THE REGULATORY DILEMMA ON MASS COMMUNICATIONS SURVEILLANCE AND THE DIGITAL RIGHT TO PRIVACY IN AFRICA: THE CASE OF SOUTH AFRICA

DORCAS BASIMANYANE*

I. INTRODUCTION

In the pursuit of maintaining national security, African governments and telecommunications corporations constantly curtail the digital right to privacy. The right to privacy is protected under many international human rights instruments ratified by African states and is enshrined in many of their constitutions. Yet the same states continue to acquire mass surveillance infrastructure to embark on indiscriminate harvesting, interception of communications, transmission, analysing and storage of individuals' personal data and private information, without having adequate safeguards. To cover their tracks, governments continue to enact laws governing national security, terrorism, telecommunications, cybersecurity, and foreign and financial intelligence units that are more state interest focused than human rights based.

It is arguable that the entire electronic surveillance architecture under which the intelligence security services and law enforcement officials operate lacks a clear legal basis. The aforesaid lies behind the contention that surveillance laws are often passed without adequate public participation by all stakeholders and some, disputably, have not gone through the required transparent open review and scrutiny by the public.[1] Most African surveillance laws also fail to institute adequate safety and accountability controls or mechanisms that would prevent misuse of data by controllers.[2] All that is known about the surveillance legal

* Dorcas Basimanyane is a Doctoral Researcher and Project Coordinator for the Advanced Human Rights Courses Project at the Centre for Human Rights, University of Pretoria. Her LLD research is focused on Legal and Human Rights challenges of mobile and internet technology developments in Africa.

1 *The Surveillance State: Communications Surveillance and Privacy in South Africa* was produced by the Media Policy and Democracy Project for the Right2Know campaign, March (2016) 8.

2 The South African RICA fails to criminalise the illicit activities of the technology service providers and law enforcement officials tasked with the enforcement of the Act.

frameworks and the architecture is that they are for the public good: they promote national security and the fight against terrorism.

Against this background, the article proceeds by establishing the justifiability of the enduring unregulated practices of mass electronic communication surveillance in the Republic of South Africa as to whether they coincide with the proportionality test prescribed by international human rights law. Before delving into this, the article highlights the legal recognition of privacy in international and regional human rights instruments as well as South Africa's domestic law. Further, the article uses the famous metaphors of George Orwell's Big Brother[3] and Jeremy Bentham's Panopticon as further developed by Michel Foucault to discuss the intrusive impact of digital surveillance on the right to privacy. The article also highlights some surveillance and national security international best practices, laws and jurisprudence in order to come up with propositions on the necessary legal reforms in RICA, with the purpose of addressing the existing South African regulatory dilemma between individuals' right to digital privacy and national security.

II. PHILOSOPHICAL OVERVIEW: 'BIG BROTHER AND THE PANOPTICON'

The pervasiveness of modern intensive mass surveillance activities and their impact on civil liberties cannot be explained better than through the famous metaphors of Orwell's Big Brother[4] and Jeremy Bentham's Panopticon by Michel Foucault.[5] Orwell envisioned surveillance in a futuristic nation, where citizens are monitored in their homes by a telescreen, a device that both projects images and records behaviour in its field of vision.[6] He envisioned the extensive monitoring efforts being coordinated by the 'thought police' as agents of a centralised totalitarian state, which primarily uses surveillance to maintain social order and conformity.[7]

Michel Foucault, on the other hand, building upon the works of Orwell above, focuses primarily on the behavioural inhibitions arising from constant and focused observation. He unveils the mysteries of invisible and anonymous extended state authority over individuals through the panopticism philosophy.[8] He confirms through this theory that in the modern digital surveillance era individuals can never be free and governments have an outrageous power over the lives of citizens through the information they collect from them and the power of observation.[9] His

3 G. Orwell, *Nineteen Eighty-four* (1949) Free eBooks at Planet eBook.com. Available at: <https://www.planetebook.com/free-ebooks/1984.pdf> (accessed 21 March 2019).

4 *Ibid.*

5 J. Bentham, *The Panopticon Writings* (Verso, 1995) 29–95.

6 *Ibid*.

7 *Ibid*.

8 A. Brunon-Ernst, *Beyond Foucault: New Perspectives on Bentham's Panopticon* (Ashgate, 2012) 2.

9 *Ibid*.

ideas were building on the original *panopticon philosophy* formulated by Jeremy Bentham.[10]

In his work titled *Discipline and Punish*, Foucault uses the Panopticon as a metaphor to explain the government's power of surveillance over the citizens as a form of modern discipline and punishment.[11] Thus it has literally replaced the old and seemingly humiliating, tormenting and visible physical punishment of torture with a rather in-depth, invisible and anonymous punishment which can now penetrate the heart, the will and the inclinations of individuals.[12] According to him, in this shift from the physical punishment, governments extend their power of control to now include monitoring even the inner lives of the individual which makes the punishment even more rigorous than the old physical punishment of torture.[13]

In modern societies, according to Foucault, where the physical punishment was to last for a short period of time, it now lasts for a lifetime. He states that this modern type of discipline and punishment through knowledge control and observation has turned individuals into docile nationals who do not have the power to question the acts of their governments but only support them.[14] In this way, modern society attests to the original panopticon philosophy as developed by the philosopher Jeremy Bentham above as a model for the new type of prison.[15]

In the panopticon, there is a guard tower surrounded by a ring of cells and all that is necessary is to place a supervisor in a central tower and close up the whole prison.[16] In each prison cell, there is a schoolboy, a worker, a condemned man, a madman and a patient. All information about them has been harvested and stored in the safes. The supervisor on top of the tower will then be able to see all the inmates at all times and what they are doing but the inmates are not able to see him, nor can they collectively cooperate with each other in order to resist authority exercised over them.[17] On one hand, the fact that the guards can always see the inmates induces in them a state of conscious and permanent visibility that assures the automatic functioning of power over the inmates. On the other hand, the inmates in fear of being observed will always obey and follow what they are expected to do.[18]

Authority is always omnipresent and anonymous in the sense that the public will never know who is observing them, and that power depends on the citizens knowing they are under observation all the time.[19] In this case, the harvesting and processing of knowledge collection and the power to observe and isolate the people displace that physical infliction of pain which is the central aim of

10 *Supra*, note 5.
11 M. Foucault, *Discipline and Punish: The Birth of the Prison* (Penguin, 2012) 195–317.
12 *Ibid.*
13 *Ibid.*
14 *Ibid.*
15 *Ibid.*
16 *Supra*, note 5.
17 *Ibid.*
18 *Ibid.*
19 *Ibid.*

the social discipline with an invisible and a particular type of highly invisible anonymity type of punishment which targets the mind and the souls of people.[20]

