AFRICAN HUMAN RIGHTS LAW JOURNAL

To cite: LA Abdulrauf 'The challenges for the rule of law posed by the increasing use of electronic surveillance in sub-Saharan Africa' (2018) 18 *African Human Rights Law Journal* 365-391
http://dx.doi.org/10.17159/1996-2096/2018/v18n1a17

The challenges for the rule of law posed by the increasing use of electronic surveillance in sub-Saharan Africa

Lukman Adebisi Abdulrauf
Postdoctoral Research Fellow, SARChI Professorship in International Constitutional Law, Department of Public Law, University of Pretoria, South Africa; Lecturer, Department of Public Law, University of Ilorin, Nigeria

Summary

This article analyses the tension between the rule of law and the increasing use of electronic surveillance in sub-Saharan Africa. Indeed, in the sub-Saharan region today, the rule of law is severely under threat. These threats include bad governance, corruption and a poor human rights track record. Respect for human rights particularly is one of the key indices of the presence of a strong rule of law. However, sub-Saharan African states seriously lag behind in this respect. While so much has been said of the violations of other human rights, not much is said of the right to privacy. Hence, the rule of law being a fundamental component of human rights, the right to privacy faces emerging threats from practices aided by the gradual advances in technology, such as electronic surveillance. Electronic surveillance, with its capacity to effortlessly undermine human rights, is now commonplace in countries in the sub-Saharan region. This becomes more complicated with the frequently-made claim that such surveillance is 'lawful' or 'reasonable' for law enforcement or national security. What amounts to 'lawful' or 'reasonable' intrusions are not only nebulous, but also largely unquestionable. Interestingly, this is not the only difficulty concerning the practice of electronic surveillance. There seems to be a general misconception that electronic surveillance only constitutes a challenge to the right to privacy

* LLB (Zaria) LLM (Ilorin) BL (Abuja) LLD (Pretoria); lukmanrauf@gmail.com. This work is based on the research supported by the South African Research Chairs Initiative of the Department of Science and Technology and National Research Foundation of South Africa (Grant No 98338).

when it actually affects some other important values. In view of this, the article examines the ways in which the increasing use of electronic surveillance undermines the rule of law in sub-Saharan Africa.

Key words: *rule of law; surveillance; electronic surveillance; privacy; data protection; sub-Saharan Africa*

1 Introduction

Edward Snowden's ground-breaking revelation on the extent of state governments' 'mass electronic surveillance' practices has opened a Pandora's box for the rule of law.[1] It has also exposed the extent to which security agencies use various technologies to monitor and intercept the private communication of people regardless of their being suspected of having committed any crime. With the recent threats to security in many countries, especially those relating to terrorism, state governments are rapidly expanding their surveillance programmes. Recently, countries in sub-Saharan Africa have been developing a tremendous interest in spying on their citizens, which is facilitated by their growing technological capabilities. While the act of surveillance in itself is very problematic, electronic surveillance is trickier because of its ubiquitous nature. The increasing use of electronic surveillance raises a number of interesting issues for the rule of law in sub-Saharan Africa. One such issue is the impact of the unregulated use of electronic surveillance on the rule of law in the region. This concern, which is at the heart of this article, is crucial for the democratic development of the region.

Indeed, the debate on electronic surveillance in Africa has not advanced as much as that in other regions. This is one reason why, to the best of our knowledge, there has as yet been no serious consideration of the challenges which electronic surveillance poses to the rule of law in the literature. This is unlike the case in regions such as Europe where electronic surveillance is seen as a major challenge to the rule of law.[2] Nevertheless, it is high time African states seriously

1 These revelations, in summary, was that the US, National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ) were secretly operating a mass surveillance programme which enabled them to access personal information online from the world's largest internet companies, such as Yahoo, Facebook, Google, Twitter, YouTube, Skype and Apple. See Media Policy Democratic Project *An analysis of the communications surveillance legislative framework in South Africa* 5 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (accessed 1 October 2017). See also D Lyon 'Surveillance, Snowden, and Big Data: Capacities, consequences and critique' (2014) July-December *Big Data and Society* 1-13.

2 European Commission for Democracy through Law *Rule of law checklist* 5 29 http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)007-e (accessed 1 October 2017). The document identified, among others, several contemporary challenges to the rule of law that include corruption and conflict of interest and collection of data and surveillance.

considered the impact of electronic surveillance on the rule of law, considering the significant efforts being made to improve their rule of law rating internationally. Issues such as mass surveillance that can affect this rating ought to be taken seriously.

In view of the foregoing, the article poses the following crucial question: How does the increasing use of electronic surveillance impact upon the rule of law in sub-Saharan Africa? In answering the question, the article is organised in six parts. After the introduction, part two discusses the law and practice of electronic surveillance in sub-Saharan Africa. Part three establishes the link between electronic surveillance and the rule of law, while part four analyses the specific challenges which the increasing use of electronic surveillance poses to the already fragile state of the rule of law in sub-Saharan Africa. The fifth part re-evaluates the measures to entrench the rule of law in the use of electronic surveillance, before concluding with some reflections on the future of the rule of law and electronic surveillance in sub-Saharan Africa.

For the purposes of the article, some caveats are in order. First, while the article focuses on sub-Saharan Africa,[3] it does not claim to cover the entire region. The analysis focuses on particular countries that may effectively represent the region.[4] Second, although electronic surveillance is usually carried out for different purposes and by different entities, the article focuses on (electronic) surveillance practices carried out for supposedly 'law enforcement' and 'national security' purposes.[5] Third, although electronic surveillance could be either domestic or extraterritorial (foreign surveillance), the article focuses on the former category. The latter category raises broader issues of international law, which are largely beyond the scope of the present exercise.[6]

3 Sub-Saharan Africa comprises countries that are fully or partly located south of the Sahara. The sub-Saharan region comprises 46 African countries, excluding Algeria, Egypt, Libya, Morocco and Tunisia.

4 For this purpose, more reference will be made to Nigeria (representing Western Africa), South Africa (representing Southern Africa) and Uganda (representing Eastern Africa).

5 According to Brookes, electronic surveillance is generally used for security reasons, in pursuit of hobbies and for checking on spouse loyalty. See P Brookes *Electronic surveillance devices* (2001) 1. There are many other uses, such as for the purposes of monitoring employees in a work place, and so forth.

6 For more on this, see A Deeks 'An international legal framework for surveillance' (2015) 55 *Virginia Journal of International Law* 292. See also M Milanovic 'Human rights treaties and foreign surveillance: Privacy in the digital age' (2015) 56 *Harvard International Law Journal* 81.

2 Conceptualisation, practice and normative framework of electronic surveillance in sub-Saharan Africa

The normative framework on the application of electronic surveillance can be found in a number of legal instruments. However, none of these instruments defines surveillance. The question then is: What is electronic surveillance?

2.1 Conceptualising electronic surveillance

The term 'electronic surveillance', to the best of our knowledge, has not been defined in any law or policy regulating its practice in sub-Saharan Africa.[7] In fact, these instruments rarely use the term 'surveillance'; rather they use associated terms such as 'interception', 'communications', 'monitoring' and other device-specific terms. This may be because of the inherent difficulty in conceptualising such a term. Surveillance usually is defined in relation to its nature (overt or covert) or on the basis of the level of contact with the target, whether remote or direct.[8] Basically, surveillance means to monitor or closely observe.[9] This basic definition is problematic in that it anticipates the monitoring of a specific person who, for example, may be suspected of committing a crime. However, as will be shown shortly, modern surveillance practices do not necessarily involve monitoring a specific or identified person or for any particular purpose. Similarly, discussing surveillance in the context of 'monitoring' or 'observing' takes away one critical feature of modern surveillance practices, namely, the gathering or collecting of information about people and not necessarily observing them in the technical sense of the term.

