] In response to terrorist attacks in 2013, the Kenyan Government amended the Prevention of Terrorism Act (2012) by enacting the Security Laws (Amendment) Act (2014) which gives the state authority to conduct communications surveillance without checks and balances.

[71] In response to terror attacks, the Government of Uganda enacted the Anti-Terrorism Act (2002) which gives unfettered discretion to state agencies to conduct surveillance without prior judicial authorisation. In terms of Article 19(5) read together with (4) of this Act, the state authorities have powers to 'intercept phone calls, emails or other communications, to conduct electronic surveillance as well as monitor meetings, and to do any other thing reasonably necessary for the purpose of surveillance.'

[72] See Human Rights Watch, 'Egypt: Counterterrorism Law Erodes Basic Rights' (2015), available at https://www.hrw.org/news/2015/08/19/egypt-counterterrorism-law-erodes-basic-rights [Accessed on 4 February 2019].

legislation which give the executive widespread powers to conduct surveillance with potential to cause disproportionate limitations on the right to privacy.

Again, this argument reveals an underlying failure to understand the significance of privacy to the existence and development of society. Society or a state is made up of individual human beings, which means a society is a collection of individuals. A society can only be said to be developing and flourishing when the people who make up that society develop and prosper, and this happens only when each of them (as individuals) enjoy an atmosphere or environment that enables or allows them to develop their individual human capabilities. In that sense, the ultimate objective of protecting national security is to create and protect an environment where each individual is safe, free, and allowed to realise his or her human potential for the benefit of his own personhood and that of his society. Therefore, national security cannot be protected in a manner that destroys the very same nation's ability to develop and flourish. As demonstrated above, the enjoyment of privacy is a necessary pre-condition for the protection of the human being's dignity, particularly that the human being requires a private sphere within which he can nurture and develop his personality, form and develop meaningful relationships, as well as, organise his personal thoughts about how he can participate and contribute actively in shaping his society. When the human being is deprived of this private sphere, he is deprived of the environment which he needs in order for him to develop and realise his full potential and that of his nation. For example, without enjoying a private sphere to organise his thoughts and develop his personality, an individual entrepreneur is constrained from developing personal ideas on how to develop and grow his business. Consequently, his personality as a businessperson is constrained from developing and he cannot realise his full potential as an entrepreneur, and the national economy is also deprived of his contribution.

Without the freedom to meet in private and plan on how to engage public authorities on a certain policy, citizens are unable to hold their government accountable or meaningfully participate in public policy development. Thus, the privacy of the individual is not an abstract luxury. It is a basic necessity. If taken away from the human being, there are serious ramifications not only for the personal development of the human being but the collective stability and progress of the society. A government cannot successfully protect national security by taking away privacy, as doing so, would undermine the very same objective which the government is seeking to achieve. Thus, national security can only be protected through means which do not disproportionately undermine the enjoyment of the individual's fundamental rights, including the right to privacy. Surveillance laws must therefore strike a balance between the objective to protect national security and the duty of the state to protect the enjoyment of privacy by individuals. I now turn to examining how governments in selected African jurisdictions[73] have approached this subject in the design of surveillance laws.

4. Approaches applied in legislative frameworks in Africa

One of the necessary requirements for achieving a proportionate balance between protecting privacy and national security is that activities that restrict the right to privacy, such as surveillance, should be prescribed by law and should be proportionate to the legitimate aim being pursued.[74] At least 13 African countries have fulfilled the first requirement by enacting legislation to authorise and regulate surveillance and interception of communications. Such

[73] The selected countries are listed in Table 1 below. The basis for selecting these countries was that they have accessible legislation on communication surveillance and they are drawn from all the African regions (South, North, East, West and Central).

[74] See note 30 above.

authority is provided for in interception of communications legislation and or in counter-terrorism legislation.[75]

However, in order to guarantee the proportionate balance between protecting privacy and national security, the legally prescribed process of securing authorisation to conduct surveillance must involve adequate checks and balances, to ensure that the right to privacy is not disproportionately limited, even as the state conducts surveillance as means to protect national security. Such checks and balance mechanisms include the requirement that authorisation for surveillance must be granted by a competent, independent, and impartial authority.[76] Do these mechanisms exist within the legal frameworks enacted and applied in Africa? It seems that there are three prominent approaches which have been taken in order to authorise surveillance or intercept communications in African states.