The models above explain the truism of the power of surveillance in the modern era of technological advancements. The states having information of all the people extend their power to control them automatically.[21] According to this philosophy, power is not exercised over those in the prison cells only but even all those outside the prisons are still subject to an observation intended to tame them which can be referred in modern times as extraterritorial surveillance.[22]

These metaphors bring to the fore an understanding that modern developments found to be liberating, such as internet space and mobile technological developments, are in fact enhancing states' power of control even in the liberal democratic states.[23] The panopticon shows how in modern times control and punishment, which are invisible and less painful, turn up to be in actual fact the most rigorous.[24] The power of control through observation also has a discriminatory impact, in that its burdens do not fall on everyone equally, for individuals placed in categories such as Muslims, Arab and non-citizens through information collected about them becomes more coercive and stronger than those who do not fall in these groups.[25]

The cohesion among the two theories above is their strong emphasis on the rigorous nature of surveillance mechanisms on the freedoms of human people. Modern observational and informational collection activities totally destroy one's anonymity. They make every individual to indiscriminately become an unremarked part of the undifferentiated world against their own will, which buttresses the standpoint that surveillance practices are oppressive even where the intentions that underlie them are inherently benign.

However, the visible dearth of both theories as captured under the concept of the *surveillant assemblant* by Hergetty and Ericson[26] is the failure to recognise the effects of the now prevailing strong invisible hand of the private sector or the multinational corporations in modern surveillance activities. The above only suggests a stable top-down scrutiny which recognises the government as the sole actor in its surveillance activities. Whereas in Africa the reality remains that governments do not always have such an adept capacity to conduct mass digital communications surveillance, as such they use the private sector. The prevalent mass surveillance unconstitutional powers in Africa indisputably impose a gross intimidating effect on political activism, protest, debate and investigative

20 S. Horowitz, 'Foucault's Panopticon: A Model for NSA surveillance?', in R. Miller, *Power and Privacy: A Transatlantic Dialogue in the Shadow of the NSA Affair* (Cambridge University Press, 2017) 39–62.

21 *Ibid.*

22 *Ibid.*

23 *Ibid.*

24 D. Lyon, '*From Big Brother to the Electronic Panopticon.' In The Electronic Eye: The Rise of Surveillance Society* (University of Minnesota Press, 1994) 57–80.

25 *Supra*, note 5.

26 K. Hargetty and R. Ericson, 'The Surveillant Assemblage', 51 (4) *British Journal of Sociology* (2000) 605.

journalism as well as the practice of human rights law.[27] The citizens have become docile and only live according to the commands of autocratic governments.

Clarke[28] defines surveillance as 'the systematic investigation or monitoring of the actions or communications of one or more persons'. He highlights that, while freedom from tyranny is a sign of democracy, surveillance remains an element of tyranny. It conjures up cruel visions of spies, totalitarianism over individuals and suppression of ideas.[29] Greenwald[30] equates surveillance to a one-sided mirror, capable only of revealing the personal lives of citizens without them being able to see what the government does. Accordingly, surveillance creates the ultimate imbalance, which allows the most dangerous of all human conditions: the exercise of unlimited power without transparency and accountability.[31] By the meaning of a civil government and the social contract John Locke must have meant[32] a case where public officials serve the people in a transparent and accountable manner, hence the name 'public servants'. Therefore privacy – as any other inalienable fundamental natural right – can only belong to the private individual, not the government.

III. THE WAKE OF EDWARD SNOWDEN'S REVELATIONS ON MASS SURVEILLANCE PRACTICES BY THE STATES IN 2013

Surveillance measures globally intensified after the 9/11 terrorist attack as a means to counter the war against terror. However, other countries which were never the victims of the terrorist attacks also reviewed their communications surveillance measures for different reasons.[33] South Africa, for instance, at the time faced a massive crime wave that threatened social order, which consequently led to the enactment of the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) and the augmentation of their surveillance measures.[34] Later, evidence revealed that these measures were being inappropriately used: instead of being utilised to curb crime, they became weaponised to target politicians, business people and dissent.[35] One example is the revelation on the usage of the Intelligence Service's mass communication surveillance operations, unlawfully employed to intercept the phone calls of leading figures in the then Scorpions around the mid-2000s in their cause to

27 *Ibid*.

28 R. A. Clarke, 'Information Technology and Data Surveillance', 31 *Communications of the ACM* (1988) 499.

29 *Ibid.*

30 G. Greenwald, *No Place to Hide: Edward Snowden, the NSA, and Surveillance State* (Metropolitan Books, 2014) 619.

31 *Ibid.*

32 M. E. Laskar, 'Summary of Social Contract Theory by Hobbes, Locke and Rousseau', *SSRN Electronic Journal* (2013) 4. DOI 10.2139/ssrn.2410525.

33 J. Duncan, *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa* (Wits University Press, 2018) xviii.

34 *Ibid.*

35 Right 2 Know <https://www.r2k.org.za/2016/05/05/6594/> (accessed 20 May 2020).

finalise corruption charges against Jacob Zuma during his ascendency to the Presidency,[36] while in 2010 the Crime Intelligence Division (CID) of the South African Police Service (SAPS) was allegedly ordered to conduct surveillance on certain *Sunday Times* investigative journalists.[37]

In 2013, matters related to surveillance became amplified in the wake of Edward Snowden's revelations about the global surveillance programme (PRISM) of the US National Security Agency (NSA).[38] The former Central Intelligence Agency (CIA) employee's exposé revealed that the US and UK governments unconstitutionally operated the PRISM programme to harvest enormous amounts of personal information of billions of people from around the world on a daily basis from the databanks of Apple, Microsoft, Facebook and others, behind the cloak of anti-terrorism and national security.[39]

Similarly, many African governments have established mass surveillance of the scale revealed by Snowden, programs capable to gather, store and process enormous data, let alone the tapping of mobile phones and hacking of social network accounts of journalists, researchers and individual citizens. This shows that, the African governments' weakness of blind copying western culture and laws did not bypass the practices of intrusive surveillance.

In Botswana, for instance, in 2017, amid an outcry for insufficient funding and resources for development, the government could afford to finance a P10 billion safer city project for the Botswana Police Services and the Directorate of Intelligence and Security Services (DISS).[40] There was also a reported leakage of a 19-page document containing details of intrusive surveillance technology called Fin fisher GmbH developed by a Munich hacking firm which was to infect thousands of computers and mobile phones countrywide with malware implants, solely to enable the DISS to tenuously monitor journalists' and politicians' smartphones and computers on a mass scale.[41]

The Munich spy firm above, which prides itself as the best and number one in the world, is said to have done similar deals with many other African countries such as Egypt's Hosni Mubarak regime, Ethiopia and Nigeria in the past.[42] For more support, the government has also established some close affiliations with an Israeli company by the name of Verint, which supports several governments with software adept at spying on emails and social media accounts such as Facebook and Twitter.[43]

36 *Ibid*.