The term 'electronic surveillance' may even create more definitional difficulties. However, a simple definition is that of the United Nations (UN) Office on Drugs and Crime (UNODC) which is that 'surveillance is the collection or monitoring of information about a person or persons through the use of technology'.[10] The definition, though imperfect, highlights two important points which is crucial for this article. First, it mentions that surveillance involves (personal information) gathering and, second, such gathering or collection occurs with the aid of technology. However, this definition also omits

7 See United Nations Office on Drugs and Crime (UNODC) *Current practices in electronic surveillance in the investigation of serious and organised crime* 1 https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf (accessed 1 October 2017). However, the US Foreign Intelligence Surveillance Act (FISA) 1978 specifically defines surveillance in sec 1801.

8 As above.

9 *Collins concise dictionary* (2001).

10 As above. See also a related definition in M Watney 'State-on-nationals. Electronic communication surveillance in South Africa: A murky legal landscape to navigate?' http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7335047 (accessed 1 October 2017).

one important feature which is the fact that, in most circumstances, the collection of the information usually is without the consent of persons.[11] Consent is crucial as it usually is the thin line separating unlawful from lawful surveillance.

From the foregoing, electronic surveillance is the use of technology to gather information about an individual or individuals. These technologies could vary from the simple use of cameras to more intrusive means, such as the use of sophisticated software to process personal information about a person.[12] Another important point to note is that electronic surveillance is unique in that it differs from all other types of government intrusions. According to Cassie, in the case of electronic surveillance, 'there is no seizure of tangible property, no search of a defined structure or place, and if properly executed, no knowledge of the government's action by the target of the search'.[13] It is submitted that modern electronic surveillance practices does not even involve identifying a specific target. Government surveillance programmes indiscriminately collect information for no specific purpose or reason.

2.2 Increased use of electronic surveillance in sub-Saharan Africa: The move toward sophisticated surveilling technologies

It is not an exaggeration to say that sub-Saharan Africa is gradually evolving into a 'surveillance society'.[14] This is because of the extent and sophistication of the current surveillance practices in the region. According to a recent report, 'many African governments are outdoing themselves in acquiring state of the art software that will enable them to eavesdrop on their citizens'.[15] Yet, most states keep their surveillance capabilities or spying programmes a closely-guarded secret, making it difficult to document the exact nature and extent of electronic surveillance in sub-Saharan Africa.[16] Nevertheless, there is available evidence of some of these practices from a few sources.

Recently, advances in technology have seen states adopt more ubiquitous and modern methods of electronic surveillance, such as

11 Eg, the definition of electronic surveillance under the US FISA includes consent.

12 For an incisive analysis of recent surveillance technologies and the attitude of the courts, especially in the US, see T Casey 'Electronic surveillance and the right to be secure' (2008) 41 *University of California, Davis* 977.

13 Casey (n 12 above) 985.

14 According to Tzanou, there are three main features of a surveillance society: (1) the increased engagement in intelligence gathering and surveillance activities; (2) the use of new technologies and technological devices; and (3) the overall goal of enhancing security. M Tzanou 'The EU as an emerging "surveillance society": The function creep case study and challenges to privacy and data protection' (2010) 4 *Vienna Journal on International Constitutional Law* 407.

15 CIPESA *State of internet freedom in Africa 2016* (2016) 18 https://cipesa.org/?wpfb_dl=225 (accessed 1 October 2017).

16 Deeks contends that '[i]t is difficult to know precisely what types of surveillance each state is conducting, what technologies they are using, and what their targets are'; Deeks (n 6 above) 344.

the use of complex devices and software for the interception of phone conversations and activities, generally online. For example, in an exclusive report in 2013, *Premium Times*, a leading online news outfit, exposed the presence of a 'Big Brother' phenomenon in Africa.[17] It was revealed that the President of Nigeria was secretly engaging an Israeli firm, Elbit Systems,[18] 'to help it to spy on citizens' computers and internet communications under the guise of intelligence gathering and national security'.[19] This affords the government easy access to all computers and the ability to read all e-mail correspondence of citizens. This agreement was worth over $40 million and, according to *Premium Times*, the contract was 'one of the most far-reaching policies ever designed in Nigeria's history to invade the privacy of citizens'.[20] In a similar initiative, the 2013 budget of Nigeria, submitted to the National Assembly, also contained a proposal for the procurement of a Wise Intelligence Network Harvest Analyser System, an Open Source Internet Monitoring System and a Personal Internet Surveillance System.[21] All these are hi-tech online surveillance programmes. One would be able to fully appreciate how far-reaching this contract and other similar initiatives could be when it is considered in light of the level of internet penetration in Nigeria. Today, Nigeria records more than a 50 per cent internet penetration rate as against the position years ago when internet penetration was less than 10 per cent.[22] The same applies to many other sub-Saharan African countries, such as South Africa.[23]

There is credible evidence that other countries in sub-Saharan Africa are also developing similar online surveillance programmes. For example, a recent research carried out at the Munk School for Global Affairs at the University of Toronto revealed that countries such as Kenya were acquiring extensive internet surveillance and censorship programmes developed by Blue Coat. Blue Coat is an American company specialising in cyber security. Similarly, BBC recently reported that the Ugandan government has recently acquired a state-of-the-art surveillance technology which can be used to crush and

17 O Emmanuel 'Exclusive: Jonathan awards $40 million contract to Israeli company to monitor computer, internet communication by Nigerians' *Premium times* 25 April 2013 https://www.premiumtimesng.com/news/131249-exclusive-jonathan-awards-40million-contract-to-israeli-company-to-monitor-computer-internet-communication-by-nigerians.html (accessed 1 October 2017).

18 'Elbit Systems is a world leader in the fields of intelligence analysis and cyber defence, with proven solutions highly suitable for countries, armies and critical infrastructure sites.'

19 Emmanuel (n 17 above).

20 As above.

21 As above.

22 'Nigeria's internet users remain 90m in April – NCC' https://dailynigerian.com/business/nigerias-internet-users-remain-90m-in-april-ncc/ (accessed 1 October 2017).

23 South Africa also has about 52% penetration. See generally 'Freedom on the net 2016: South Africa country profile' https://freedomhouse.org/report/freedom-net/2016/south-africa (accessed 1 October 2017).

blackmail opposition.[24] Codenamed *Fungua Macho*, the Ugandan government adamantly denies the existence of the programme. An investigation by Privacy International (PI) titled Uganda's Grand Ambitions of Secret Surveillance further confirms this surveillance practice.[25] The investigation discloses that the Ugandan military procured a malware – FinFisher – by Gamma International GmbH (Gamma).[26] This malware, according to PI, is capable of collecting, modifying and extracting data communicated and stored on a device – say a computer or phone – once installed.[27] Thus, once installed, FinFisher can remotely transmit information to the operator. This technology can also be deployed to buildings, vehicles, computers, mobile phones, and so forth. Even if a user's device is encrypted, it cannot deter the function of the malware.

South Africa is also not left out in the electronic surveillance game. A recent report disclosed that the 'unregulated' National Communication Centre (NCC) also recently purchased a license for the sophisticated FinFisher.[28]

2.3 Rationale for increased electronic surveillance: National security as a mask

From the foregoing, two main rationales usually are put forth by governments to justify their increased surveillance activities. These are law enforcement and national security. With regard to law enforcement, the constitutions of most countries give the government and its security agencies wide law enforcement powers. National security reasons seem to be the most problematic. Commenting on the difficulties of national security justification, Navi Pillay, the former United Nations High Commissioner for Human Rights, observed:[29]

> How do we define the legitimate parameters for national security surveillance? Indeed, states may use targeted surveillance measures provided for example that such surveillance is case-specific, and on the basis of a warrant issued by a judge on showing of probable cause or

24 N Hopkins & J Morris 'UK firm's surveillance kit used to crush Uganda opposition' http://www.bbc.com/news/uk-34529237 (accessed 1 October 2017).