4.1 The Executive Approach

One approach is where the legislation gives a member of the executive the power to authorise surveillance and interception of communications. I call this model 'the executive approach'. Under this model, the legislation empowers a designated member of the cabinet (usually responsible for national security) to authorise surveillance and interception of communication. The application requesting for such a warrant must, amongst other details, disclose the following information: the person (if known) whose communication is to be intercepted; full particulars of all the facts and circumstances alleged by the applicant in support of the application; the period for which interception is required and whether alternative means

[75] See Table 1 below: Approaches followed in African jurisdictions in respect of authorisations for communications surveillance.

[76] See note 30 and note 42 above. Also see African Commission on Human and Peoples' Rights, 'Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa' (2015) p 36.

of investigation have been applied and have failed to produce the required information, or the reason why other investigative procedures appear to be unlikely to succeed if applied.[77]

If the application succeeds, the permission is granted in the form of a warrant which ,amongst other things, specifies the person(s) whose communications are to be intercepted and the period for such interception.[78] The warrant for interception of communications is supposed to be issued if there is a reasonable belief that a serious crime is being or has been planned or executed and or if there is an actual or potential threat to national security which requires certain information to be gathered.[79] Upon expiration, the warrant may be renewed by the same cabinet member, who may take that decision in consultation with the Attorney General.[80] See Table 1 below for the list of countries which apply this approach.

4.2 The Judicial Approach

The other model, which is used in some African jurisdictions, is that the procedure for securing a warrant to intercept private communications involve a designated judge or court of law. 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 a judge who must consider a set of factors which are more or less similar to those described under the executive model above.

[77] See for example section 5 (3) of the Interception of Communications Act [Chapter 11:20] of Zimbabwe. For other examples, see Table 1 below: Approaches followed in African jurisdictions in respect of authorisations for communications surveillance.

[78] See Section 7 of the Interception of Communications Act [Chapter 11:20] of Zimbabwe.

[79] Ibid, section 6.

[80] Ibid, section 7.

For instance, in South Africa a judge is designated to receive and adjudicate over applications for warrants to intercept private communications .[81] Except under certain circumstances[82], the application must be in written form and must set out the prescribed details.[83] However, in circumstances of an emergency[84], where there is danger to human life and 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. The judicial approach is applied in a significant number of African jurisdictions as is shown in Table 1 below.

4.3 The Hybrid Approach

Some countries apply a hybrid of executive and judicial approach 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 former legislation, authorisation for communication surveillance is given by a judge while an application made in terms of the latter is adjudicated over by a Minister, and the Anti-Terrorism Act is supreme to the Interception Act, when investigating acts of terrorism.[85] Table 1, below, identifies countries which apply the hybrid approach and how they do so.

---

[81] See Section 16 (1) of The Regulation of Interception of Communications And Provision of Communication-Related Information Act 70 of 2002 of South Africa.

[82] Which are set out in *Ibid* at section 23.

[83] Ibid, section 16 (2).

[84] Such as those detailed at section 7, ibid.

[85] This perhaps reveals the underlying assumption that when countering terrorism, the protection of individual privacy is not so important.

