AFRICAN HUMAN RIGHTS LAW JOURNAL

To cite: O Saki '"We will visit your bedrooms": Testing the adequacy of safeguards in the interception of communications in Zimbabwe through the lens of the *AmaBhungane* case' (2025) 25 *African Human Rights Law Journal* 822-851
http://dx.doi.org/10.17159/1996-2096/2025/v25n2a15

'We will visit your bedrooms': Testing the adequacy of safeguards in the interception of communications in Zimbabwe through the lens of the *AmaBhungane* case

*Otto Saki**
Doctoral candidate, University of the Western Cape, South Africa
https://orcid.org/0009-0002-8924-9365

Summary: *Targeted or bulk interception of communications is a permanent feature of contemporary society. Ancient states deployed rudimentary practices such as raiding mailmen, shooting carrier pigeons and rerouting telegrams. In modern times, the interception of communications happens effortlessly. Under these laws, interception targets are usually not informed. Laws compel public and private actors to cooperate with government directives mandating real-time, targeted or bulk surveillance. Government officials have openly acknowledged the state's capacity to intercept private communications and intrude upon private spaces. In most regimes, the laws lack oversight and effective remedies. The article looks at Zimbabwe's Constitution and international legal obligations and frameworks on surveillance. It problematises the various provisions of the national law authorising interception against international human rights standards, comparatively with the South African laws. The article contrasts provisions of Zimbabwe's Interception of Communications Act of 2007 (IC Act), on interception and surveillance*

* LLB (Zimbabwe) LLM (Tanzania) LLM (USA); 4119180@myuwc.ac.za

of communications against the decision in AmaBhungane v Minister of Justice & Others *which found provisions of South Africa's Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) unconstitutional. The article observes that the RICA provisions are uncannily similar to the Act's provisions and, therefore, concludes that the IC Act cannot stand a constitutional test. If these provisions are challenged, a court would have no option but to find them repugnant to constitutional and international human rights standards. In addition to the fully developed principles of necessity and proportionality, the article proposes the expansion of principles of adequate safeguards as essential to protecting individuals against arbitrary surveillance that allows visitation in people's bedrooms. Any surveillance law must start from the basis of achieving adequate safeguards, and in this instance any amendments to the IC Act must fulfil this basic requirement.*

Key words: *surveillance; interception; oversight; safeguards; privacy*

1 Introduction

Since 2001, with the 11 September terrorist attacks in the United States (US), the recurring justification for both targeted and bulk interception of communications is the protection of national security against crime and terrorism.[1] Increasingly, new vectors are emerging, creating complex challenges that compel governments to surveil individuals' private communications and personal spaces, thereby infringing on the right to privacy.[2] Fundamental rights are increasingly endangered by the false dichotomy between liberty and security.

However, Zimbabwe faces no immediate security threats, and even if those threats existed, regulation and oversight of surveillance is non-negotiable.[3] In the absence of credible security threats, autocratic legalism legitimatising targeted and bulk surveillance of personal

1 UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism Report on human rights implications of the development, use and transfer of new technologies in the context of counterterrorism and countering and preventing violent extremism, AHRC52/39 1 March 2023.

2 JA Mavedzenge 'The right to privacy v national security in Africa: Towards a legislative framework which guarantees proportionality in communications surveillance' (2020) 12 *African Journal of Legal Studies* 360.

3 A Munoriyarwa 'The growth of military-driven surveillance in post-2000 Zimbabwe' May 2021 Media Policy and Democracy Project University of Johannesburg's Department of Communication and Media and the University of South Africa's Department of Communication Science.

communications becomes the norm. This surveillance is conducted through a vast human and technology infrastructure selectively targeting government critics and opponents such as opposition parties, journalists and human rights defenders.[4] In Zimbabwe, as is the case in South Africa, these surveillance practices are designed to silence critics, suppress dissent and state accountability reminiscent of the colonial and apartheid regimes. Invoking history, Madlanga J in *AmaBhungane* recalls that 'the pursuit of skewed notion of national security was weaponised and calculated to subvert the dignity of the majority of South Africans under the apartheid regime'.[5] While apartheid and colonial regimes were characterised by injustice and illegality, national security interests in independent, lawful states cannot be dismissed. As the Inter-American Court of Human Rights in *Castillo Petruzzi v Peru* pointed out, there can be no doubt that the state has the right and the duty to guarantee its own security, but this is not 'a license to exercise unbridled power or to use any means to achieve its ends'.[6]

Sadly, many regimes, that of Zimbabwe included, use unbridled power to complete a permanent state of surveillance and targeting of government opponents. Modern Zimbabwe has maintained and perfected an arsenal of obnoxious security laws reminiscent of the colonial era.[7] These laws have consolidated state capacities to carry out surveillance against citizens under the narrow guise of advancing national security interests, including protecting the President's image.[8]

In July 2007 a prominent Roman Catholic priest's private engagements were broadcast on government-controlled media outlets.[9] The priest had consistently criticised President Mugabe's

4 T Matsilele, B Mutsvairo & B Karam 'Social media as a sphere of political disruption' (2021) Utrecht University, Institute for Justice and Reconciliation & Solidarity Peace Trust 'Policing the state: An evaluation of 1 981 political arrests in Zimbabwe: 2000-2005' (2006) Institute for Justice and Reconciliation, Solidarity Peace Trust.

5 *AmaBhungane Centre for Investigative Journalism NPC & Another v Minister of Justice and Correctional Services & Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC & Others* [2021] ZACC 3 para 1.

6 *Castillo Petruzzi v Peru* IACHR 30 May 1999 Ser C No 52 para 204.

7 Since 2000, the opposition Movement for Democratic Change members have been routinely arrested and prosecuted on charges of subverting a constitutionally elected government, publishing or communicating falsehoods. The laws include the Criminal Law Codification Reform Act Chapter 9:23, and the Maintenance of Public Order Act (MOPA) Chapter 11:23.