37 *Ibid.*

38 T. C. Sotteck and J. Kopfstein, 'The Verge: Everything You Need to Know about PRISM, 17 July 2013. Available at <https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet> (last accessed 20 June 2019).

39 *Ibid.*

40 *Ibid.*

41 Botswana Guardian, 'DIS Launches a Massive Surveillance Programme', available at <http://www.botswanaguardian.co.bw/news/item/1284-dis-launches-massive-surveillance-programme.html> (last accessed 23 February 2019).

42 *Ibid.*

43 *Ibid.*

In South Africa, a 2013 exposé by Privacy International revealed that, despite unending poverty, the South African government allocated public funds to Vashtech (SA) Pty Ltd, a company that sells mass surveillance technologies.[44] Recently, the government employed a company by the name Vumatel, which as of March 2019 had reportedly installed 889 CCTV cameras in 48 Johannesburg suburbs, and expected to complete the project by 2020. Altogether the project is estimated to have cost the South African government an amount of R500 million.[45] The recent study conducted by the Wall Street Journal[46] also revealed that one of China's giant technology companies, Huawei, is continuously spreading intrusive surveillance measures on the continent – including artificial intelligence surveillance mechanisms – through the enrolment of the 5G network with no clear legal rules guiding such activities.

The next section contextualises privacy.

IV. THE RIGHT TO PRIVACY

Privacy remains one of the ubiquitous concepts of modern times which is yet to crystallise a universally accepted definition.[47] Despite several attempts to define the concept of privacy, no universal definition has yet to be formulated.[48] The claim for the right to privacy remains universal, but its concrete form differs according to the prevailing societal characteristics, culture and economic circumstances of the time.[49] This illustrates the non-static nature of the right to privacy, thus the concept is fluid and has continued to evolve over time influenced by the changing times, practices, culture and other developments in societies. As such, even the effective protection of the right to privacy must take into consideration the prevailing developments in both society and the law. This essentially means that, despite privacy being rooted in such a long history, in modern digital settings it must be interpreted in light of the current era and be examined in the current context.[50]

In the main, privacy may be legally defined as, 'an individual's condition of life characterised by exclusion from publicity'.[51] The concept bestows power

44 S. Mchunu, 'DTI "funded Ghadaffi's spyware"', *Mail & Guardian*, 22 November 2013, available at <https://mg.co.za/article/2013-11-22-dti-funded-gaddafi-spyware> (last accessed on 22 June 2019).

45 R. Mpofu, 'Mixed Feelings about Johannesburg's "Big Brother" Network', *Sunday Independent* (3 March 2019), available at <https://www.iol.co.za/news/south-africa/gauteng/mixed-feelings-about-joburgs-big-brother-network-19606157> (last accessed 8 July 2019).

46 Available at <https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017> (last accessed 30 September 2019).

47 A. Lukács, 'What Is Privacy? The History and Definition of Privacy' (2016) 259. Available at: <http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf> (accessed 19 March 2019).

48 F. Schoeman, 'Privacy: Philosophical Dimensions', 21 (3) *American* Philosophical *Quarterly* (1984) 199–213.

49 A. D. Moore, 'Privacy: Its Meaning and Value', 40 *American Philosophical Quarterly* (2003) 215–27.

50 *Supra*, note 48.

51 J. Neethling et al., '*Neethling's Law of Personality* (Butterworths, 1996) 36.

and control on an individual over their personal information, allowing conduct of personal affairs free from unwarranted intrusions.[52] It does not solely refer to the individual personal space, but it equally extends to the home, the family and correspondence and, in certain circumstances, a person's honour and reputation.[53]

The right to privacy, arguably, has two facets: substantive autonomy and informational autonomy.[54] Substantive autonomy is the presumption that a person should have a private sphere with or without interaction with others, free from state intervention and from unsolicited intervention by other uninvited individuals upon which he can be able to make choices about his personal life.[55] Informational autonomy denotes that the individual's private communications should be safeguarded and kept private. This leg is the central focus of this article, and it enables an individual to be able to communicate freely, to exchange information in a platform that is free from intrusions by the state or other individuals, and that the communications should be received only by the intended recipients without any interference.[56]

The right to privacy also mirrors the liberal concept of an individual's freedom and autonomy as a self-governing being. In addition, it is essential for the preservation of an individual's human dignity, including his physical, psychological and spiritual well-being.[57] To date, the right of every person to be protected against arbitrary or unlawful interference with their privacy is a fundamental human right guaranteed under international law.[58]

V. LEGAL RECOGNITION OF THE RIGHT TO PRIVACY

The right to privacy has grown steadily into one of the most significant human rights of the modern age. It is enshrined in several international human rights instruments such as Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 16 of the Convention on the Rights of the Child (CRC), Article 22 of the Convention on the Rights of People with Disabilities (CRPD) and Article 14 of the UN Convention on Migrant Workers (CMW). It is also enshrined in regional human rights instruments such as the European Convention on the Protection

52 C. M. van der Bank, 'The Right to Privacy: South African and Comparative Perspectives', 10 (6) *European Journal of Business Sciences* (2012) 77.

53 Y. Burns, *Communications Law* (Butterworths, 2001) 3.

54 B. T. Balule and B. Otlhogile, 'Balancing the Right to Privacy and the Public Interest: Surveillance by the State of Private Communications for Law Enforcement in Botswana', 37 (1) *Statute Law Review* (2015) 19–32.

55 *Ibid.*

56 *Ibid.*

57 *Supra*, note 4.

58 Article 12 of the Universal Declaration of Human Rights, 17 of the International Covenant on Civil and Political Rights, 8 (1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms 4, 1950, Europ TS No. 5 213 UNTS 221, and 11 of the American Convention on Human Rights OAS Treaty Series No. 36, 1144 UNTS 123 of 1978.

of Human Rights and Fundamental Freedoms[59] and the American Convention on Human Rights and Article 10 of the African Charter on the Rights and Welfare of the Child (ACRWC).[60] However, the right to privacy is conspicuously excluded from the African Charter of Human and Peoples' Rights (ACHPR) and its Protocol on the Rights of Women in Africa (Maputo Protocol).