25 Privacy International (PI) *Uganda's grand ambitions of secret surveillance* https://privacyinternational.org/node/656 (accessed 1 October 2017).

26 PI *For God and my president: State surveillance in Uganda* https://privacyinternational.org/sites/default/files/Uganda_Report.pdf (accessed 1 October 2017).

27 As above.

28 H Swart *Communications surveillance by the South African intelligence services* February 2016 26 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (accessed 1 October 2017). See also P de Wet 'Spy wars: South Africa is not innocent' https://mg.co.za/article/2013-06-21-00-spy-wars-south-africa-is-not-innocent (accessed 1 October 2017).

29 Opening remarks by Ms Navi Pillay, United Nations High Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age, 24 February 2014, Palais des Nations, Geneva, Switzerland http://www.ohchr.org/EN/NewsEvents/Pages/ DisplayNews.aspx?NewsID=14276&LangID=E (accessed 1 October 2017).

reasonable grounds. However, the scope of national security surveillance in many jurisdictions has expanded significantly in recent years.

2.4 Normative framework regulating electronic surveillance in sub-Saharan Africa

Since the rule of law concerns doing things according to laid-down laws and procedure, it is important to identify the law and policy on electronic surveillance. In sub-Saharan Africa, the law and policy on electronic surveillance may be said to be contained in a combination of legal instruments. First, electronic surveillance is regulated by the provisions on the right to privacy in the constitutions of the countries since, in many cases, it is an unwarranted interference with the privacy of a person. The constitutions of countries in the sub-Saharan region provide for respect for the right to privacy in their Bills of Rights.[30] In some of these countries, such as Nigeria[31] and South Africa,[32] there is also well-developed jurisprudence on the protection of privacy through private law. Second, the provisions of international human rights instruments on privacy also regulate electronic surveillance.[33] Surprisingly, the African Charter on Human and Peoples' Rights (African Charter) does not contain a right to privacy. However, the right to privacy is found in the African Charter on the Rights and Welfare of the Child (African Children's Charter).[34]

A third category of legal instruments which has a direct bearing on electronic surveillance and which has been established specifically to regulate the gathering of personal information by electronic means, such as electronic surveillance, are data protection instruments. Since the ultimate goal of surveillance is to collect information which, in most cases, relate to or identifies an individual, these naturally will fall in the scope of data protection laws. In this respect, the sub-Saharan region has both international and domestic laws and policies. The African Union (AU) recently adopted the AU Data Protection Convention which specifically seeks to regulate some of the threats resulting from the advances in technology.[35] Other regional instruments on data protection have provisions affecting electronic surveillance, such as the Economic Community of West African States

30 Sec 37 Constitution of the Federal Republic of Nigeria, 1999; sec 14 South African Constitution, 1996; sec 27 Constitution of the Republic of Uganda, 1995.

31 See ES Nwauche 'The right to privacy in Nigeria' (2007) 1 *Review of Nigerian Law and Practice* 67.

32 See A Roos 'Data protection law in South Africa' in A Makulilo (ed) *African data privacy law* (2016) 196.

33 Art 12 Universal Declaration of Human Rights; art 17 the International Covenant on Civil and Political Rights (ICCPR).

34 See art 10 of the African Children's Charter http://www.achpr.org/instruments/child/#a10 (accessed 1 October 2017).

35 African Union Convention on Cyber Security and Personal Data Protection https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 1 October 2017).

(ECOWAS) Supplementary Act on Data Protection, the Southern African Development Community (SADC) Model Law, and so forth. Domestic data protection laws also regulate electronic surveillance in sub-Saharan Africa. Currently, only a few countries in the region have data protection instruments,[36] while a number of countries, such as Nigeria, still have data protection Bills before their legislative assemblies.

Electronic surveillance may also be regulated through the interception of communications legislation. Such legislation basically gives the government or security agencies powers to intercept individuals' communications under certain explicitly-stated circumstances, in most cases for the purposes of law enforcement. Examples are the South African Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002[37] and the Regulation of Interception of Communications Act 2010 of Uganda.[38] Nigeria currently does not have legislation on the interception of communication. However, a draft regulation of the Nigerian Communications Commission has that effect.[39] These laws are useful in that they provide for the permissible limit of surveillance.

Interception of communication or surveillance policies are found in other laws, especially emergency laws or national security laws. This is the case with laws on terrorism. For example, the Nigerian Terrorism (Prevention) (Amendment) Act 2013 provides for specific cases where there may be monitoring of communications of 'suspected' persons through the instrumentalities of electronic surveillance.[40] Similarly, the Kenyan National Intelligence Service Act 2012[41] gives security agencies the power to carry out surveillance under certain circumstances. The Ugandan Anti-Terrorism Act 2002 has a similar provision.[42] The same principles are also found in cybercrime legislation.

With regard to electronic surveillance specifically, the courts have not made any significant impact. Perhaps this is because infractions have not been identified and brought before the courts.

36 See G Greenleaf 'Global tables of data privacy laws and bills' (2017) 145 *Privacy Laws and Business International Report* 14.

37 Act 70 of 2002.

38 Act 18 of 2010.

39 Lawful Interception of Communications Regulations, http://www.ncc.gov.ng/documents/328-lawful-interception-of-comunications-regulations/file (accessed 1 October 2017).

40 Sec 29.

41 Sec 6(2)(c) National Intelligence Service Act 28 of 2012, http://kenyalaw.org/lex/rest//db/kenyalex/Kenya/Legislation/English/Acts%20and%20Regulations/N/National%20Intelligence%20Service%20Act%20No.%2028%20of%202012/docs/NationalIntelligenceServiceAct28of2012.pdf (accessed 1 October 2017).

42 The whole of Part VII of the Act provides for 'interception of communications and surveillance'.

Ideally, we may proceed on the assumption that the principles of the rule of law with regard to electronic surveillance can be found in the above-mentioned instruments. Nevertheless, it remains crucial to specifically establish the nexus between the rule of law and electronic surveillance.

3 Establishing the link between electronic surveillance and the rule of law

There is some uncertainty about the relationship between electronic surveillance and the rule of law as this has not been the subject of much academic discussion. Yet, the European Commission for Democracy through Law, in developing a rule of law checklist, listed (electronic) surveillance as one example of contemporary challenges to the rule of law.[43] To clarify this uncertainty, electronic surveillance raises two broad issues when considered in the context of the rule of law. The first is human rights issues, generally; the second is rule of law issues. We will consider these two issues in turn.

3.1 Human rights dimension: The right to privacy in perspective

While it may be impossible to identify all the elements of the rule of law with certainty, certain components seem to be globally accepted as indicators of the presence of the rule of law. These indicators are constitutionalism; the notion that the constitution controls the actions of government; an independent judiciary; and the requirement that the law must be fairly and consistently applied.[44] Others are the notion of transparency and accessibility of law; the efficient and timely application of the law; and respect for all categories of human rights.[45] Among all these elements, respect for human rights seems to be receiving the most attention. Therefore, it is not surprising that the UN Secretary-General defines the rule of law as

> a principle of governance in which all persons, institutions and entities, public and private, including the state itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, *and which are consistent with international human rights norms and standards.*[46]

From the above definition, it would seem that all other indicators must be subject to 'international human rights norms and standards'. This invariably means that respect for human rights is a *sine qua non* to the realisation of rule of law.