8 Individuals have been arrested in Zimbabwe for insulting the President on social media platforms. Zimbabwe Lawyers for Human Rights 'Policeman arrested in social media blitz on dissent as imprisoned opposition councillor fights for Freedom Camp' 14 July 2020, https://www.zlhr.org.zw/?p=2112 (accessed 5 January 2023).

9 M Wines 'Pius Ncube, a Zimbabwean archbishop, steps down' 11 September 2007, https://www.nytimes.com/2007/09/11/world/africa/11iht-zim.5.7470951.html (accessed 19 December 2022).

regime and its human rights practices. In disdain, President Mugabe remarked that some priests 'claim they swore to celibacy, yet they sleep around with countless women'.[10] This unscripted remark confirmed state sanctioned surveillance of intimate personal spheres decimating the essence of the right to privacy. In 2014, confirming the unregulated deployment and absence of adequate safeguards on state surveillance, the State Security Minister in the Zimbabwean President's office remarked that the government 'sees everything … we have our means of seeing things these days, we just see things through our system. So, no one can hide from us in this country.' The Minister further warned Zimbabweans to be 'careful not to denigrate our president [Robert Mugabe], we will visit your bedrooms and expose what you will be doing'.[11]

More striking is that this surveillance occurred outside the bounds of the law, and even if it had been lawful, the priest posed no legitimate threat to national security. Prior to this incident, the Supreme Court had in 2004 declared provisions of the Postal and Telecommunications Act, which authorised bulk interception and surveillance, unconstitutional in *Law Society of Zimbabwe v Minister of Transport*.[12] The Interception of Communications Act (IC Act) was only promulgated on 3 August 2007.[13]

In regimes such as that of Zimbabwe, while the presence of a law makes some difference, it is not sufficient if the law itself lacks adequate and independent oversight mechanisms. This is where a law ceases to be a just law.[14] Due to the advances in technology, governments are relying on sophisticated '*stealthocratic*' surveillance software.[15] An independent report accused the Zimbabwean government of procuring unregulated surveillance software with remote capacity

10 C McGreal 'How secret camera in archbishop's "love nest" silenced vocal Mugabe critic' 20 July 2007, https://www.theguardian.com/world/2007/jul/21/zimbabwe.chrismcgreal (accessed 19 December 2022).

11 'CIO watching your bedrooms, Mutasa warns critics' *New Zimbabwe* 10 June 2014, https://allafrica.com/stories/201406110354.html (accessed 19 December 2022).

12 *Law Society of Zimbabwe v Minister of Transport and Communications & Others* (2004) ZWSC 127.

13 Interception of Communications Act: Date of commencement 3 August 2007.

14 The test on limitation of rights and laws includes that there must be a law in existence (legality), and this legality must be constitutionally proportionate, independent of other test limitations. *Democratic Assembly for Restoration and Empowerment & 3 Others v Saunyama NO & 3 Others* CCZ 9/18, Civil Appeal CCZ 5/18.

15 Some of the software is exploiting the weaknesses in mobile companies and the data troves from compulsory SIM registration. See UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression A/HRC/41/35, 28 May 2019. Zimbabwe requires all SIM cards to be registered in terms of Statutory Instrument 95 of 2014 Postal and Telecommunications (Subscriber Registration) Regulations 2014.

to access different personal information including texts, calls and location data.[16] Similar intrusive software has been used in Australia, Belgium, Botswana, Chile, Denmark, Ecuador, El Salvador, Estonia, Equatorial Guinea, Guatemala, Honduras, Indonesia, Israel, Kenya, Malaysia, Mexico, Morocco, Nigeria, Peru, Serbia, Thailand, the United Arab Emirates (UAE), Vietnam and Zambia, targeting human rights activists, politicians and journalists.[17]

The article commences with an analysis of the international legal safeguards on surveillance. It proceeds to conduct a national level analysis of the surveillance framework with a focus on the IC Act. The next part analyses provisions of the South African Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) and the *AmaBhungane* decision. The final part focuses on the enhancement of surveillance oversight mechanisms and safeguards and recommendations for Zimbabwe.

2 International legal safeguards on surveillance

The extent of surveillance regulation has for long varied across countries due to the absence of international standards regulating surveillance.[18] This regulatory *lacuna* has clouded state practices on targeted and bulk surveillance, increasing the risk of fundamental rights violations and impunity. In the absence of a shared international framework, civil society and privacy advocates formulated International Principles on the Application of Human Rights to Communications Surveillance in an endeavour to advance global practices safeguarding human rights during surveillance operations.[19] These international principles are derived from international human rights law standards such as the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (Universal Declaration).[20]

16 B Marczak and others 'Running in circles: Uncovering the clients of Cyberespionage Firm Circles' Citizen Lab Research Report 133, University of Toronto, December 2020.

17 As above.

18 There are calls for global regulation of surveillance software especially by UN mechanisms, as this software cannot be 'human rights free zone'. See UN Special Rapporteurs call for surveillance tech moratorium, https://www.computerweekly.com/news/252505287/UN-special-rapporteurs-call-for-surveillance-tech-moratorium (accessed 20 January 2023).

19 International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org/13-principles/ (accessed 24 December 2022).

20 UN Human Rights Council Resolution on the Right to Privacy in the Digital Age (2021) UN Doc A/HRC/RES/48/4 (7 October 2021).

Zimbabwe has ratified international and regional human treaties, including ICCPR in 1991 and the African Charter on Human and Peoples' Rights (African Charter) in 1986. The treaties constitute domestic law to the extent of their domestication.[21] Section 327(6) of the Constitution of Zimbabwe requires courts, when interpreting domestic laws, to interpret the Bill of Rights in a manner that promotes international human rights law binding on Zimbabwe.[22] In the case of *Biri v State*, the Court surmised that

> by ratifying the ICCPR and ACHPR Zimbabwe committed to be bound by those Conventions. Therefore, when Zimbabwean courts and tribunals are interpreting the right to … as provided in the Declaration of Rights, they must take into account the interpretations given to these rights under these Conventions.[23]

Similarly, South African courts are constitutionally compelled to take account of international human rights treaties and decisions when interpreting the Bill of Rights.[24] For both jurisdictions, therefore, any limitations that are imposed on human rights must be consistent with the state's public international human rights law commitments.