Table 1: Approaches followed in selected African jurisdictions in respect of warrant regimes for authorising communications surveillance

Country	**Primary Legislation Regulating Communications Surveillance**	**Authority designated to adjudicate over application for warrant for surveillance**	**Approach**		
			Judicial	**Executive**	**Hybrid**
South Africa	Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) 2002	Section 16 of the Act requires application to be adjudicated by a designated judge.	□		
Zimbabwe	Interception of Communications Act	Section 5 of the Act requires application to be adjudicated by the responsible Minister		□	
Namibia	Communications Act of 2009	Section 70 (8) requires a request for interception to be accompanied by a warrant	□		
	Prevention and Combating of Terrorist and Proliferation Activities Act of 2012	Section 37 of the Act provides that the application shall be adjudicated by a judge			
Egypt	Telecommunication Regulation Law of 2003	Article 64 (2) requires operators and providers of internet services to allow national security agencies to have access			

		to their systems. The Act does not prescribe that the security agencies must secure judicial authorization before they can intercept communications.		□	
	The Anti-Terror Law of 2015	Article 46 of the Act gives the public prosecutor or the relevant investigating authority the power to authorize communications surveillance.			
Botswana	The Intelligence and Security Service Act	Section 22 of the Act requires the application for warrant to be adjudicated by a senior magistrate or judge of the high court.	□		
	The Counter-Terrorism Act	Section 20 of the Act requires the application for warrant to be adjudicated by a senior magistrate or judge of the high court.			
Uganda	Regulation of Interception of Communication Act	Section 4 requires the application for warrant to be adjudicated by a judge	.		□
	The Anti-terrorism Act	Section 18 gives the responsible Minister the authority to adjudicate over applications for warrants			
Nigeria	Cybercrimes (Prohibition, Prevention, Etc) Act 2015	Section 39 requires interception to be authorized a judge			

	The Terrorism (Prevention) (Amendment) Act 2013	Section 29 of requires warrant to be secured from a judge	□		
Kenya	National Intelligence Act of 2012	Section 42 (3) (c) and (d) of the Act requires that interception of communication be authorized by application a judge			
	The Prevention of Terrorism Act 2012	Section 36 (1) of the Act requires application for warrant to be adjudicated by a judge	□		
Ghana	Anti-Terrorism Act 2008	Section 34 of the Act requires application for warrant to be adjudicated by a judge			
	Electronic Communications Act	Section 100 of the Act authorizes the President to order interception of communications			□
Morocco	The Code of Criminal Procedure	Article 108-116 require application for warrant to be adjudicated by a judge	□		
Democratic Republic of Congo	The Framework Law No. 013-2002	Articles 54(a), 55 and 59 make provision for adjudication of the application by the Attorney General in a judicial case or by the Minister in relation to national security.			□
Lesotho	The Communications Act 2012	Section 44(1)(f) of the Act prohibits communications surveillance without prior judicial authorization.	□		
Tanzania	The Prevention of Terrorism Act 2002	Section 30 (1) gives the Minister the power to direct service providers to intercept communications, while section			□

		31 of the same Act requires interception of communications by a police officer to be done subject to judicial authorization.			

5. A critique of the approaches and recommendations for reform

I must point out forthwith that form does not really matter. What matters is whether the approach or model that has been chosen provides for adequate measures or mechanisms to guarantee adherence to the principles, in this case the achievement of the proportionate balance between protecting privacy and national security. To achieve proportionality there must be an objective and impartial analysis of the facts presented. Such an analysis may be done only by an authority who is independent and technically competent on the subject. A committee of experts[86] on this subject has thus recommended that in order to achieve proportionality:

> 'Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be: (a) separate from the authorities conducting communications surveillance; (b) conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights; and (c) have adequate resources in exercising the functions assigned to them.'

This provides a useful framework against which the approaches applied by Governments should be evaluated.

The executive approach, as described above, has certain conceptual deficiencies which increase the risk of abuse of power with potential to obliterate the enjoyment of the right to privacy and other rights. One of these deficiencies is that the procedure for securing permission

[86] See note 30 above.