43 European Commission for Democracy through Law (n 2 above) 29.

44 See BM Hager *The rule of law: A lexicon for policy makers* (1999) 21-49.

45 As above.

46 United Nations Security Council (UNSC) Report of the Secretary-General *The rule of law and transitional justice in conflict and post-conflict societies* 4 http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2004/616 (accessed 1 October 2017) (my emphasis).

Although it would appear that there is general consensus that the respect for human rights is a fundamental pillar of the rule of law, there are contrary views. A strong argument exists against the inclusion of respect for human rights among the benchmarks for the rule of law. Tamanaha, for example, contends that the 'definition of the rule of law focuses only on law – it does not include democracy and does not include human rights'.[47] The scholar gives three reasons for his view, based on an analysis of the definition of the UN Secretary-General above. First, 'rule of law', 'democracy' and 'human rights' are 'separate elements that focus on different aspects of a political-legal system, which can exist separately or in combination'.[48] Each must, therefore, be understood on its own terms. Second, the notion of human rights is not an aspect of the rule of law as contending otherwise implies defining the rule of law in terms of institutions that match those of liberal democracies. This, in turn, suggests that the rule of law is only present in liberal democracies. Third, he argues, human rights cannot be included in the definition of the rule of law as it is contrary to the tenet of liberalism.[49]

Without a doubt, the argument of the scholar against the inclusion of human rights (and democracy) as a component of the rule of law seems convincing but, then, certain points must be appreciated. First, even in its initial conception by Dicey, human rights were envisioned as a core value of the rule of law.[50] Although there are modern applications of this concept, that does not mean one should totally derogate from its roots or the ideals in its conception. Secondly, it is difficult to argue for the presence of the rule of law in a state that does not respect human rights. Indeed, one of the aims of limiting power is to curtail arbitrariness which could lead to an abuse of human rights. In any case, there is a difference between the use of the term 'human rights' (which connotes the wide sense) and 'respect for human rights' (in the narrow sense). The concept of the rule of law actually anticipates the use of 'human rights' in the narrow sense. In this regard, Shivute notes:[51]

> It could be said that, in that parochial sense, the concept of *the rule of law* in itself says nothing of the justness and fairness of the laws. The upshot is that, if that narrow view is taken of the rule of law, states which do not respect human rights can carry on business as usual without the observance of the rule of law. But it is non-controversial that the rule of law is considered a prerequisite for democracy and democratic practice. It cannot, therefore, be contradicted that the rule of law plays a crucial role in the protection and promotion of human rights, democracy and good governance.

47 BT Tamanaha 'The history and elements of the rule of law' (2012) *Singapore Journal of Legal Studies* 233.

48 As above.

49 Tamanaha (n 47 above) 234.

50 AV Dicey *Introduction to the study of the law of the Constitution* (1915).

51 P Shivute 'The rule of law in sub-Saharan Africa: An overview' in N Horn & A Bösl (eds) *Human rights and the rule of law in Namibia* (2009) 214.

It is our view, therefore, that Tamanaha's contention is not in tandem with the ideals of the rule of law. In further support of this view, the Council of Europe (CoE), in developing benchmarks for the rule of law, rightly observed that the rule of law is linked not only to human rights but also to democracy.[52]

Much academic ink has been spilled on the nature and extent to which the right to privacy today has been severely under threat.[53] This has more to do with recent advances in technology and the increasing deployment of very intrusive technologies – 'privacy destroying technologies' – by governments and private entities alike. In view of this fact, one may safely argue that electronic surveillance constitutes one of the greatest challenges to the right to privacy (and other fundamental rights), hence to the rule of law, not only in advanced countries but also in developing countries. However, while advanced nations have taken significant strides to put governments under check and demand quality protection due to the high level of awareness, developing African states have not done so.

3.2 Rule of law dimension: Curbing arbitrariness of the state

An analysis of how electronic surveillance impacts on the rule of law naturally raise issues of privacy. However, one may argue that increasing electronic surveillance actually trumps mere privacy/human rights interests. It affects something greater. Some argue that to insist otherwise is to limit the impact which electronic surveillance has on society. Austin, for example, contends that '[t]he [electronic] surveillance debate … has to focus more on the deep reasons for this tension with the rule of law and less on the nature of the impact of such practices on individual privacy rights'.[54] Since the rule of law is all about curtailing the arbitrary use of power, perhaps one should consider electronic surveillance more in that light. Surveillance in itself has the capacity to bestow broad powers on governments, and, therefore, it should be considered in the context of the urgent need to curb the arbitrary powers of state authorities. From this perspective, electronic surveillance has much more to do with some other tenets of the rule of law, such as the principle of legality which anticipates that state actions are subjected to law. The next part will consider this broader impact of electronic surveillance in detail.

52 European Commission for Democracy through Law (n 2 above) 9.

53 See D Solove *The digital person* (2004). See also DJ Solove *Understanding privacy* (2008).

54 L Austin 'Surveillance and the rule of law' (2015) 13 *Surveillance and Society* 295.

4 Increasing use of electronic surveillance as a challenge to the rule of law in sub-Saharan Africa

The general attitude towards respect for the rule of law makes its realisation a mirage for countries in the sub-Saharan region. The newly-found penchant for electronic surveillance by state governments creates diverse challenges. However, how electronic surveillance becomes a challenge to the rule of law remains unclear. The fact that governments usually justify electronic surveillance with reference to law enforcement and national security further adds to these uncertainties. The next part analyses the specific challenges to the rule of law by electronic surveillance.

4.1 Impact on human rights and civil liberties

The human rights track record of most sub-Saharan African states is not a particularly bright one based on available reports. According to Freedom House, sub-Saharan Africa is home to most of the world's worst performing countries in terms of respect for human rights.[55] In the World Justice Project's rule of law index, most of the countries in the sub-Saharan region are the worst performers with regard to human rights.[56] The same scenario also emerges in the Amnesty International Report, where African states are said to have failed 'to convert rhetoric on human rights into action'.[57] Although these reports do not specifically consider surveillance *per se*, the fact remains that the state of human rights is poor, and increasing electronic surveillance will only worsen this.

Irrespective of the uncertainties, respect for human rights indeed is an essential component of the rule of law. Therefore, a threat to any human right certainly constitutes a challenge to the rule of law in the sub-Saharan region. Several human rights are threatened by electronic surveillance, although most commentators only consider the impact of surveillance on the right to privacy. The general argument with regard to electronic surveillance, especially 'covert' surveillance, is that it constitutes an unreasonable intrusion into individuals' private and family lives. This is particularly true for specific instances where the activities of individuals are monitored without any lawful justification

55 Freedom House *Sub-Saharan Africa* https://freedomhouse.org/regions/sub-saharan-africa (accessed 1 October 2017).

56 World Justice Project *Rule of law index* https://worldjusticeproject.org/sites/default/files/documents/RoLI_Final-Digital_0.pdf (accessed 1 October 2017). Eg, Ethiopia and Zimbabwe, respectively ranked 111 and 113 out of 113 countries, were subjected to the assessment.

57 See Amnesty International *Amnesty International Report 2016/17: The state of the world's human rights* (2017) 23 https://www.amnesty.org/download/Documents/POL1048002017ENGLISH.PDF (accessed 1 October 2017).

or authorisation by the courts. However, most of the laws that guarantee the right to privacy also make exceptions to this right.[58] This restricts the full realisation of the right.

The 'traditional' right to privacy arguably is affected more by the traditional form of surveillance, which includes the physical monitoring of a person. The modern form of surveillance, increasingly being used in the sub-Saharan region, impacts more on the aspect of privacy which has to do with personal information and falls within the scope of data protection law. Currently, however, there is a vibrant movement making the claim that data protection cannot be subsumed under the right to privacy.[59] The former is argued to be an independent *sui generis* right distinct from the latter. In fact, in many European countries and the European Union (EU), both rights are provided for separately. This article will not attempt to consider the merits of these arguments. What matters is that electronic surveillance which results in the collection, processing and use of personal information (that is, information which 'relates to' or 'identifies' a person) constitutes a greater challenge to human rights and thus a challenge to the rule of law. The 'processing' of personal information obtained from electronic surveillance carries specific risks.