The Human Rights Committee General Comment 16 reiterates that any interferences with human rights must be in accordance with the law.[25] The principle of legality is not the same as autocratic legalism where surveillance practices are outside the rubric of lawfulness but clothed in legal semblance. The quality of the law must be impeccable and compatible with the rule of law, meaning that it should first be specified in law, and it should be accessible and allow foreseeability of consequences.[26]

At the African Union (AU) level, the African Charter contains no specific right to privacy.[27] Despite the absence of a specific right to

21 Sec 34 of the Constitution of Zimbabwe, Domestication of International Instruments, states that '[t]he State must ensure that all international conventions, treaties and agreements to which Zimbabwe is a party are incorporated into domestic law'.

22 Sec 327(6) of the Constitution of Zimbabwe states that when interpreting legislation, every court and tribunal must adopt any reasonable interpretation of the legislation that is consistent with any international convention, treaty or agreement which is binding on Zimbabwe, in preference to an alternative interpretation inconsistent with that convention, treaty or agreement.

23 *Felix Biri v The State* Unreported High Court Harare 722-22.

24 Sec 39(1)(b) Constitution of the Republic of South Africa, 1996; compare with Constitution of Zimbabwe sec 46(1)(c).

25 General Comment 16: Article 17 (Right to privacy) The right to respect of privacy, family, home and correspondence, and protection of honour and reputation, adopted at the 32nd session of the Human Rights Committee, 8 April 1988.

26 *Kruslin v France* Application (1990) EHRR 547 para 27.

27 *Chinhamo v Zimbabwe* (2007) AHRLR 96 (ACHPR 2007) was the first case to allege a violation of the right to privacy under the African Charter. The African Commission dismissed the case for failure to exhaust domestic remedies. If the case had proceeded on merits, the African Commission was going to interpret

privacy, the interpretation and application of the African Charter require that state parties duly consider their obligations under international law treaties.[28] In that regard, the African Commission on Human and Peoples' Rights (African Commission) in its protective mandate has interpreted the African Charter to incorporate rights not expressly provided for.[29] Progressively, AU treaties and African Commission resolutions are explicitly recognising the right to privacy.[30] Furthermore, the African Charter contains no specific right to a remedy. However, it is common cause that for every human rights violation there must be a remedy.[31] This right to an effective remedy remains applicable even when states engage in secret surveillance; secrecy does not equate to impunity or exemption from accountability.[32]

3 Legalising surveillance at national level

Both Zimbabwe and South Africa are constitutional democracies. The Constitution of Zimbabwe (2013) was adopted following a political agreement between the ruling and opposition parties after the 2008 violent elections. The Constitution of the Republic of South Africa, 1996 marked the end of an illegitimate apartheid regime. The respective constitutions are the supreme laws, and any inconsistent subsidiary laws and practices are null and void. These constitutions are binding on all levels of government, including

other provisions of the African Charter to make a pronouncement on the right to privacy in Africa. It would not have been difficult to prove the protection of the right to privacy. See A Singh & M Power 'The privacy awakening: The urgent need to harmonise the right to privacy in Africa' (2019) 3 *African Human Rights Yearbook* 202.

28 Art 60 African Charter.

29 *Social and Economic Rights Action Centre (SERAC) & Another v Nigeria* (2001) AHRLR 60 (ACHPR 2001) interpreted the right to housing being deemed as implied in other rights, as one could not enjoy the right to life without the right to food. The African Commission is inconsistent in interpretation of this provision in its promotion mandate. In its ordinary session of November 2022, the African Commission denied observer status for non-governmental organisations working on LGBTIQ rights on the grounds that sexual orientation is not an expressly recognised right or freedom under the African Charter, and contrary to the virtues of African values, as envisaged by the African Charter.

30 African Commission on Human and Peoples' Rights Resolution 326 of 2012 on the Right to Freedom of Information and Expression on the Internet in Africa ACHPR/Res.362(LIX)2016. See also art 10 of African Charter on the Rights and Welfare of the Child (1990) and art 8 of the African Union Convention on Cyber Security and Personal Data Protection (2014).

31 GM Musila 'The right to an effective remedy under the African Charter on Human and Peoples' Rights' (2006) 6 *African Human Rights Law Journal* 441-464.

32 African Commission on Human and Peoples' Rights Resolution on the Deployment of Mass and Unlawful Targeted Communication Surveillance and its Impact on Human Rights in Africa ACHPR/Res.573 (LXXVII) 2023; Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018) para 36.

natural and juristic persons.[33] The right to privacy, which includes privacy of communications, is protected under the Declaration of Rights in Zimbabwe, and the Bill of Rights in South Africa, sections 57 and 14, respectively.[34]

As under ICCPR, the rights in these constitutions are not absolute. The Zimbabwean Constitution notes that the limitation of rights must be 'fair, reasonable, necessary and justifiable in a democratic society based on openness, justice, human dignity, equality and freedom'[35] in addition to other factors and considerations.[36] It is this limitation of rights that is interpreted to mean the authorisation of lawful invasion of privacy through monitoring or interception of communications.[37] Similarly, in South Africa, the limitation clause in section 36(1) of the Constitution emphasises taking into account all relevant factors. Any limitation of the right must be interpreted narrowly, with courts increasingly focusing on the actual impact of the limitation.[38] The courts will not affirm laws that obliterate the right's minimum content. This should also take into consideration the often-invoked national security limitations.[39] Governments tend to regard those opposing its policies as posing national security threats, experiences all too familiar in Zimbabwe's and South Africa's past and current histories. The Zimbabwean and South African Constitutions reinforce the protection of human rights while enforcing national security interests.[40] Any limitation of human rights, including for national security reasons, must 'serve a legitimate purpose, and meet the requirements of suitability, necessity, and proportionality which render [them] necessary in a democratic society'.[41] The restriction chosen must be the least restrictive and must be open to judicial review.[42] Any of the rights limitations must achieve a harmonious