Due to the then lack of explicit legal recognition of the digital right to privacy regionally and abroad, this inalienable natural right to privacy attracted for itself some 'unfounded myths' throughout the years. Some argue that, in the era of technological advancement, the concept of privacy is dead, people do not care about privacy, people with nothing to hide have nothing to fear, and lastly privacy is bad for business.[61] In Africa, privacy is perceived to be 'alien' to the continent, because the African legal system rather embraces collectiveness than individualism.[62]

Nonetheless, views such as the above raise some burning contestations. The right to privacy is indispensable to human dignity, one of the cornerstones of the African human rights legal system, and it also fortifies other rights such as expression, access to information and association.[63] All these civil rights and freedoms are indivisible and interrelated. Individually or collectively, they act as tools for ensuring the accountability of governments and promote development through improved governance and public participation.[64] The absence of explicit protection under the ACHPR cannot be interpreted to suggest absolute denial of the existence of the right to privacy in the African legal system.

The African Commission in *SERAC* v. Nigeria[65] highlighted the existence of implied rights, where the existing rights can be interpreted to include others, and the right to privacy is likely to fall within this category. Precisely, the right to privacy is embedded in the African philosophical principle of Ubuntu, which can be interpreted to mean humanness or humanity. This is because there can utterly be no human being in the African continent without humanity or personal dignity and there cannot be humanness without privacy even within the context of the African collective identity.

But is it not ironic though that the same governments and security agency officials are uttering statements such as 'if you have nothing to hide what do

59 Article 8 of ECHR provides that: '(i) Everyone has the right to respect for private and family life, his home and his correspondence. (ii) There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

60 African Charter on the Rights and Welfare of the Child of 1990, Article 10.

61 N. M. Richards, 'Four Privacy Myths', in Austin Sarat, *A World Without Privacy?* (Cambridge University Press, 2015) 34.

62 A. B. Makulilo, 'The Quest for Information Privacy in Africa', 8 *Journal of Information Policy* (2018) 317–37; JSTOR, <www.jstor.org/stable/10.5325/jinfopoli.8.2018.0317>.

63 O. Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015) 110.

64 M. Tushnet, *Advanced Introduction to Freedom of Expression* (Edward Elgar 2018), 2.

65 *Social and Economic Rights Action Center & the Center for Economic and Social Rights (SERAC) v. Nigeria* (2001) AHRLR 60 (ACHPR 2001).

you fear?' while they themselves have secured their personal mobile and other digital devices with strong passwords and encryption systems to protect their informational privacy? Clearly, this is the highest form of hypocrisy. Why can't the ordinary citizens, journalists, civil society, and researchers be left alone to equally enjoy their fundamental right to privacy online without unreasonable interference, and not only people of certain status and power?

In addition, the right to privacy is recognised in the international human rights instruments discussed above, and willingly ratified by many African states which subscribe to democracy. It is also enshrined in the domestic constitutions of many African states.[66] In all, it remains the international law responsibility of every individual state to respect, promote and fulfil all the fundamental human rights guaranteed under the instruments they have ratified, without discrimination, and to uphold the rule of law in their domestic terrains.

In 2014, the African Union (AU) and United Nations Economic Commission for Africa (UNECA) contrived a Convention on Cyber Security and Personal Data Protection 2014 as an endeavour to respond to the continental digital fundamental rights breaches by the governments.[67] The Convention calls upon the state parties to establish legal frameworks that protect data and fundamental human rights in the digital space including the right to privacy, to penalise the violators and to establish independent authorities that oversee the processes.[68] Further, Article 25(3) of the Convention explicitly provides that, in the process of adopting legal measures to curb the growing threats to cybersecurity, such adopted measures must not stifle the rights of citizens as guaranteed by national constitutions and international conventions, particularly the ACHPR. Though the ACHPR has no explicit legal recognition of the right to privacy, the convention recognises data privacy under Article 8(1).

Even so, despite such a landmark development, due to the alleged lack of transparency on the drafting process, the lack of adequate protection of human rights provisions and the clauses that had the effect of expanding the judiciary powers, the convention was subjected to severe criticism.[69] To date, it has not yet attracted sufficient ratification of 15 states to bring it into force – only eight countries have ratified and South Africa is not one of them.[70] This shows a lack of political will to ensure protection of the digital rights in the continent, more

66 Constitution of South Africa 1996, section 14, Constitution of Kenya 2010, Article 31 Constitution of Uganda 1995, article 27, Constitution of Egypt 2014 Article 57 and many others.

67 L. A. Abdul Rauf and C. M. Fombad, 'The African Union's Data Protection Convention: A Possible Cause for Celebration of Human Rights in Africa?', 8 *Journal of Media Law* (2016) 67–97.

68 *Ibid.*

69 NATO Cooperation Cyber Defense Centre of Excellence Mixed Feedback on the African Union Convention on Cyber Security and Personal Data Protection, available at <https://ccdcoe.org> (last accessed 14 February 2017).

70 <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf> (last accessed 9 December 2020).

especially the right to privacy. To date, only sixteen African countries have data privacy protection laws.[71]

The states have resorted rather to addressing the issue from their sub-regional economic groupings, which have shown a tremendous positive impact to date, though they also have their shortfalls.[72] The current developments in the area are: the SADC Model Law on Data Protection (2010), the ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010) and the EAC Framework for Cyber Laws (2008). One groundless argument raised against the above has been the question of consistency of the laws with each other.[73] However, the misconception of classifying Africa as monolithic or a homogeneous society is way too overdue.[74] Diversity is the precise concept which should be embraced by Africa. African states have different post-colonial histories, ethnicities, human rights, cultures, historical legal systems, and traditional practices and customs, which each country individually should consider when formulating its own national laws.

Therefore the African laws on digital privacy cannot be expected to be directly consistent with each other. Perhaps the real question should be that of ensuring the adequacy of the African laws so enacted to regulate digital privacy against its competing interests, considering the diverse sub-regional and national needs and challenges, and rather drawing lessons from international best practices where possible. Further, except for the Economic Community of West African States (ECOWAS), the other frameworks are merely model laws and guidelines which do not legally bind the state parties. The AU Convention on cybersecurity is also backed up by declarations and resolutions on digital rights, which also seek to affirm protections for all digital human rights and freedoms.[75] The discussion which follows provides an analysis of privacy in the South African context.

VI. LEGAL PROTECTION OF THE RIGHT TO PRIVACY IN SOUTH AFRICA

The right to privacy is a constitutionally protected and justiciable right under section 14 of the South African Constitution of 1996 and common law. The explicit protection of digital privacy, in particular, is found under section 14(d). Further, the yet to be fully implemented Protection of Personal Information Act (POPI) also recognises the right to digital privacy by stating that:

71 Deloitte Touche Tohmatsu Limited, *Privacy Is Paramount Personal Data Protection in Africa* (2018), Report 6, available at <https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf> (last accessed 22 September 2018).