Surveillance or dataveillance can have a 'chilling effect' on individuals, causing them to modify their behaviour. In this case, it is immaterial whether the person is actually being watched or not, provided there is the feeling that such a person could be watched. As aptly put by Lynskey, 'whether or not an individual is actually being monitored is not decisive in these circumstances: The mere perception of surveillance may be sufficient to inhibit individual behaviour.'[60] Specifically, such surveillance can hinder an individual's self-development because of the unconscious urge to conform to certain invisible codes or rules. As Richards puts it, surveillance threatens a value called 'intellectual privacy' which is a theory that suggests that new ideas are most likely developed away from intense public scrutiny.[61] It is here that Jeremy Bentham's famous Panopticon finds relevance.[62] Even if one is actually not being watched, that unconscious feeling that there is a possibility of being monitored has a

58 Eg, sec 37 of the Constitution of the Federal Republic of Nigeria 1999 guarantees the right to privacy, and this right is limited by the effects of sec 45.

59 See eg M Tzanou 'Data protection as a fundamental right next to privacy? Reconstructing a not so new right' (2013) 3 *International Data Privacy Law* 99; J Kokott & C Sobotta 'The distinction between privacy and data privacy in the jurisprudence of the CJEU and ECtHR' (2013) 3 *International Data Privacy Law* 222; LA Bygrave 'The place of privacy in data protection law' (2001) 24 *UNSW Law Journal* 277.

60 O Lynskey 'Deconstructing data protection: The "added-value" of a right to data protection in the EU legal order' (2014) 63 *International and Comparative Law Quarterly* 589.

61 NM Richards 'The dangers of surveillance' (2013) 126 *Harvard Law Review* 1946.

62 See JH Reiman 'Driving to the Panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future' (1995) 11 *Santa Clara Computer and High Technology Law Journal* 27 35.

significant impact on an individual's way of life. This definitely has an impact on the exercise of other rights guaranteed in a democratic society, such as freedom of liberty, association and assembly.

The UN recently acknowledged the potential impact of states' massive surveillance capabilities and its privacy implications in a General Assembly Resolution. Adopted in December 2013, the Resolution called on states 'to respect and protect the right to privacy', especially in the context of electronic surveillance and digital communications.[63] In a way, the Resolution effectively alerts states to take heed of their obligations to respect the rule of law, especially in their electronic surveillance practices.

Privacy, as stated earlier, is not the only right affected by the increasing use of electronic surveillance in sub-Saharan Africa. Other human rights are also under threat, either independent of privacy or because privacy is a gateway to the realisation of these rights.[64] In particular, electronic surveillance affects the right to freedom of association and assembly, freedom of thought, conscience and religion and freedom of expression.[65] For example, a report has shown that the Ugandan government under President Museveni's direction dismantled the post-election protest movement using surveillance spyware.[66] This same spyware was also used to supress free speech and legitimate freedom of expression.[67]

In recognition of the nexus between privacy and other human rights, the UN General Assembly, in a recent resolution on the promotion, protection and enjoyment of human rights on the internet, noted that 'privacy online is important for the realisation of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association'.[68]

Increased mass surveillance could lead to discrimination, thereby affecting the right against discrimination, which is equally guaranteed by the constitutions of countries in the sub-Saharan region.[69] The right against discrimination seems to be one of the most threatened human rights resulting from dataveillance. According to Roos, the information gathered may be incomplete, inadequate, accessed without authorisation or even destroyed.[70] Making a decision or

63 UNGA Resolution 68/167 The right to privacy in the digital age https://ccdcoe.org/sites/default/files/documents/UN-131218-RightToPrivacy.pdf (accessed 1 October 2017).

64 P Bernal 'Data gathering, surveillance and human rights: Recasting the debate' (2016) 1 *Journal of Cyber Policy* 245.

65 For more on this, see generally Bernal (n 64 above).

66 PI (n 26 above).

67 As above.

68 UNGA (n 63 above).

69 See sec 42 of the Nigerian Constitution; sec 4 of the South African Constitution.

70 A Roos 'The law of data (privacy) protection: A comparative and theoretical study' unpublished LLD thesis, University of South Africa 2003 6.

forming an opinion based on such erroneous details may lead to discrimination against an individual. Similarly, electronic surveillance facilitates profiling (like terrorism profiling) and dealing with an individual based on such a profile, with the high possibility of errors.

4.2 Lack of transparency

Because of national security and law enforcement justifications, electronic surveillance programmes usually are shrouded in mystery. This is why it is very difficult to document its practices. For example, it took a meticulous and bold media network to reveal the manner in which the former Nigerian President authorised the electronic surveillance of Nigerians' activities online. But for such a revelation, one would find it difficult to believe that this actually exists. Commenting on the problem of lack of transparency with regard to surveillance programmes, the former UN High Commissioner for Human Rights, Ms Navi Pillay, observed:[71]

> [T]he secretive nature of security surveillance in many places inhibits the ability of legislatures, judicial bodies and the public to scrutinise state powers. This lack of transparency, together with a lack of clear and appropriate limitations to surveillance policies and practices, creates serious obstacles to ensuring that these powers are not used in an arbitrary or indiscriminate manner.

No doubt, one of the essential principles of the rule of law is transparency in not only law and policy making, but also activities of the government. Indeed, the UN, in its definition of the rule of law, includes 'legal and procedural transparency'.[72] This also serves to further curtail the powers of potential autocrats. Transparency in government activities is a necessity in a democratic society. It also brings about accountability. Electronic surveillance naturally leads to abuse when one cannot even be aware of its existence, let alone question its rationale or the justification.

Transparency is one of the key principles of data protection law being a part of the fair information principles (FIPs). It is for this reason that some argue that the FIPs in data protection laws are not mere procedural requirements but aspects of the rule of law. Austin contends that the FIPs 'which underpin our data protection statutes, are better understood in rule of law terms than in terms of privacy'.[73]

---

71 See Ms Navi Pillay Opening remarks (n 29 above).

72 United Nations Security Council (UNSC) Report of the Secretary-General *The rule of law and transitional justice in conflict and post-conflict societies* 4 http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2004/616 (accessed 1 October 2017).

73 LM Austin 'Enough about me: Why privacy is about power, not consent (or harm)' in A Sarat (ed) *World without privacy?: What can/should law do* (2014) 131.

4.3 Restriction of judicial intervention and access to justice/lack of judicial oversight

Although it is difficult to find cases on electronic surveillance that have come before the courts in the sub-Saharan region, some inferences may be made from other jurisdictions since the approaches toward national security issues are basically the same. When it comes to anything that concerns national security, courts most likely will dismiss challenges to such programmes for lack of standing on the basis that mere surveillance creates no harm *per se*.[74] In any case, surveillance practices can only be challenged if they are known.[75] Similarly, in considering measures to curb criminal activities such as terrorism, members of the judiciary usually are sworn partners of the executive and would not want to be seen as an obstacle to the realisation of national security. This definitely amounts to a restriction on access to justice, which is one of the cardinal requirements of the rule of law. In this way, electronic surveillance, especially those justified for national security purposes, impinges on the rule of law in sub-Saharan Africa.