33 Secs 2(1) & 2(2) Constitution of Zimbabwe; sec 2 Constitution of the Republic of South Africa.
34 Before 2013, Zimbabwe's Constitution did not explicitly protect the right to privacy.
35 Sec 86(2) Constitution of Zimbabwe; sec 36(1) Constitution of the Republic of South Africa.
36 *Democratic Assembly for Restoration and Empowerment & Others v Saunyama NO & Others* (2018) ZWCC 9.
37 *Womah Mukong v Cameroon* Communication 458/1991 UNHR Committee UN Doc CCPR/C/51/D/458/1991 (1994).
38 *In re Munhumeso & Others* 1994 (1) ZLR 49 (S) 62F; *S v Makwanyane* 1995 (3) SA 391 (CC) para 104.
39 See Open Society Justice Initiative 'Understanding the global principles on national security and the right to information' (2013).
40 Secs 206(1) & (3)(a) Constitution of Zimbabwe; secs 198(a) & 198(c) Constitution of the Republic of South Africa. The pursuit of national security does not mean that citizens live in fear as any national security interests must be compliant with the international rule of law, and human rights.
41 *Donoso v Panama* IACHR (27 January 2009) Ser C 193 para 56.
42 *Supreme Court of India, Bhasin v Union of India* (2020) Writ Petition (Civil) 1031/2019.

balance of interdependence or interconnectedness of human rights, and this is the essence of adequate safeguards.[43]

4 Regulating surveillance through the Interception of Communications Act

The IC Act was gazetted in Zimbabwe in 2007.[44] The Act provides for lawful interception and monitoring of certain communications, and the establishment of a monitoring centre.[45] The ministerial administration of the IC Act was contested during the 2009-2013 government of national unity. President Mugabe and his party, ZANU PF, refused to hand over the IC Act's administration to an opposition ICT minister.[46] This was a clear demonstration of the importance of this Act in the scheme of power retention. The President has reserved the IC Act administration for the presidency.[47]

The IC Act was amended in 2021 by the Cyber and Data Protection Act, to introduce the Cyber Security and Monitoring of Interception of Communications Centre as a unit in the Presidents' office and a Cyber Security Committee (Committee).[48] The monitoring centre is the sole facility for authorised interception and oversees the enforcement of the IC Act.[49] The director of the monitoring centre is advised by an *ad hoc* advisory Committee on the issuing of warrants,[50] and the minister determines the Committee's conditions of service.[51] This Committee is composed of 11 ministerial appointees from the Postal and Telecommunications Regulatory Authority of Zimbabwe

43 I find the concept of proportionality closely aligned with the idea of a harmonious balance of rights. See C Rautenbach 'Proportionality and the limitation clauses of the South African Bill of Rights' (2014) 17 *Potchefstroom Electronic Law Journal* 2229-2267.

44 Interception of Communications Act: Date of commencement 3 August 2007.

45 From the purpose, the IC Act purports to focus on certain communications, meaning that these must be narrow and not bulk surveillance and interception.

46 'Goche to oversee mail-spying law' *The Zimbabwean* 23 May 2009, https://www.thezimbabwean.co/2009/05/goche-to-oversee-mail-spying-law/ (accessed 8 January 2023).

47 Statutory Instrument 212 of 2018 Assignment of Functions (His Excellency the President of the Republic of Zimbabwe) Notice, 2018. The IC Act, however, can be assigned to the Minister of Transport and Communications or any other minister to whom the President may assign it. Currently, the IC Act is assigned to the President, therefore, technically and administratively, the President is responsible for warrant applications as the IC Act is reserved for his administration.

48 Cyber and Data Protection Act Chapter 12:07 sec 37 Amendment of Cap 11:20.

49 Secs 4A, 4A(a) & 4A(h) IC Act.

50 Sec 4(2) IC Act. The IC Act, however, states that the minister issues the warrant of interception under secs 3(1)-(3) of the IC Act. No person shall intercept communications unless they are authorised by warrant.

51 Schedule and sec 4B(5) IC Act. This is an *ad hoc* committee, and the minister determines the conditions of service. The functional and administrative independence of the committee is compromised.

(POTRAZ); ministries of ICT, Science and Technology, Justice, Defence; Zimbabwe Republic Police (ZRP); National Prosecution Authority; Central Intelligence Organisation (CIO), Prisons and Correctional Service; and a monitoring centre representative. The eleventh member is appointed on an *ad hoc* basis from 'any sector of the economy' or 'any other person who may be necessary to the deliberations' of a warrant.

The authorised warrant applicants are the Chief of Defence Intelligence; Director-General in the President's department for national security (CIO); ZRP commissioner; Zimbabwe Revenue Authority commissioner general or their nominees.[52] These applicants have subordinate representation in the *ad hoc* Committee, which compromises their subordinates' capacity to disagree or differ with their principals' directives or even authorised applicants. The minister refers the application for a warrant to the Committee to advise on grounds for issuance of a warrant.[53]

The minister only issues a warrant of interception upon being satisfied of the existence of certain grounds under the IC Act. First, the warrant is issued on the grounds of reasonable suspicion of commission of a serious offence; or, second, for gathering of information concerning an actual threat to national security; or, lastly, for any compelling economic interest and gathering information concerning potential threat to public safety or national security.[54] However, the minister can provisionally authorise interception, which can be withdrawn without prejudice if the Committee advises that there are no grounds to issue a warrant.[55] The warrant is issued *ex parte*. The warrant is initially valid for three months, and renewable for another three months. Any further renewal must be in consultation with the Attorney-General or through an Administrative Court *ex parte* application.[56]

Under sections 9(1)(a) to (b) of the IC Act telecommunications service providers must install infrastructure that enable interception of communications.[57] More importantly, the expense of installing this equipment is borne by the service provider in terms of section 12(4) of the IC Act. This interception capability has to allow for real-time and full-time monitoring, with more than one interface and capability for

52 Sec 5 IC Act.
53 The IC Act sec 4(2) as amended suggests that the warrant advice is given to the director by the Cyber Security Committee established under sec 4B(1).
54 Secs 6(1)(a)-(c) IC Act.
55 Secs 3(4) & 4B (8) IC Act.
56 Sec 7(2) IC Act.
57 Secs 9(1)(a)-(b) IC Act.