72 *Ibid.*

73 *Ibid.*

74 R. Williams and H. G. Broadman, *Forbes* magazine online, 'Africa The Continent of Misperceptions', 31 March 2016, accessed at <https://www.forbes.com/sites/harrybroadman/2016/03/31/africa-the-continent-of-economic-misperceptions/?sh=4b7785686c54> (accessed 8 December 2020).

75 'African', Windhoek Declaration on Promoting an Independent and Pluralistic African Press of 1991.

> the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.[76]

Section 39(1) of the same Constitution above moreover, urges the courts when interpreting the Bill of rights, to promote the values that underlie an open and democratic society based on *human dignity*, equality and freedom, and the right to privacy is a core value of human dignity. This was confirmed by the Supreme Court of India in the landmark judgment of *Puttaswamy* v. *Union of India*,[77] where the court stated:

> Dignity cannot exist without privacy. Both reside within the inalienable values of life, liberty and freedom, which the Constitution has recognised. Privacy is the ultimate expression of the sanctity of the individual. It is a constitutional value which straddles across the spectrum of fundamental rights and protects for the individual a zone of choice and self-determination.[78]

This case does not bind South Africa, but it may be considered for guidance in accordance with Article 39(1)(c) of the Constitution.

Furthermore, South Africa is a state party to several international human rights legal instruments highlighted above which protect the right to privacy namely: UDHR, ICCPR, CRC, ACRWC. However, as a matter of doctrine, whether international law is directly applicable or not to a state is dependent on the domestic legal system. South Africa is a dualist state and therefore international instruments can only be directly applicable after domestication unless in the case of self-executing treaties or customary international law. The constitution stipulates that international law *may be* considered when interpreting the law as provided by the Constitution under section 39(1b) and section 233 which provides that:

> When interpreting the Bill of Rights, the courts 'must consider international law and prefer any reasonable interpretation of the legislation that is consistent with international law over any alternative interpretation that is inconsistent with international law'.[79]

The Constitutional Court also acknowledged in the case of the *Government of the Republic of South Africa and others* v. *Grootboom and others* that, where the relevant principles of international law bind South Africa, such principles may be directly applicable.[80]

In terms of section 232 of the Constitution, international customary law is considered the law of the land.[81] Therefore the Vienna Convention's general rules

76 Protection of Personal Information Act 2013.
77 *Justice K. S. Puttaswamy* v. *Union of India* (2017) 10 SCC 1.
78 *Ibid.*
79 Constitution of the Republic of South Africa 1996, section 233.
80 *Government of South Africa* v. *Grootboom* (2000) 11 BCLR 1169 (CC), 26.
81 Constitution of the Republic of South Africa 1996, section 232.

of interpretation (Articles 31–32) are directly applicable. The rules provide the critical elements[82] to be considered in the interpretation process; in addition, the *pacta sunt servanda* clause in Article 26 provides that the states are bound by the treaties they have freely ratified and they have a duty to fulfil their obligations in good faith.[83] This essentially means that South Africa has a duty to comply with the treaties above in good faith.

In all, as highlighted above, though the POPI Act is not yet fully operational, from all the above it could be agreed that the right to privacy, including digital privacy, is comprehensively protected under South African law.[84] South Africa therefore has an obligation to ensure that the right to privacy is adequately protected, respected and fulfilled within its terrains regardless of its nature.

VII. THE SHORTFALLS OF THE SOUTH AFRICAN NATIONAL SECURITY AND ELECTRONIC COMMUNICATION SURVEILLANCE REGULATORY FRAMEWORK

The South African national security surveillance is regulated by a cocktail of pieces of legislation, namely RICA,[85] the Financial Intelligence Centre Act (FICA)[86] and the National Strategic Intelligence Act (NSIA)[87] among others. However, the main legal regime for electronic and communications surveillance is RICA which is the subject of the current study.

RICA under section 49 criminalises any unauthorised communications surveillance and monitoring, but this provision applies exclusively to 'private human persons' while it conspicuously remains silent for private entities or public authorities.[88] In addition, the only legally authorised body to conduct communication surveillance in the whole country, in terms of RICA, is the Office of the Interception Centre established in terms of sections 32–37,[89] yet there are other secret public bodies under the Intelligence Agency which operate under a legal black hole.

The primary role of the National Communications Centre (NCC) is to conduct both targeted and indiscriminate electronic surveillance and snooping of both foreign and domestic signals. It is known to have the largest surveillance capabilities and ranks close to the United States (NSA) and the United Kingdom

82 Article 31 set out the elements such as (1) 'a treaty'; (2) 'good faith'; (3) 'ordinary meaning of terms'; (4) 'context'; and (5) 'object and purpose' to be taken into account in interpreting the treaties.

83 Article 26, Vienna Convention on the Law of Treaties 1969.

84 Article 12 of the UDHR.

85 Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

86 Financial Intelligence Centre, Act 38 of 2001.

87 National Strategic Intelligence Act 39 of 1994.

88 Section 49, No. 70 of 2002.

89 *Supra*, sections 32–37, RICA No. 70 of 2002.

(GCHQ) as exposed by Snowden in 2013 above.[90] However, despite being the mother law for communication surveillance law in the land, RICA does not have any provisions regulating the NCC's operations. In addition to this, RICA is equally silent on the actual mass surveillance operations though capable of being conducted by government bodies such as the NCC.[91] In addition, the safeguards prescribed by the law over government and private sector surveillance practices have also been weak and ineffective.

While RICA creates impunity over the illicit activities of technology service providers and government bodies, the unparalleled level of the secretive tradition endorsed by the national security sector, the lack of legal provisions for public oversight mechanisms and the lack of transparency in their operations totally eliminates their duty of accountability towards the people they serve.[92] All of the above causes paranoia and distrust of their operations in the country.

RICA is silent on the procedure to be followed by state officials when examining, copying, sharing and storing intercepted data. RICA mandates the surrender of personal information during the registration of Subscriber Identity Module (SIM) cards to private corporations, but it does not suggest how such entities and service providers should handle and protect such data.