4.4 Prevalence of statutory exemptions and its impact on the rule of law

Even in enacting laws that have to do with upholding the rule of law in electronic surveillance practices, legislatures are quick to insert broad exceptions, sometimes for the flimsiest of reasons. This is not only true for provisions on fundamental human rights in the bill of rights, but also for other laws and policies on electronic surveillance. For example, after providing very extensive and robust principles on protection of personal information, the South African Protection of Personal Information Act (POPIA) provides that the processing of personal information (say by means of electronic surveillance) will not be considered in breach of the conditions stated if the Regulator[76] is 'satisfied' that 'the public interest in the processing outweighs, to a substantial degree, any interference to privacy of the data subject that could result from such processing'.[77]

Obviously frustrated by the ease in which the rule of law may be suspended in legislation, Sellers notes:[78]

> Scholars may sometimes advocate partial departures from the rule of law, or its incomplete realisation, or its differing application in different societies, because of transient or unfortunate circumstances, but no one can deny that every departure from the rule of law is a denial of justice.

74 See the US case of *Clapper v Amnesty International* 568 US 398 (2013).

75 Richards (n 61 above) 1934.

76 This is the public agency in charge of administering the South African data protection law.

77 Sec 37 Protection of Personal Information Act of South Africa 4 of 2013.

78 M Sellers 'An introduction to the rule of law in comparative perspective' in M Sellers & T Tomaszewski (eds) *The rule of law in comparative perspective* (2010) 9.

> The ultimate goal of every society and every legal system should be equal and impartial justice for all. *Imperia legume potentioraquam hominumesto.*

4.5 Electronic surveillance, the rule of law and independence of the judiciary

Recently in Nigeria, the rule of law was put to the test in relation to the requirement of independence of the judiciary or non-interference with the judiciary. There was a crackdown on 'corrupt' judges by security agencies. Part of the strategies adopted by the security agencies was the monitoring of their 'expensive' and 'luxurious' lifestyles, including the monitoring of their bank accounts and call logs. Their houses were raided at very odd hours. The Nigerian Judicial Council (NJC), the judicial regulator in the country, described the raids as 'the height of impunity' and an 'attempt to intimidate the judiciary'.[79] The NJC also seriously berated those acts and unequivocally stated that 'it will not allow the independence of the judiciary, or its impartiality to be mocked by the SSS [State Security Service] or any arm of government'.[80] In a sharp turnaround of events, one of the judges who was on the watch list was discharged and acquitted along with two other accused persons. In his ruling, the trial judge held that 'the prosecution has failed to establish any *prima facie* case against the defendants'.[81] The use of surveillance in this particular context raises a number of issues with respect to the rule of law in Nigeria. First, security agencies are willing to act on evidence emanating from surveillance with any serious investigation. Second, and more disturbing, is the fact that even the mere allegation of corruption which is not substantiated by credible evidence can be used as a basis for interference with judicial independence. Indeed, based on the evidence gathered from various sources, including electronic surveillance, these judges were suspended from office for quite some time.

The above should not be taken as being in support of corruption in the judiciary. The argument here is that placing heavy reliance on the evidence from electronic surveillance by security agencies could be a challenge to the rule of law, as is demonstrated by the discharge and acquittal of the judge mentioned above. In the case of clear unequivocal evidence, nobody will argue against the actions of security agencies or the government. For example, a situation similar to the Nigerian case also occurred in Ghana where an investigative journalist, Anas Aremeyaw Anas, used electronic surveillance material

79 E Okakwu 'NJC formally replies SSS, says arrest of judges "denigration of judiciary"' http://www.premiumtimesng.com/news/headlines/212733-njc-formally-replies-sss-says-arrest-judges-denigration-judiciary.html (accessed 1 October 2017).

80 As above.

81 CA Oloyede 'BREAKING: Justice Ademola, wife, SAN discharged, acquitted' *Daily Trust* 5 April 2017 https://www.dailytrust.com.ng/news/law/breaking-justice-ademola-wife-san-discharged-acquitted/192239.html (accessed 1 October 2017).

to implicate some senior judges in bribery scandals. Anas said that 'he ha[d] nearly 500 hours of video evidence on tape, showing judges allegedly asking for bribes and demanding sex'.[82] It was on the basis of this documentary evidence that 22 judges were suspended. In this case, there was no reason to question the use of electronic surveillance since the evidence was stated to be 'very clear' and 'incontrovertible'.

Overall, the state must be very careful in relying on evidence obtained from electronic surveillance when dealing with judges. Judges have a higher duty to the state and, as such, their independence must be jealously guarded. Besides, accusing judges of corruption based on unsubstantiated evidence obtained from electronic surveillance can lead to a loss of confidence by the public in the judiciary. In many cases, these judges are subjected to large-scale media trials. All these have a multi-dimensional impact on the rule of law in the county.

4.6 Propensity for massive abuse of power by government

One of the greatest dangers which electronic surveillance poses to the rule of law is the propensity for massive abuse of power by state authorities. This is all the more disturbing considering that most governments in the sub-Saharan region are working hard towards the harmonisation of the databases of the key public agencies. These databases of course will be easily accessible by a mere click, using unique identifiers on the internet. For example, the Nigerian President recently directed all agencies involved in the processing of biometric information to harmonise their databases.[83] This means that the government will effectively have almost every kind of information on its citizens which is hosted on clouds on the internet. This situation naturally gives the government untold powers over its citizens with a high probability of abuse. Indeed, it has been rightly noted that 'government surveillance of the internet is a power with the potential for massive abuse. Like its precursor of telephone wiretapping, it must be subjected to meaningful judicial process before it is authorised.'[84]

The threat which these harmonised databases pose, coupled with the possibility of monitoring, is one dimension to this challenge. It must also be considered that such electronic databases can also be a source of danger to individuals, especially if they are accessed by

82 'Ghana suspends High Court judges after Anas Aremeyaw Anas' film' http://www.bbc.com/news/world-africa-34452768 (accessed 1 October 2017).

83 These agencies include NIMC, FRSC, NCC and INEC. See N Ibeh 'FRSC, NIMC to harmonise biometric data' https://www.premiumtimesng.com/news/more-news/189110-frsc-nimc-to-harmonize-biometric-data.html (accessed 1 October 2017). Some agencies have already complied; see NIMC 'NIMC and INEC comply with presidential directive on harmonisation of biometric data: Set up joint technical committee'https://www.nimc.gov.ng/nimc-and-inec-comply-with-presidential-directive-on-harmonisation-of-biometric-data-set-up-jointtechnical-committee/ (accessed 1 October 2017).

84 Richards (n 61 above) 1961.

unscrupulous persons or foreign governments. Such 'big data' facilitates 'mass surveillance' and exposes individuals to other unanticipated risks. It is probably the realisation of the potential dangers of these databases that data protection instruments hold data controllers (in this case, the government) to task when it comes to the standard of security safeguard of electronic databases. For example, the South African POPIA requires strict protection of the information in the hands of the government based on sections 19 to 22.[85] Regionally, the AU Data Protection Convention also requires in article 21 that state governments 'must take all appropriate precautions, according to the nature of the data, and in particular, to prevent such data from being altered or destroyed, or accessed by unauthorised third parties'.

4.7 Increase in asymmetric relationship between the people and the government

For the rule of law to prevail in a society, there has to be some form of evenness between the government and the governed. The authority the state wields over the people itself is enough to always tilt power in its favour. The rule of law, therefore, seeks to ensure that this critical balance is maintained irrespective of the inherent powers of the state. When a government has substantial information about its people and is willing to gather more, this will definitely tilt power in favour of the government. As it is often said, 'information is power and more information is more power'. Electronic surveillance has the intrinsic capability of generating so much information for the government in this era of 'big data'. This is more disturbing in view of the significant efforts made by state governments to harmonise their databases. In this regard Richards observes:[86]

> A second special harm that surveillance poses is its effect on the power dynamic between the watcher and the watched. This disparity creates the risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement, where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance.