simultaneous interceptions by more than one authorised person.[58] In addition to real-time monitoring, service providers are also required to collect personal information for the identification of customers upon registration for services.[59]

For purposes of enhancing secrecy of the surveillance, neither service providers nor their employees are permitted to disclose any information obtained through surveillance.[60] This reduces the prospects of a person under surveillance to challenge the process. If at any point intercepted information is encrypted, the government can order that the communications are subject to decryption based on a notice of disclosure.[61] The service provider must ensure that the decrypted information is intelligible,[62] and any costs associated with the decryption incurred by the service provider are reimbursed by the state.[63] Equally, if there are call diversions, service providers must provide access to such calls.[64] The IC Act provides for the destruction of intercepted information. The disposal of the information is in terms of section 11(7) of the IC Act. The destruction of the information is without any form of disclosure to the targeted individual of the nature, content and duration of the interception. Anyone aggrieved by the issuance of a warrant for interception can appeal to the Administrative Court within 'one month of being notified or becoming aware of it' as provided in section 18(1) of the IC Act. This provision assumes (i) that the IC Act has a notification procedure, and (ii) that the issuance of warrants has mechanisms for disclosing the actual warrants issued. This certainly is not the case. The issued warrants are only reviewed each year by the Attorney-General, and mandatory directions are given to the minister on future authorisations for interception.[65]

5 Summary of issues in *AmaBhungane*

In South Africa, RICA regulates the interception of communications.[66] However, the constitutionality of the RICA provisions was contested before the Constitutional Court in the *AmaBhungane* case.[67] Briefly, the facts of this case were the following: In 2008, Mr Sole, a long-

58 Secs 9(h)(i)-(ii) IC Act. The identities of the agents must not be disclosed to any unauthorised person in terms of sec 16 IC Act.
59 Sec 10 IC Act.
60 Sec 16 IC Act.
61 Sec 11 IC Act.
62 Secs 11(4)(b) & 11(8) IC Act.
63 Sec 13(4) IC Act.
64 Secs 9(1)(c)-(d) & 9(1)(g) IC Act.
65 Secs 19(1)-(3) IC Act.
66 Other laws include the National Strategic Intelligence Act 30 of 1994 and the Intelligence Services Control Act 40 of 1994.
67 *AmaBhungane* (n 5).

standing investigative journalist, suspected that his communications were being intercepted and that he was under surveillance. In 2009 he approached the Inspector-General of Intelligence in an attempt to determine whether he was under surveillance. The Inspector-General refused to confirm his suspicion, only indicating that no wrongdoing had been established on the part of the National Intelligence Agency or the police.[68] This tacit confirmation was not sufficient to constitute grounds to appeal or challenge the surveillance. Fortuitously, in 2015 and in a separate matter, court transcripts confirmed that Mr Sole was the target of communications surveillance.[69] On this basis, Mr Sole approached the High Court challenging RICA's shortcomings in providing safeguards.[70] The High Court made six specific orders in respect of RICA.[71] The first order declared sections 16(7), 17(6), 18(3)(a), 19(6), 20(6) and 21(6) unconstitutional for failing to provide for a notification regime. The declaration of invalidity was suspended for two years to allow parliamentary processes to cure the defect and provided alternative sections on a notification regime to be followed.[72] The second order nullified the 'designated judge' definition and provided alternative wording pending rectification by Parliament. The third and fourth orders declared sections 16(7), 35 and 37 unconstitutional for inadequate safeguards on *ex parte* applications of warrants for interception, and the failure to prescribe proper procedures for handling of intercepted information. The fifth order held sections 16(5), 17(4), 19(4), 21 (4)(a), and 22(4)(b) unconstitutional for failure to consider the circumstances when the subject of surveillance is a lawyer or a journalist. In orders three, four and five, the High Court provided directions to cure the defect pending Parliament's amendment of RICA. The final order declared bulk surveillance activities and foreign signals interception undertaken by the RICA National Communications Centre unlawful and invalid.

The High Court decision in *AmaBhungane*[73] was taken for confirmation before the Constitutional Court. The Constitutional Court largely upheld the High Court decision. It was held by the Constitutional Court that RICA provisions were unconstitutional for failing to (a) provide for safeguards to ensure that a judge designated in terms of section 1 is sufficiently independent; (b) provide for

68 *AmaBhungane* (n 5) para 13.
69 *AmaBhungane* (n 5) para 14.
70 *AmaBhungane* (n 5) para 15.
71 *AmaBhungane Centre for Investigative Journalism NPC & Another v Minister of Justice and Correctional Services & Others* 2020 (1) SA 90 (GP).
72 *AmaBhungane* (n 5) para 3, noting the relief granted by the High Court as the full order, which cannot be reproduced here in full.
73 *AmaBhungane* High Court (n 71).

notifying the subject of surveillance of the fact of their surveillance as soon as notification can be given without jeopardising the purpose of surveillance after surveillance has been terminated; (c) adequately provide safeguards to address the fact that interception directions are sought and obtained *ex parte*; (d) adequately prescribe procedures to ensure that data obtained pursuant to the interception of communications is managed lawfully and not used or interfered with unlawfully, including prescribing procedures to be followed for examining, copying, sharing, sorting through, using, storing or destroying the data; and (e) provide adequate safeguards where the subject of surveillance is a practising lawyer or journalist. In addition, the Constitutional Court suspended the enforcement of the provisions for 36 months to 'afford Parliament an opportunity to cure the defect causing the invalidity'.[74] Pending the amendment process in Parliament, the Constitutional Court made specific directives operational as provisions to be read into RICA for disclosing the identity of a subject of surveillance to the designated judge if such subject is a lawyer or journalist. Further, the Constitutional Court ordered that a post-surveillance notification procedure be implemented, whereby a subject may be informed 90 days after the surveillance, and a designated judge or magistrate must be notified 15 days thereafter.[75]