Additionally, the Act prescribes designated judges to authorise surveillance practices through the awarding of warrants to applicants after hearing the case, but such court applications are brought before the RICA court on an *ex parte* basis. Only the applicant is given an opportunity to be heard, which in most cases are state officials and not the targeted party. Such proceedings undermine transparency, a core value of good governance, and the rules of natural justice, such as the right to be heard, which all require the governed to have a say in what is being done in their names rather than secretive proceedings. Furthermore, courts seldom reject such applications. The high success rate of RICA orders has also fuelled the assertion that such courts have ceded independence and it is now arguable as to whether the RICA court is part of the judiciary or is acting as an appendage of the executive.[93]

Finally, RICA does not provide a clear balance between the constitutionally protected right to privacy and the acts of electronic surveillance which are conducted in the name of maintaining public order and national security. Importantly, the law does not have provisions for mass surveillance and is not regulated under South African law. The present position on the ground is that the national security laws such as RICA render the privacy rights legal protections otiose, which is the cause of the prevailing regulatory dilemmas.

90 J. Duncan Bulk, 'Communication Surveillance in South Africa – Fix It or Nix It', *Daily Maverick* <https://www.dailymaverick.co.za/article/2019-09-30-bulk-communication-surveillance-in-south-africa-fix-it-or-nix-it/30> September 2019 (accessed on 12 October 2019).

91 Right2Know, 'The Surveillance State, Communications Surveillance and Privacy in South Africa' (2016) *Media and Democracy*, available at <https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf> (accessed on 9 October 2019).

92 Section 32, RICA No. 70 of 2002.

93 *Supra*, note 91.

VIII. GUIDANCE FROM INTERNATIONAL LAW: RESOLUTION FOR THE REGULATORY DILEMMA ON DIGITAL PRIVACY AND SURVEILLANCE

Despite the above, there is currently no multilateral treaty on surveillance, personal data protection and other illegal practices on the internet. In 2013, after noting the extended powers exercised by most states over cyberspace, a global coalition of civil society, technology and privacy experts drafted the International Principals on the application of Human Rights Law to communications surveillance, while the UN General Assembly (GA) and the Human Rights Council (HRC) issued resolutions on the 'right to privacy in the digital age' in 2015. The latter accord digital rights a similar status of protection as afforded to offline rights, including the right to privacy.[94]

In 2016, the UN General Assembly and the UN Human Rights Commission endorsed a resolution declaring the 'promotion, protection and enjoyment of human rights on the internet' online freedom, a human right that must be protected.[95] The resolution demanded consideration of a comprehensive human rights-based approach when providing and expanding access to the internet and for the internet to be open, accessible and nurtured.[96] Though some countries such as Russia, China and South Africa rejected the resolution, it was ultimately adopted.[97]

Regionally, there are other initiatives such as the Council of Europe Convention for the protection of individuals with regard to the Automatic Processing of Personal Data (CeE Convention), Derivative 95/46/EC of the European parliament of 24 October 1995, and the EU General Data Protection Regulation of 2018. Additionally, the Organisation for Economic Cooperation and Development (OECD) guidelines on surveillance and data privacy have significantly influenced the drafting of many national security and privacy laws around the globe.[98]

In Africa there is no treaty on surveillance. While there is continuing work on the development of initiatives that seek to protect digital rights, most of the initiatives are merely declaratory and have no legal binding force in the states.

IX. THE LEGITIMACY OF ELECTRONIC MASS SURVEILLANCE AS A STRATEGY FOR NATIONAL SECURITY IN AFRICA

As with many other fundamental human rights, the right to privacy is not absolute. It may be limited in the interests of others under specific conditions, if the interference is not arbitrary or unlawful. At times, national security through

94 United Nations, GA69/166, 3 the Right to Privacy in the Digital Age (2014) and the HRC, UN Doc. A/HRC/28/L.27, available at <https://www.ohchr.org/en/hrbodies/hrc/. . . /session27/documents/a-hrc-27-37_en.doc> (accessed 21 March 2019).

95 *Business Insider* digital journal (2016), available at <https://www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7?IR=T> (accessed 18 October 2018).

96 *Ibid.*

97 *Ibid.*

98 OECD Guidelines and Surveillance and OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at <www.oecd.org/sti/ieconomy/49710223.pdf> (accessed 16 January 2019).

surveillance can represent a reasonable ground for the limitation of the right to privacy. However, national security cannot always be a blanket justification for wanton breaches of fundamental rights.[99] Surveillance cannot be conducted in an indiscriminate manner, it must be conducted legitimately, be lawful and used only where necessary.[100] In a democratic and constitutional state such as South Africa, such limitation must be in line with the constitution and must pass the prescribed section 36[101] limitation test.[102]

X. JUSTIFIABILITY OF DIGITAL PRIVACY BREACHES FOR NATIONAL SECURITY PURPOSES UNDER INTERNATIONAL LAW

Under international law, the doctrine of proportionality prescribes that 'a balance be maintained between the action and the purpose for which the powers have been conferred'.[103] This measure is used to ascertain whether the limitations and measures impinging upon human rights employed by the state befittingly respond to legitimate public interest, such as in the case of national security. However, the concern with regard to mass surveillance issues is that states, including the United States of America, failed to prove the effectiveness of mass surveillance measures in maintaining national security or stopping imminent terrorism attacks.[104] Therefore, in the absence of proof of the effectiveness of achieving a legitimate aim of national security, these acts are considered not appropriate and hence in most cases prohibited.

The proportionality principle also denotes that it must be proven that mass surveillance is necessary under the given circumstances, and there should be no other less intrusive method of achieving the purpose aimed at. But cases of mass surveillance are always different as there is no target, the acts are indiscriminate and every citizen becomes a suspect. Rather, critics of mass surveillance view that targeted surveillance may have better effects than mass surveillance in terms of maintaining national security.[105] This is because targeted surveillance is conducted when there is at least an imminent threat to national security by someone or a

99 *Supra*, note 62.

100 Report of the Special Rapporteur on the promotion and Protection of the Right to Freedom of Opinion and Expression Surveillance and Human Rights, <https://www.undocs.org/A/HRC/41/35> (last accessed 15 September 2019).

101 Section 36, Constitution of the Republic of South Africa 1996.

102 *Digital Rights Ireland* v. *Seitlinger* v. *Minister for Communications, Marine and Natural Resources*, C-293/12 and (2014) C594/12 CURIA.

103 C. Thomas et al., *The Principle of Proportionality in International Law*', NCCR Trade Working Paper No. 38 (2012) 1–34, available at <https://www.wti.org/media/filer_public/9f/1b/9f1bd3cf-dafd-4e14-b07d-8934a0c66b8f/proportionality_final_29102012_with_nccr_coversheet.pdf>.