The foregoing has shown how electronic surveillance impacts on the rule of law in sub-Saharan Africa. The next part considers how to entrench the rule of law in the practice of electronic surveillance.

85 Protection of Personal Information Act 4 2013.
86 Richards (n 61 above) 1935.

5 Measures to entrench the rule of law in electronic surveillance and the challenges for sub-Saharan African states

While admitting that electronic surveillance is sometimes necessary for national security, its overwhelming challenges to the rule of law cannot be casually dismissed. Therefore, the question is how the principles of the rule of law can be infused into current practices to ensure that 'it does not provide the state an unlimited power to control the life of individuals'.[87] Various mechanisms are available to curtail the powers of governments in surveillance practices.

First, there is the need for countries in sub-Saharan African to reconsider and take seriously their international obligations. Scholars have re-emphasised the significance of international and regional frameworks in entrenching the culture of the rule of law in a country. As mentioned earlier, there is no internationally-binding treaty on electronic surveillance. However, scholars are increasingly calling for one as electronic surveillance doubtlessly is one issue which requires a concerted action at a multilateral level, especially because of its foreign dimension. Deeks, for example, using the international relations theory, argues that

> [s]tates turn to international law to achieve different goals, including overcoming collective action problems, co-ordinating on issues that inherently require a multilateral approach, and signaling [sic] normative commitments. Whether one looks at the problem from a realist, institutionalist, liberalist, or constructivist perspective, there is reason to think as a positive matter that current conditions are ripe for states to employ international law to regulate foreign surveillance.[88]

Quite convincing arguments were put forth by the above scholar for such an international legal framework. The justifications include the ability of states to collectively set the agenda, lessen the pressures on human rights fora and signal an underlying commitment to accountable government.[89] Nevertheless, one has strong reasons for being sceptical about the possible emergence of an international legal framework on surveillance. Electronic surveillance issues have to do with the right to privacy, and regulating privacy has over the years been a source of serious controversy. It goes without saying that when it comes to surveillance, the power brokers in the world are far from agreeing on what privacy means and how it should be protected. In this regard, for example, we find that the approach of the United States and the EU are poles apart.[90] Considering the influence of both

87 European Commission for Democracy through Law (n 2 above).
88 Deeks (n 6 above)
89 As above.
90 For more on these, or differences even among Western states, see JQ Whitman 'The two Western cultures of privacy: Dignity versus liberty' (2004) 113 *Yale Law Journal* 1151.

jurisdictions in international politics, it is unlikely that countries in sub-Saharan Africa can campaign for the adoption of an international instrument of electronic surveillance.

While we await such an internationally-binding treaty, it must be stated that there are several international instruments that create binding obligations on sub-Saharan African states in relation to electronic surveillance.[91] The critical challenge for the rule of law, however, is the sub-Saharan states' unreceptive attitude towards international obligations. First, the ratification of the necessary international and regional treaties is a major problem. For example, since the adoption of the AU Data Protection Convention in 2014, only seven sub-Saharan countries have signed this Convention[92] and one has ratified it.[93] Another example of this unreceptive attitude towards international obligations, and which borders directly on online surveillance, is South Africa's action in voting against the recent UN Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet in July 2016.[94] The efforts by some sub-Saharan African states to ratify the CoE's Data Protection Convention, which is the only international binding instrument of data protection, however, is noteworthy and commendable.[95] Second, states rarely comply with the obligations created by such instruments even when they eventually ratify them. In fact, compliance with international instruments is an obvious challenge to most African states. In this regard, Viljoen notes that 'the greatest challenge [in Africa] is to bring about compliance with the treaty provisions by government officials and nationals alike'.[96] The dualist approach to international agreements in most sub-Saharan African states further compounds this problem.[97] For an international treaty to be binding and enforceable in a state, it must not only be ratified but must be domesticated.[98]

91 As discussed in part 2.4 above.

92 See https://www.au.int/web/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_.pdf (accessed 30 September 2017).

93 Only Senegal, based on records made available by the AU. This is another clear example of the unreceptive attitude toward privacy.

94 'Freedom on the net 2016' (n 23 above).

95 Sub-Saharan states such as Mauritius, Senegal, Burkina Faso and Cape Verde. See generally AB Makulilo 'African accession to Council of Europe Privacy Convention 108' (2017) 41 *Datenschutz und Datensicherheit – DuD* 364-367.

96 F Viljoen *International human rights in Africa* (2012) 25.

97 For more on the problems of attitude towards African states to international legal obligations, especially in relation to data protection, see LA Abdulrauf & CM Fombad 'The African Union Data Protection Convention: A possible cause for celebration of human rights in Africa' (2016) 8 *Journal of Media Law* 67.

98 See eg sec 12 of the Nigerian Constitution.

In all, it must be re-emphasised that while the right to privacy under international human rights law is not absolute, any instance of interference must be subject to a careful and critical assessment of its necessity, legitimacy and proportionality.[99] This justifies the need for independent oversight and enforcement institutions and a strong judiciary.

Besides international instruments as a means of curbing the excesses of arbitrary states in electronic surveillance practices, other measures are available. Constitutions also have a key role to play. Indeed, the constitution is probably the strongest instrument to foster the rule of law. This fact is further confirmed by constitutions like that of South Africa where it provides, in section 1(c), that South Africa is founded on the supremacy of the Constitution and the rule of law. Constitutions, in their guarantee of the right to privacy, also constitute one of the measures for the regulation of electronic surveillance. Therefore, electronic surveillance must not only be carried out with respect for the rule of law, but also for the right to privacy contained in the constitution. However, there are two main challenges in this respect: The first is the national security justification. Most constitutions, although guaranteeing the right to privacy, provide derogations, which are usually unreasonably relied upon by the government and its security agencies. However, it has been stated that 'it is not acceptable to use national security concerns as a blanket justification to excuse unwarranted privacy breaches'.[100] A second challenge with constitutions as a means of fostering the rule of law in electronic surveillance practices in sub-Saharan African is well captured by a commentator in the following terms:[101]

> Although many African countries have excellent constitutions providing for the protection of fundamental rights and freedoms, it is disheartening to note that these rights are in some instances not respected in reality. Wanton disregard of the rights of the citizenry, principally by the executive, is a phenomenon which can be noted amongst some African states. This situation ultimately stems from skewed implementation of the separation of powers doctrine, characterised by timid judiciaries and legislatures run by the executive.

Yet another measure to infuse the rule of law principle in electronic surveillance in sub-Saharan Africa is a clearly-drafted surveillance law (or provisions). According to Dicey, one of the foundations of the rule of law is that states must consider making laws which sincerely show a willingness to limit the discretion of public officials.[102] These rules must also be made as clear and as transparent as possible. It goes without saying that incorporating the rule of law in surveillance

99 Ms Navi Pillay 'Opening remarks' (n 29 above).

100 A Gwagwa & A Wilton 'Protecting the right to privacy in Africa in the digital age' http://www.hrforumzim.org/wp-content/uploads/2014/06/Protecting-the-right-to-privacy-in-Africa-in-the-digital-age.pdf (accessed 1 October 2017).

101 Shivute (n 51 above) 218.

102 Dicey (n 50 above).

practices requires that the laws and policies are clear as legal certainly itself is one of the benchmarks for the rule of law.[103] A major problem with respect to laws and policies on surveillance, according to the UN Special Rapporteur, is that they are obsolete and hardly ever clear.[104] For example, as noted above, none of the normative framework defines 'electronic surveillance' in spite of it wide usage.