to intercept communications does not involve any independent checks and balances. As noted by Privacy International in its report on Zimbabwe (where the executive model is applied), the 'authorities may obtain warrants to intercept private communications through a process that is controlled by members of the executive and not subject to independent scrutiny and oversight.'[87] Security persons, who work for executive agencies request permission from a member of the executive to intercept private communications. Thus, the request is generated from the executive and it is adjudicated over by a member of the executive. By their nature, warrants for surveillance are supposed to be secured and executed secretly, without the knowledge of the persons targeted for such surveillance. However, international standards (as cited above) require that the process of obtaining the warrant must be based on independent checks and balances, yet, the executive model has no one from outside of the executive branch of government to check if all the procedural and substantive requirements of law are complied with in the process of applying, adjudicating, and issuing the warrant. This is even more worrisome given that the cabinet member usually enjoys wide discretion when making a decision to authorise interception.[88] The absence of strong checks and balance mechanisms within this model leaves the right to privacy vulnerable to disproportionate limitations and widespread abuse of surveillance powers, under the guise of the need to protect national security. For instance in Uganda it has been observed that:

[87] See Privacy International, 'Stakeholder Report Universal Periodic 26th Session: *The Right to Privacy in Zimbabwe*, March 2016 at para 10. Also see Privacy International, 'State of Privacy Kenya' (2018) available at https://privacyinternational.org/state-privacy/1005/state-privacy-kenya [Accessed on 4 February 2019].

[88] See Privacy International, 'State of Privacy Uganda' (2018) available at https://privacyinternational.org/state-privacy/1013/state-privacy-uganda#commssurveillance [Accessed on 4 February 2019]. Also see See Privacy International, 'State of Privacy in Egypt' (2018) available at https://privacyinternational.org/state-privacy/1001/state-privacy-egypt#commssurveillance [Accessed on 2 February 2019] and Privacy International, 'State of Privacy Kenya' (2018) available at https://privacyinternational.org/state-privacy/1005/state-privacy-kenya [Accessed on 4 February 2019].

> Over the past decade, there has been an increased concern about surveillance of political dissidents, human rights defenders, and journalists…, particularly in response to the government's increased efforts to allegedly address the threats of terrorism. In 2007, State House brought in a team of Israeli computer experts to coach Uganda's Intelligence security organs on how to; (i) hack into e-mail accounts of individuals perceived to be opponents of government including opposition politicians, human rights activists, journalists and lawyers among others, (ii) carry out forensic investigations on computer hard drives especially those allegedly found in possession of opponents of government and (iii), operate surveillance equipment that monitors both voice and data communications.[89]

Similar observations have been made about other jurisdictions which include Kenya[90], Zimbabwe,[91] Tanzania,[92] and Egypt,[93] where the executive model or certain elements of the executive model are applied. This has led the United Nations Special Rapporteur to conclude that:

---

[89] See Unwanted Witness, 'Preliminary Human Rights Defenders' Surveillance Perception Report in Uganda' (2016) at p 7 available at https://www.unwantedwitness.org/wp-content/uploads/2017/03/Preliminary-Human-Rights-Defenders%C3%A2__-Surveillance-perception-Report-in-Uganda-2016-1.pdf [Accessed on 14 November 2019].

[90] See Privacy International, 'Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya' (2017) available at https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf [Accessed on 14 November 2019].

[91] See Privacy International, 'Stakeholder Report Universal Periodic Review 26th Session: *The Right to Privacy in Zimbabwe,* March 2016 para 34-40 available at https://privacyinternational.org/advocacy-briefing/791/right-privacy-zimbabwe [Accessed on 14 November 2019].

[92] See Privacy International, 'Stakeholder Report Universal Periodic Review 25th Session: *The Right to Privacy in Tanzania,* September 2015 at paras 11-25 available at https://privacyinternational.org/advocacy-briefing/703/right-privacy-tanzania [Accessed on 14 November 2019].

[93] See Privacy International, 'State of Privacy in Egypt' (2018) available at https://privacyinternational.org/state-privacy/1001/state-privacy-egypt#commssurveillance (Accessed on 2 February 2019).