104 M. Cayford, W. Pieters and C. Hijzen, 'Plots, Murders, and Money: Oversight Bodies Evaluating the Effectiveness of Surveillance Technology, 33 (7) *Intelligence and National Security* (2018) 999–1021.105

105 T. Houston, 'Mass Surveillance and Terrorism: Does PRISM Keep Americans Safe?' *Chancellor's Honors Program Projects, University of Tennessee: Knoxville* (2017) 40 <https://trace.tennessee.edu/utk_chanhonoproj/2058> (accessed 20 May 2019).

group of people acting on behalf of a foreign government or organisation which has the potential to pose a serious threat to the government of the country.[106]

Further, the law in a democratic state should stipulate in clear terms upon which crimes electronic surveillance may be employed and to what extent.[107] This is to ensure that legitimate and normal activities in a democratic state such as journalism, civic protests, trade unionism and political opposition are not subjected to unwarranted surveillance because the individuals involved have different interests and goals than those in power. It also ensures that relatively minor crimes, especially those that would not generally involve telecommunications for facilitation, are not used as excuses to conduct intrusive surveillance for political or other reasons.

In 2004, the Court of Justice of the European Union (CJEU), a court known for its growing reputation for the quality of its jurisprudence on the rule of law, handed down a landmark judgment in the case of *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*.[108] This case was mainly about the legality of the Data Retention Derivative, which allowed universal and indiscriminate retention and access to data by 'certain national authorities'. Upon failure to verify the appropriateness of the data retention measures in such capacities (thus proving whether the measures were appropriate and necessary to attain the objective), the CJEU invalidated the derivative from the date of its inception. This was mainly on the basis that the law seriously threatened fundamental rights and did not limit such significant interference with the rights of privacy and data protection to the measures and circumstances that were strictly necessary.[109]

Again, not long ago, the European Court of Human Rights (ECHR) delivered a ruling in the case of *Big Brother Watch and Others* v. *United Kingdom*.[110] The court ruled against the 2014 Retention and Investigatory Powers Act (RIPA), a legal surveillance architecture which authorised the Government Communications Headquarters (GCHQ) to conduct mass surveillance on the personal accounts, communications and mobile phones of millions without discrimination, under the auspices of monitoring terrorism. The court ruled that RIPA was invalid and inconsistent with Article 8 of the European Convention on Human Rights, which guarantees the right to privacy. The court held that the law is against the principles of democracy that the country subscribes to.

The foreign case law above is not legally binding on South Africa, but it may be considered as a guide to interpretation. From the above, one can deduce the evident resonance of the legal ills of the South African RICA. Thus clearly the RICA law does not conform to the international human rights law standards.

106 US Foreign Intelligence Surveillance Act 50 of 1978 USC §§ 1801–11.

107 *Ibid.*

108 *Digital Rights Ireland and Kärnten Land – esregierung Seitlinger and Others* (2014) ECLI:EU:C at 238.

109 *Ibid.*

110 *Big Brother Watch and Others* v. *United Kingdom* (2018) 58170/13, 62322/14 and 24960/15.

Similarly, the United Nations Human Rights Committee General Comment No. 16 on communications surveillance proscribes surveillance, stating:

> Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.[111]

The Special Rapporteur on the right to privacy considers the powers exercised by states over the internet in contravention of Article 19, para. 3, of the International Covenant on Civil and Political Rights (ICCPR).[112] He states that any curtailment of digital rights in whatever manner as well as their supporting grounds of justifications are disproportionate to the violations of human rights and they can never satisfy the proportionality test as prescribed under international human rights law.[113] The UN therefore continues to urge states to ensure effective data protection to protect the citizens from exploitation by the official authorities and commercial organisations which are presently in a position to exploit personal data and threaten the privacy of individuals.[114]

XI. THE JUSTIFIABILITY OF DIGITAL PRIVACY BREACHES FOR NATIONAL SECURITY PURPOSES UNDER SOUTH AFRICAN LAW

In South Africa, there has been a gross regulatory dilemma as far as the right to privacy and national security are concerned since the inception of RICA. Thus, while the law prima facie protects the right to privacy, the deficiencies in the law tend to nullify such protections to some extent. Law enforcement and security officials charged with protecting privacy happen to be its targets. The limits of the right to privacy in the digital age are largely unclear and same as the limits of surveillance. The legally protected informational autonomy continues to be subjected to severe curtailment through mass surveillance measures.

The South African limitation clause[115] states that any restriction of a right must be limited only in terms of the law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, considering all relevant factors. It prescribes that the limitation should be authorised by the 'law, applicable to all, reasonable and justifiable and proportionate in an open and democratic society, considering the core values of the constitution, being human dignity, equality and freedom'. However, it remains questionable whether mass surveillance is justifiable and reasonable under South African law. The position concerning this

111 Human Rights Committee, General Comment 16 (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, UN Doc. HRI/GEN/1/Rev.1 at 21 (1994).

112 United Nations Human Rights Office of the Commissioner, *The Right to Privacy in the Digital Age*, available at <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx> (last accessed 20 May 2018).

113 *Ibid.*

114 *Ibid.*

115 Section 36 of the South African Constitution of 1996.

is that mass surveillance activities are currently unregulated under South African law, while evidence reveals that they continue to be conducted in secret. It is also questionable whether the law, as it currently stands, is in line with the constitutional values, more especially dignity and freedom as well as whether it upholds principles of the rule of law and democracy that the country subscribes to.

This could also take one back to the question of whether the law satisfies the other requirement listed above 'in a democratic and open society', more specifically the hearing of RICA court order application being brought by an applicant who happens in most cases to be a law enforcement official in front of a single retired judge. The court proceedings are on an *ex parte* basis, and are only heard by a retired judge based on presentations made by the applicant in secret. Clearly, this also contradicts the rules of natural justice, which would rather coincide with the adversarial judicial proceedings than biased secretive proceedings. The RICA law states that the people must consent to the collection and interception of their personal data, but the RICA proceedings do not promote this – instead, RICA promotes secretive spying on individuals unknowingly.[116]

The absence of mass surveillance provisions in RICA, for instance, allows the constitutionally enshrined rights to be limited in secret and without the consent of the right holders. In all, the above evidently showed that some provisions of RICA are clearly invalid, undemocratic and inconsistent with the constitution and international human rights standards.

As a consequence of the failure to adequately protect the right to privacy and failure to adequately regulate surveillance activities despite constant abuse by government officials and the private sector, in March 2016 the UN Human Rights Committee expressed concerns over RICA.[117]Alongside the above, AmaBhungane Investigative Journalism as highlighted above also emerged victorious in their legal proceedings against the South African Ministry of Correctional Services and others.[118]

In their case, they challenged the constitutionality of some sections of RICA such as sections 16(5), 17(4), 19(4), 21(4)(a) and 22(4)(b) which authorised the interception of communications of people by authorised officials subject to certain conditions and the constitutionality of the unregulated bulk interception activities and foreign signals interceptions.[119] The High Court declared the sections above invalid and unconstitutional as well as the bulk of mass interception activities and foreign signals interceptions.[120] The declaration has been suspended for two years to allow parliament to rectify the confirmed legal defects of RICA. The findings of the High Court were later affirmed by the Constitutional Court in February 2021.[121] This case remains a landmark development in the area so far and hopefully other African states will follow suit.