Many of these provisions in RICA, which the *AmaBhungane* case found to be unconstitutional, are similar to IC Act provisions. A few sections in both RICA and the IC Act will suffice to exemplify the uncanny similarity of the provisions. In terms of section 16(7) of RICA, 'an application must be considered, and an interception direction issued without any notice to the person or customer to whom the application applies and without hearing such person or customer'. This section in RICA was found unconstitutional as it failed to provide safeguards for *ex parte* applications and is similar to sections 6 and 7 of the IC Act on the issuing of a warrant and the scope of warrant renewal. The warrant applications are carried out as *ex parte* applications without the knowledge of the surveillance target in terms of section 9(1)(i) of the IC Act. Further, section 6 of the IC Act does not provide, as ruled in the *AmaBhungane* case, the circumstances where a subject of surveillance is either practising lawyer or a journalist, resulting in the nullification of several RICA sections.[76] The RICA and IC Act provisions fail to preserve legal

74 *AmaBhungane* (n 5) para 157.
75 As above.
76 *AmaBhungane* (n 5) para 3.

privilege in respect of lawyers and their clients, and preserve the confidentiality of the sources of investigative journalists.[77]

The IC Act contains no specific provisions on the destruction or storage of intercepted information. In terms of sections 11(7)(b) and 17 of the IC Act, an authorised person or nominees designated in section 5(1) of the IC Act can destroy all records of the disclosed information if in their opinion no criminal or civil procedures will be instituted in connection with the records or the records will not be required for any criminal or civil proceedings. The IC Act fails to give specific guidance on the destruction or storage of the information, and in fact this provision obliterates any remedial prospects, in the unlikely event of the interception target being aware of the surveillance, as all evidence might be destroyed. In *AmaBhungane* sections 35 and 37 of RICA were found contrary to the Constitution of South Africa for failing to implement safeguards regarding the destruction or storage of information obtained from interceptions. The RICA and IC Act provisions on storage or destruction of interception communications have similar implications, which constitute a violation of the right to privacy. Personal information collected from surveillance, once aggregated and stored or destroyed without proper safeguards, has the capacity to disclose intimate details and profiles of subjects of surveillance resulting in privacy invasion.[78] The risk of such violations is exacerbated if the laws do not provide for notification to the interception targets.

The various sections of the IC Act, in particular sections 6, 7, 11, 14, 15 and 19 that relate to the issuing of warrants, the renewal of warrants, the destruction of intercepted communications and review of ministerial powers, do not require the notification of the interception target. These provisions are similar to the absence of a notification regime in RICA, which the Constitutional Court held unlawful, thereby nullifying sections 16(7), 17(6), 18(3)(a), 19(6), 20(6), 21(6) and 22(7) for failure to articulate valid post-surveillance notification. These provisions were not providing sufficient safeguards. The IC Act allows for bulk surveillance in terms of section 9(1)(a) in that the interception occurs at all times, and stores all call-related information in terms of section 12. In *AmaBhungane* the Court observed that there were no lawful provisions authorising bulk interception as neither RICA nor the National Strategic Intelligence

77 *Big Brother Watch & Others v The United Kingdom* ECHR (25 May 2021) Applications 58170/13, 62322/14 and 24960/15) para 442: 'The safeguards to be afforded to the press are of particular importance, and the protection of journalistic sources is one of the cornerstones of freedom of the press.'

78 Mavedzenge (n 2) 363.

Act[79] relied upon by the state authorised bulk interception. It can be argued that the bulk surveillance provisions in the IC Act should include notification and limitation requirements at least as strict as those for targeted, specific interceptions. Without these safeguards, bulk surveillance would be unconstitutional. Unlike RICA, which has judicial oversight in terms of warrants of interception applications, the IC Act provides for warrants to be made before the minister in terms of section 5(2). This provision in the IC Act certainly is unconstitutional to the extent that it fails to provide for an independent and impartial judicial authority. RICA provides for a designated judge, whom the Constitutional Court has held, under section 1 of RICA, to be sufficiently independent to exercise judicial oversight.

6 Enhancing implementation of adequate safeguards

6.1 Overview of surveillance laws and safeguards

Ordinarily, laws such as RICA and IC Act are designed to allow lawful, legitimate and proportionate interception of personal communications. These laws constitute the basis for limitation of rights as enshrined in sections 86(2) and 36(1) of the Constitutions of Zimbabwe and South Africa, respectively. It is assumed that these laws have sufficient safeguards to inhibit excessive conduct by anyone, especially state agents. However, these laws and others, such as national data protection laws, are often inadequate or make broad exceptions for law enforcement and intelligence agencies.[80] *AmaBhungane* contributes to the debate and development of an understanding of what constitutes adequate safeguards on interception and surveillance of communications. The Court declared section 16(7) of RICA unconstitutional insofar as it does not provide adequate safeguards for *ex parte* interception orders. The use of *ex parte* applications is designed so as not to alert the subject of surveillance. However, there are risks of abuse of this process, as observed in *AmaBhungane*, that surveillance on journalists was based on 'blatant mendacity'[81] and 'unadulterated lies'.[82] The risk of abuse of RICA provisions demonstrates the general deficiencies and

79 National Strategic Intelligence Act 39 of 1994.
80 United Nations General Assembly Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, AHRC/51/17 4 August 2022 para 49.
81 *AmaBhungane* (n 5) para 41.
82 *AmaBhungane* (n 5) para 96.

requires better safeguards to limit the chances of unlawful privacy intrusions.[83]