> It is clear, however, that a lack of effective oversight has contributed to a lack of accountability for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Internal safeguards without independent, external monitoring in particular have proven ineffective against unlawful or arbitrary surveillance methods.[94]

However, it should be acknowledged that in some jurisdictions, this approach may nevertheless achieve proportionality because of the contextual realities that are peculiar to those jurisdictions. For instance, it may as well be that the political culture in some jurisdictions allows members of cabinet to independently make value based, impartial, and objective determinations over applications for communications surveillance warrants. Or, the approach may produce positive results because the particular cabinet member mandated to adjudicate over such applications is someone who is technically competent and is capable of exercising an independent mind, notwithstanding the pressures that could be exerted upon him or her from other quarters. In that case, it simply means that the approach is working well not necessarily because it is based on an enduring strong legal framework but because of the individuals involved during that specific period. Thus, there is no guarantee that the approach will continue to produce positive results. It is therefore necessary that the legal framework should provide that the determination over applications for communications surveillance be done by an institution (rather than individual) which is competent and independent. Most of the cabinet members in Africa are appointed by politicians and serve at the pleasure of the appointing authority. It can also be argued that the political culture in most jurisdictions does not allow cabinet members the autonomy to make value based and objective analysis free from political influences and pressures.[95] Therefore, both institutionally and politically, cabinet members are

[94] See United Nations Special Rapporteur, 'The Right to Privacy in the Digital Age' A/HRC/27/37 (2014) para 37.

[95] Because in most of the jurisdictions, members of cabinet are political appointees who serve at the behest of the President and are appointed to implement a political program.

not independent and therefore are unlikely to guarantee an objective and impartial adjudication which is necessary for the achievement of proportional balance between protection of privacy and national security. This makes the executive approach incompatible with the principle of proportionality both conceptually and in practice.

On the other hand, the judicial approach (as described above) is touted as the ideal model.[96] It seems that advocacy for this model is predicated on the assumption that the judiciary is competent and independent to make an objective and impartial analysis of the facts presented in the application for the communications surveillance warrant. Whilst this may be true in some countries, in some jurisdictions the judiciary may be lacking independence from political influences or the judges may not be technically competent to adjudicate on matters relating to communications surveillance and protection of national security. Adjudicating over these issues requires specialised technical knowledge and not just legal knowledge. National security may also be a highly emotive subject, which attracts a lot of attention and pressure to those adjudicating over applications for surveillance warrants. This is likely to be the case especially in countries which often experience high crime rates and terrorism. Thus, adjudicating over these matters require a combination of a high degree of institutional and individual independence as well as technical knowledge of communications surveillance and national security. In view of the widespread challenges relating to judicial independence in Africa[97] and the technical complexities involved in adjudicating over security matters, it would

[96] See Amie Stepanovich and Drew Mitnick, 'Universal Implementation Guide for the International Principles on the Application of Human Rights to Communication surveillance' (2015) *Access*.

[97] See Carolyn Logan, 'Ambitious SDG Goal Confronts Challenging Realities: Access to Justice is Still Elusive for Many Africans' (2017) *Afrobarometer Policy Paper No. 39.*

not be surprising if the judicial approach may fail to produce the desired results in some jurisdictions.[98] What then is the ideal approach?

It is better to take a principled approach when designing communications surveillance legislation. The best model remains one which gives power to authorise communications surveillance to an institution that is independent and technically competent to adjudicate objectively and impartially between the demands of national security and those of the right to privacy. Such an institution does not always have to be the judiciary. It can also be an independent commission or an administrative agency that is established to receive and decide over applications for warrants to conduct communications surveillance. What matters is whether the authority to deal with such applications is given to an institution that is independent and technically competent. If the judiciary is selected as the appropriate authority to adjudicate over applications for such warrants, then it is important to ensure that the judges are genuinely independent and they are exposed to adequate technical training in order to enhance their knowledge of the technical operations involved in communications surveillance and the dynamics of national security. The same must be done with respect to members of any commission or agency which may be designated to perform these duties.