116 *Supra*, note 3.

117 South African Human Rights Commission (2017), Civil and Political Rights Report 2016/2017.

118 *Supra*, note 3.

119 *Ibid.*

120 *Ibid.*

121 *AmaBhungane Centre for Investigative Journalism NPC and Another* v. *Minister of Justice and Correctional Services and Others; Minister of Police* v. *AmaBhungane Centre for Investigative*

XII. POSSIBLE LESSONS TO BE DRAWN FROM THE UNITED STATES FREEDOM ACT OF 2015, FOR RICA REFORMS

In other jurisdictions such as the United States of America with arguably the highest per capita surveillance apparatus in the world, there are rules and regulations regarding when, how, where and for what purpose it is justifiable to use surveillance to maintain national security, though the contestations on the adequacy of such rules are ongoing.

The United States of America signed into law the Freedom Act in 2015 in order to remedy the legal ills of the then Patriot Act,[122] particularly to end the unconstitutional bulk collection of telephone metadata by the National Services Authority (NSA), and to do away with the secretive proceedings of the court of the Foreign Intelligence Surveillance Act (FISA).[123]

Section 103 of the Freedom Act discussed above prohibits indiscriminate surveillance while section 401 directs the presiding judicial officer of the FISA court and the FISA court of review to jointly designate at least five individuals to serve as amicus curiae to assist in the consideration of any application for an order or review that presents a novel or significant interpretation of the law, unless the court finds that such appointment is not appropriate.[124]

The amicus curiae, for instance, is required to provide legal arguments that advance protections of privacy and other freedoms and other legal arguments related to intelligence collection or communications technology. Importantly, section 402 demands the declassification of the review of each decision, order or opinion issued by the FISA court or the FISA court of review that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of 'specific selection terms' as defined in the Act.

Decisions, orders or opinions are also to be made publicly available to the greatest extent practicable, subject to permissible redactions. The above is missing in the South African RICA.

XIII. DOES THE POPI ACT ADDRESS THE RICA ILLS?

While the above remains the coming into effect of the POPI Act has been a ray of hope as far as adequate protection of data privacy is concerned, including the regulatory dilemmas of RICA above.

The majority of the sections of the long-awaited data privacy legislation's POPI Act' came in to effect as from 1 July 2020, with a one-year grace period.[125] The POPI is considered a landmark development in the sub-region, as

Journalism NPC and Others (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC).

122 United States of America Patriot Act Public Law No. 107–56, 107th Congress; of 2001,

123 Section 103(3) of the USA Freedom Act of 2015, Public Law No. 114–23.

124 Section 401 of the USA Freedom Act of 2015.

125 See also <https://www.michalsons.com/blog/popi-commencement-date-popi-effective-date/13109> (last accessed on 8 December 2020).

it comprehensively guarantees data privacy and accords the data subject some legally enforceable personal data rights, such as the right to consent to how data is to be used and be notified.

The Act further provides eight mandatory data processing conditions to be complied with by responsible parties (public or private bodies and any other person). These include: accountability, openness, consent, limiting processing of personal data, collecting information only for a lawful and specific purpose, further processing must be compatible with the purpose of processing, processing accurate information and securing the integrity of the data processed.[126]

The POPI Act also has a broader scope of application: it protects the rights of all persons under South African jurisdiction whereas the latter only protects citizens. The Act further holds all stakeholders, including the private sector, accountable for human rights breaches on their way to accessing, storing and disseminating personal data and safeguarding measures in place to ensure the protection of the right to privacy under section 8.

Although the POPI Act is not national security legislation, by virtue of being the mother law for data protection and digital privacy in the land it raises some positive expectations as far as provisions crosscutting RICA are concerned. One would expect to see the POPI Act as having created a balance between digital privacy and competing interests, or providing guidance on how to deal with such cases.

However, the POPI Act, conspicuously, does not apply to data collection for purposes of national security and/or law enforcement. In fact, it has explicit exemptions for these areas, which remain worrisome, as so much unfettered power and control over the personal data of individuals remains in the hands of these sectors despite their proven inability to carry out their mandate in a transparent, accountable and rights-based manner.[127] Despite the beautiful provisions and strict conditions on face value, the POPI Act resembles a barking toothless dog which is unable to bite. It would have been rather reasonable for the two sectors to work together in addressing the data protection lacunas of RICA.

By way of interpretation, however, it can be implied that the POPI Act prohibits mass surveillance practices under the data minimisation principle, and it has laid foundational grounds for data protection. The responsible sector can now draw lessons and align the RICA with the constitution and POPI for consistency, the rule of law, democracy and social justice.

XIV. CONCLUSIONS AND RECOMMENDATIONS

The dilemmas created by the South African RICA threaten the rule of law, democracy and social justice which the country subscribes to and therefore contravenes international human rights law. This article affirms that the court had not erred in declaring unconstitutional the provisions of RICA. This landmark

126 POPI Act 4 of 2013, Chapter 3.
127 Section 37(2) of POPI.

decision by learned Justice Sutherland was commended by the whistleblower of our time Edward Snowden through a tweet.[128]

Consequently, it is recommended that the mass surveillance legal lacunas in the RICA be addressed and reforms be made, thus the law must clearly state the limits of surveillance to curb the chances of misuse and unjustified breaches of privacy rights. RICA must be revised and harmonised with both the POPI Act and the constitution. Currently, RICA has the effect of limiting protections guaranteed by the POPI Act and the constitution, but there is completely no synergy between the laws.

Other issues such as the alarming rate of orders granted to police officials in terms of section 206 to obtain telephonic records from the private sector must be looked at. There is also a need to strengthen the privacy safeguards and oversight measures in the digital age to ensure that both private sector and public organs involved in surveillance measures are held accountable for human rights breaches. The one-sided proceedings before a single retired judge must be reconsidered as a panel of judges on a case-by-case basis while independent privacy experts should be appointed on an amicus curiae basis similar to the American model discussed above.

128 Business Day, 'Landmark Rica Ruling Impresses Even Ultimate Whistle-Blower Edward Snowden' (17 September 2019), available at <https://www.businesslive.co.za/bd/opinion/2019-09-17-landmark-rica-ruling-impresses-even-ultimate-whistle-blower-edward-snowden/> (accessed 3 October 2019).