One more point to note with regard to the law regulating surveillance is the significance of data protection instruments. It is apposite to state that data protection instruments are more properly placed to ensure that surveillance is carried out in accordance with the rule of law. Indeed, most of the discourses on surveillance and the law are carried out within the context of privacy and data protection.[105] This is not surprising, considering that in most cases surveillance involves the accumulation of personal information which falls within the scope of data protection law. Furthermore, data protection instruments contain principles such as legality and proportionality which are ordinarily meant to foster the rule of law. What this implies is that all African states must attempt to put in place data protection instruments based on their obligations under the AU Convention on data protection and other regional treaties.

Third, independent data protection authorities/agencies (DPAs) are indispensable in fostering the rule of law regarding electronic surveillance in Africa. This point is justified by the fact that authors are increasingly identifying independent enforcement institutions as paramount for democracy and constitutionalism in Africa.[106] Regarding electronic surveillance, no institution is better placed to curb the excesses of state governments than truly independent DPAs. This is so for two reasons: First, DPAs, by their architecture, are supposed to be composed of specialists in identifying when an information processing programme is *ultra vires.* Second, they are

103 European Commission for Democracy Through Law (n 2 above).

104 'Legal standards are either non-existent or inadequate to deal with the modern communications surveillance environment. As a result, states are increasingly seeking to justify the use of new technologies within the ambits of old legal frameworks, without recognising that the expanded capabilities they now possess go far beyond what such frameworks envisaged. In many countries, this means that vague and broadly conceived legal provisions are being invoked to legitimise and sanction the use of seriously intrusive techniques' UNGA *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,* Frank La Rue para 50 13 http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed 1 October 2017) 50-51.

105 See Solove (n 53 above); Bernal (n 64 above); Tzanou (n 14 above).

106 See eg CM Fombad 'The role of emerging hybrid institutions of accountability in the separation of powers scheme in Africa' in CM Fombad (ed) *Separation of powers in African constitutionalism* (2016) 325.

independent of government to ensure objectivity in their actions.[107] Even the UN General Assembly in a resolution called on states

> [t]o 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.[108]

Similarly, Navi Pillay drew attention to the challenge of infusing the rule of law principles in electronic surveillance without an effective enforcement mechanism.[109] She contended that 'a lack of effective oversight and review to monitor compliance and enforcement contributes to a lack of accountability for arbitrary or unlawful intrusions on the right to privacy'.[110] She further expressed the view that 'internal safeguards without independent, external monitoring are ineffective against the abuse of surveillance methods'.[111] With regard to external monitoring specifically, the AU has been criticised for adopting a data protection treaty without specific provisions for a region-wide monitoring institution.[112]

A fourth measure is the need for a strong judiciary. Indeed, while there are no settled approaches in realising the rule of law, the role of a strong judiciary is incontrovertible.[113] Therefore, judges and courts must recognise their crucial role as agents in promoting the rule of law. They should also be protectors of rights and liberties while upholding the law. This may be somewhat problematic for the rule of law, as observed by Graver, as 'sometimes these two expectations are in conflict'.[114] What should a judge do when faced with an electronic surveillance regulation (for national security purposes) which affects human rights and civil liberties? Should they uphold the law or let human rights prevail? According to Graver, 'the judge has to choose whether to side with the legislator or to side with the ideals of the rule of law'.[115] This means that the court must act according to three principles which are essential to a judiciary committed to the rule of

107 See G Greenleaf 'Independence of data privacy authorities: International standards' (2012) 28 *Computer Law and Security Review* 3; G Greenleaf 'Independence of data privacy authorities: International standards and Asia-Pacific experience' (2012) 28 *Computer Law and Security Review* 3.

108 UNGA (n 63 above).

109 Ms Navi Pillay 'Opening remarks' (n 29 above). See art 10 http://www.achpr.org/instruments/child/#a10 (accessed 1 October 2017).

110 As above.

111 As above.

112 See Abdulrauf & Fombad (n 97 above) 91.

113 HP Graver *Judges against justice: On judges when the rule of law is under attack* (2015) 1, where Graver elaborately considered the role of the judge when confronted with autocratic or oppressive rules. See also SD O'Connor 'Vindicating the rule of law: The role of the judiciary' (2003) 2 *Chinese Journal of International Law* 1.

114 As above.

115 As above.

law: independence, integrity and competence.[116] It is also submitted that this kind of situation calls for judges to be meticulous and proactive.

Fifth is the role of civil society organisations (CSOs), non-governmental organisations (NGOs) and the media. In the words of Shivute:[117]

> These organisations play a crucial role as they take on the responsibility of being watchdogs, tasked with ensuring that governments live up to their obligations. It goes without saying that critical voices are a necessary component to any democratic state.

There are several CSOs and NGOs that play the critical role of infusing the rule of law in surveillance practices of the government. The role of the media also cannot be overemphasised. Together, all these institutions have helped to expose the surveillance programmes of governments in the sub-Saharan region which, as observed earlier, are covert in nature. In particular, the role of CSOs such as the Electronic Frontier Foundation (EFF);[118] the Electronic Privacy Information Centre (EPIC);[119] Privacy International (PI);[120] and Global Internet Liberty Campaign (GILC),[121] is noteworthy.

In concluding this section, it is important to make two points. First, the tension between surveillance and the rule of law can be significantly reduced if it is not used as an instrument of first resort. Thus, electronic surveillance as an investigative tool in the context of law enforcement should only be used when other 'less intrusive means have proven ineffective or when there is no reasonable alternative to obtain crucial information or evidence'.[122] Second, surveillance practices must comply with the principles of necessity and proportionality. In this regard, the International Principles on the Application of Human Rights to Communications Surveillance is noteworthy.[123] This is a set of principles resulting from a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology. The principles are legality; legitimate aim; necessity; adequacy; proportionality; competent judicial authority; due process; user notification; transparency; public oversight; integrity of

116 O'Connor (n 113 above) 1. According to O'Connor, '[d]espite the important differences among nations, and legal systems, these bedrock principles have proven themselves indispensable in upholding the rule of law'.

117 Shivute (n 51 above) 218.

118 https://www.eff.org/ (accessed 1 October 2017).

119 https://epic.org/# (accessed 1 October 2017).

120 https://www.privacyinternational.org/ (accessed 1 October 2017).

121 See http://gilc.org/ (accessed 1 October 2017).

122 UNODC (n 7 above).

123 Otherwise called the 'Necessary and Proportionate Principles' or '13 Principles'. This is a set of 13 principles which came out from a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology.

communication and systems; safeguards for international co-operation; and safeguards against illegitimate access.[124] In a nutshell, it is submitted that these principles appropriately embody the idea of the rule of law in respect of electronic surveillance.

6 Conclusion: The future of electronic surveillance and the rule of law in sub-Saharan Africa

The above has made one point clear, namely, that the increasing use of electronic surveillance significantly undermines the rule of law in sub-Saharan Africa and this seems to be taken for granted by both the people and the governments. It has been argued that the debates with regard to the link between electronic surveillance and the rule of law far transcend privacy intrusions. The rule of law itself is an independent democratic ethos which is also significantly affected in that surveillance gives states (or individual surveilling) untold powers which is susceptible to abuse. This is true especially when presented with a national security justification. As most reports show, the rule of law has not fared well in sub-Saharan Africa, although no serious consideration has been given to the kind of threats electronic surveillance poses to rule of law. Yet, it is obvious that any further analysis of the rule of law in sub-Saharan Africa must pay specific attention to the impact of increasing electronic surveillance. There is no better time for that to be done in the region than now.

124 International Principles on the Application of Human Rights to Communications Surveillance https://www.eff.org/files/necessaryandproportionatefinal.pdf (accessed 1 October 2017). For more on the principles, see EFF *Necessary and proportionate: International principles on the application of human rights law to communications surveillance* http://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf (accessed 1 October 2017).