In order to enhance the checks and balances, as well as reinforce the impartiality of the agency, there is also a need to ensure that certain third parties participate in the process of

[98] Although not talking specifically about Africa, the UN Rapporteur made similar observations stating that 'judicial involvement in oversight should not be viewed as a panacea; in several countries, judicial warranting or review of the digital surveillance activities of intelligence and or law enforcement agencies have amounted effectively to an exercise in rubber-stamping.' See United Nations Special Rapporteur, 'The Right to Privacy in the Digital Age' A/HRC/27/37 (2014) para 38.

adjudicating over applications for warrants of surveillance. The United Nations Special Rapporteur has particularly called for 'the creation of public interest advocacy positions within surveillance authorization processes'[99] to provide the agency with independent advice, monitoring, and review to ensure strict adherence to the law. Various suggestions have been made regarding who these third parties should be. In some jurisdictions, it has been suggested that such third parties could be internet service providers[100], members of civil society, or attorneys.[101] What is critical, however, is that the third party must be independent and impartial, and his or her views must be given due consideration when the decision to grant or refuse the warrant is made.

It should of course be acknowledged that in certain circumstances of emergency, it may not be possible to follow the elaborate approach of conducting surveillance only after the warrant has been issued. Practical considerations, such as the nature and imminence of the threat may have to be taken into account in order to protect individual and national security. Thus, even though it is important to ensure that applications be adjudicated over by an independent and competent agency, the legislative frameworks ought to provide for mechanisms to deal with urgent threats but in a way that does not allow a disproportionate limitation of individual privacy. In certain circumstances of urgency[102], the legislative framework should authorise law enforcement agencies to conduct surveillance without prior authorisation but must immediately inform the regulatory authority of their decision as well as

[99] United Nations Special Rapporteur, 'The Right to Privacy in the Digital Age' A/HRC/27/37 (2014) para 38.

[100] Ibid.

[101] I am indebted to Peter Cater QC who suggested this to me during my discussions with him on this subject.

[102] Such as those set out in section 23 of The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 of South Africa.

demonstrate why they had to do it without authorisation.[103] The regulatory authority must have the power to make any determination including to order that the surveillance be discontinued or be continued on certain terms.

6. Conclusion

Governments have a clear and unequivocal obligation to protect national security, especially against threats such as organised crime and terrorism. When fulfilling this obligation, they may have to conduct communications surveillance. However, such surveillance should comply with a number of internationally accepted principles and normative standards. One of them is that surveillance should not be conducted in a manner that causes a disproportionate limitation of the right to privacy. Protecting national security is as important as protecting individual privacy because the ultimate goal of protecting national security is to create and protect an environment where every individual enjoys freedom (including privacy) and is able to prosper in all the faculties of his or her life. Furthermore, the enjoyment of privacy by individuals is a pre-condition for the enjoyment of a range of other fundamental rights including the preservation of human dignity. Thus, when individuals are deprived of privacy, they are in effect deprived of a range of other rights including their dignity, and in a sense, the goal of national security is defeated. For those reasons, it is critical to ensure that privacy is not excessively limited even as the state fulfils its duties towards protecting national security by means of carrying out communications surveillance.

Decisions to authorise communications surveillance must be made after an objective and impartial evaluation of facts that have been presented in the application for a warrant. An

[103] As is the case in South Africa. See section 23 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

independent, impartial, and competent authority is a pre-condition for such an evaluation to be done. Whilst there is a perception that the judiciary is the best institution to make these determinations, it should also be acknowledged that any agency can properly perform this function as long as it is institutionally and individually independent, as well as technically competent and well-resourced to adjudicate impartially over the often highly complex matters relating to communications surveillance technologies and national security. Thus, the best approach towards designing the appropriate legislative framework is the principled approach as opposed to a formalistic or models approach.

However, it is critical to point out that the abuse of communication surveillance powers and capabilities by governments will not necessarily be addressed by establishing an independent, impartial, and technically competent authority to adjudicate over applications for warrants to conduct communication surveillance. There are numerous cases of arbitrary surveillance even in jurisdictions where authorisation for communication surveillance is supposedly done by independent and impartial authorities.[104] A lot more needs to be done in order to curb this scourge. There is a need to ensure oversight on the way in which an agency is adjudicating over applications for surveillance. It is also important to ensure that victims of arbitrary surveillance have access to effective remedies

[104] See Privacy International, 'State of Privacy South Africa' (2018), available at https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa#commssurveillance [Accessed on 2 February 2019].