The IC Act authorises bulk surveillance and real-time data collection and, if there are no safeguards of data processing, subjects of surveillance are likely to suffer harm. The proposed safeguards in RICA were designed to address these harms. What is important to observe is that collected data must have safeguards on how it is processed or destroyed. The RICA provisions were deemed insufficient in so far as they were not clear regarding the discretion to store or delete under section 35. In the event that a subject of surveillance intends to challenge the interception orders, they will need access to the information collected and stored. However, RICA 'needs to be clear on the parameters and exercise of discretion'[84] of what is kept or destroyed. The Constitutional Court should have also referred to the various provisions of the Protection of Personal Information Act (POPIA).[85] The South African Constitutional Court was laying grounds of what is required for a subject of surveillance to vindicate their rights in future, and the absence of clear parameters on data storage and destruction shows a lack of adequate safeguards. In essence, sections 35 and 37 of RICA on information management, if read with section 16(7), which forbids disclosing interception information to the surveillance target, mean that the individual under surveillance will remain unaware. This perpetual secrecy in RICA creates grounds for suspecting that the law is being and will be abused. If the objective of the surveillance was a legitimate interest, there should be no reason for not informing the subject of surveillance. This reasoning applies to the IC Act whose provisions in sections 9, 11, and 17 prohibit disclosure of identities of monitoring agents, interception targets, destruction of collected information without any parameters or safeguards. In terms of the Cyber and Data Protection Act, Zimbabwe must have adequate safeguards for all processed data.[86]

The additional safeguards proposed in *AmaBhungane* reinforce existing international surveillance principles. The safeguards start with

83 *AmaBhungane* (n 5) para 99.
84 *AmaBhungane* (n 5) 103.
85 South Africa Protection of Personal Information Act 4 of 2013.
86 Zimbabwe Cyber and Data Protection Act 12:07. Sensitive personal information includes information about financial, criminal data. Sensitive personal information has additional safeguards when collecting, such as consent unless in terms of sec 11(5)(d) if the processing is necessary for national security laws. National security laws are not listed in the Cyber and Data Protection Act, but one analysis of the IC Act might constitute a security law. That said, I hold the view that data collected for national security purposes under the IC Act must be provided, and data protection safeguards under secs 18(1)-(5) and 24 of the Cyber and Data Protection Act.

the requirement of reasonable suspicion, preventing indiscriminate targeting that has led to discriminatory surveillance and profiling of specific groups.[87] The ordinary safeguards of reasonable suspicion are again not enough, especially if the laws allow for *ex parte* applications or contain no notification requirements. The reasonability clause, as observed by privacy advocates, allows for too low a threshold for interference with an individual's privacy, and this provision can be abused to justify unlawful surveillance practices.[88] While the Constitutional Court did not address this issue, future amendments to RICA must incorporate grounds to issue a warrant of interception not on reasonable suspicion only but on a higher degree of probability as that will deter the malicious use of surveillance.

AmaBhungane reinforces the importance of any form of surveillance being subjected to independent oversight and effective safeguards. Independent oversight can take various forms, with judicial oversight being the most commonly used, alongside other mechanisms such as executive and legislative oversight.[89] The type of oversight may not be contested; rather, the Court focused on its effectiveness, noting that without it, impunity prevails and further abuses are encouraged.[90] In my analysis, any form of oversight provided under South Africa's RICA or Zimbabwe's IC Act must, at the very least, be an entity with functional and administrative independence removed from the executive, especially any political interests. In addition to functional and administrative independence, the oversight mechanisms must be capable through the enabling laws to demand and enforce 'end-to-end'[91] safeguards. This simply means that during authorisation, execution, after termination of surveillance, and throughout the data life cycle, adequate safeguards exist to protect against state excesses.[92] The safeguards include post-surveillance notification, which in my analysis must include judicial determination of whether, if at all, there are risks of jeopardising ongoing investigations, as law enforcement agents can be arbitrary in their determination.[93]

87 The developments in the US following the 11 September 2001 attacks caused Muslims or anyone suspected of being such and of Arab origin to be profiled and in some instances attacked. C Mala Corbin 'Terrorists are always Muslim but never white: At the intersection of critical race theory and propaganda' (2017) 86 *Fordham Law Review* 455.

88 A Mare & J Duncan 'An analysis of the communications surveillance legislative framework in South Africa' Media Policy and Democracy Project (November 2015) 22.

89 Mavedzenge (n 2) 378-383 discussing the different oversight approaches as executive, judicial and a hybrid of executive and judicial.

90 *AmaBhungane* (n 5) paras 41-42.

91 *Big Brother Watch* (n 77) para 351.

92 As above.

93 *AmaBhungane* (n 5) para 89.

Post-surveillance notification constitutes a form of transparency report, and even service providers have a responsibility to inform users regarding government requests for access to their personal communications.[94] Unfortunately, in South Africa and Zimbabwe there are no provisions for telecommunications providers to notify users and, in fact, RICA and the IC Act prohibit disclosure. In South Africa, privacy advocates established that the three largest telecommunication operators disclosed a minimum estimate of 70 000 subscribers' call records each year to law enforcement.[95] If undertaken, notification to the subject of surveillance will include disclosure of the identity of government agencies and number of authorisations granted, including whether unauthorised interception took place.[96] Post-surveillance notification and transparency reports should all include external government requests as countries share intelligence.[97]

Another emerging concern with surveillance is the transnational surveillance in which governments share intelligence either as part of mutual cooperation frameworks or clandestine cross-border operations. To prevent abuse through data sharing and transfers, laws must set out safeguards for both sending and receiving states.[98] As governments routinely share information, the safeguards must address transnational data sharing as this will reduce secretive transnational surveillance through government information-sharing agreements that lack independent oversight.[99] The transnational surveillance has also affected civil society activists, journalists and

94 UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021).

95 H Swart 'Cell phone privacy: Law enforcement pulls 70 000 subscribers' call records each year and that's a minimum estimate' *The Maverick* 23 August 2017, https://www.dailymaverick.co.za/article/2017-08-23-cell-phone-privacy-law-enforcement-pulls-70000-subscribers-call-records-each-year-and-thats-a-minimum-estimate/#.WfCO40zMxTY (accessed 11 July 2023).

96 Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016) para 43 noted that South Africa should increase the transparency of its surveillance policy. The Global Principles on National Security and the Right to Information (Tshwane Principles), Open Society Foundations, 2013.

97 Open Society Foundations 'Globalising Torture CIA Secret Detention And Extraordinary Rendition', 2013. Zimbabwe was involved on numerous occasions in the rendition of several suspected Al Qaeda terrorists who were later released without prosecution.

98 Provisions of the Cyber and Data Protection Act 2021 and Protection of Personal Information Act 2013 would apply to data transfers.

99 This is the principle of adequate protection in data transfers. See *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* (C-311/18), Judgment, Grand Chamber, Court of Justice of the European Union (16 July 2020). Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014).

political opponents, as seen, for instance, in the widely publicised *Pegasus* case.[100]

The above summarises some of the adequate safeguard principles, which are not new interpretations of the established limitations, but serve as a reinforcement of the understanding of what constitutes acceptable limitations and associated safeguards. When this analysis is applied against the IC Act provisions, one will come to the inescapable observation that there are several constitutional and human rights compliance gaps. This article cannot exhaust all the issues in the IC Act, but uses a comparative approach based on the above RICA provisions and discussion of the *AmaBhungane* judgment. For purposes of this chapter, the gaps are categorised under three interconnected headings, namely, powers of surveillance, oversight of surveillance and remedies for surveillance.

6.2 Powers of surveillance

The IC Act provides powers and grounds for the lawful interception of communications and carrying out surveillance. These powers must not be unregulated and are based on reasonable suspicion which, although insufficient, creates a basis for surveillance.[101] The issuance of warrants based on reasonableness is designed to safeguard against arbitrariness and malicious use of surveillance powers. However, this is only effective if an independent judicial authority considers the reasonable suspicion requirement, other than an individual with executive authority.[102] The IC Act authorises two forms of surveillance. The first relates to certain targeted communications through a warrant, which is targeted under sections 5 and 6, and second to real-time and all-time bulk surveillance under section 9. The surveillance under section 9 is framed in such a way that a service provider must install facilities and devices that enable interception of communication at all times or when so required. Further, the IC Act provides that service providers in their assistance must have services capable of rendering real-time and full-time monitoring facilities. In terms of the IC Act, these facilities must provide all call-related information, meaning that meta data is collected.[103]

100 'Revealed: Leak uncovers global abuse of cyber-surveillance weapon' *The Guardian* 18 July 2021, https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus (accessed 11 July 2023).
101 IC Act Preamble, sec 6 Issue of warrant.
102 *Kruglov & Others v Russia* ECHR 4 February 2020 App 11264/04 para 125.
103 Sec 9(1)(d) IC Act.

The first form of surveillance is based on a warrant of interception obtained through application before the responsible minister, in terms of sections 5 and 6 of the IC Act, by authorised persons. The authorised persons in terms of section 5 of the IC Act are all security agents, except the Commissioner-General of Zimbabwe Revenue Authority, responsible for taxes. Following the amendment of the IC Act in 2021, the minister is now advised on issuing warrants by an *ad hoc* committee composed of ministerial appointees. The *ad hoc* ministerial appointees include representatives of ZRP, CIO (President's office department responsible for national security), and Ministry of Defence and War Veteran Affairs.[104] These representatives are identical to the individuals authorised to issue warrants. In my view, there is no distinction between the persons desiring the interception and the persons approving it. I would agree with South African High Court Judge Sunderland in *AmaBhungane* when the Court expressed the need for safeguards as those constituted or available through an independent authority that approves interceptions. Sunderland J noted that 'this model, in which the person desiring the interception is distinct from the person authorising it, is designed to prevent, as far as possible, abuse of the system'.[105] The IC Act fails the basic test of differentiating between the authorised persons, from the approving minister to the *ad hoc* advisory committee advising the minister.

The powers of surveillance granted to the minister under the IC Act are neither restrained nor subjected to an independent oversight. This position was reaffirmed in the Lesotho case of *Mofomobe and Shale*[106] where section 26(2) of the National Security Services Act on the issuing of warrants was challenged on constitutional grounds. The Lesotho High Court held that 'there are no safeguards to guard against abuse of the power to issue warrants'. In fact, the issuance of warrants under section 26(2) is presided over by a minister without external independent supervision and lacks the necessary safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse.[107] The *ad hoc* committee members, under the IC Act, do not constitute external supervision. They are from the same offices as the person authorised to apply for warrants and, as such, are unlikely to object to warrants requested by their offices or superiors. In *AmaBhungane*, the Constitutional Court referenced the *Mistry* case,[108] which dealt with warrants of search and seizure, stating:

104 Sec 4B(2)(a) IC Act.
105 *AmaBhungane* (n 71) para 35.
106 *Mofomobe and Shale v The Prime Minister & Others* [2023] LSHC 125.
107 *Mofomobe* (n 106) para 81.3.
108 *Mistry v Interim National Medical and Dental Council & Others* 1998 (4) SA 1127 CC para 25.

> The existence of safeguards to regulate ways in which state officials may enter the private domains of ordinary citizens is one of the features that distinguish a constitutional democracy from a police state … when it came to … security legislation, vast and often unrestricted discretionary powers were conferred on officials and police. Generations of systemised and egregious violations of personal privacy established norms of disrespect for citizens that seeped unto public administration and promoted amongst a great many officials habits and practices inconsistent with the standards of conduct now required by the Bill of Rights.

The *Mistry* rationale in *AmaBhungane* is relevant for Zimbabwe, as security agents are notorious for selective and partisan acts, and unrestricted discretionary conduct violating the Constitution.[109] Even with the passage of the Zimbabwe Independent Complaints Commission Act, the security agencies remain unchecked as the IC Act is administered and assigned to the President in terms of section 2(2).[110] Section 6(2) of the IC Act allows the minister to order something other than a warrant of interception. The IC Act s6(2)(a) provides that the 'minister may, if he or she is of the opinion that the circumstances so require upon an application being made, issue instead of warranting any directive to a service provider not involving any interception or monitoring of communications'. This ministerial directive is not based on reasonable suspicion because it is not a warrant issued in terms of section 6(1) of the IC Act. This provision, undeniably, is wide, vague and susceptible to abuse.

In *Azer Ahmadov v Azerbaijan* the European Court of Human Rights noted that

> as secret surveillance is a serious interference with a person's right to respect for private life, the judicial authorisation serving as the basis for such surveillance cannot be drafted in such vague terms as to leave room for speculation and assumptions with regard to its content and, most importantly, with regard to the person in respect of whom the measure is being applied.[111]

True to form, the minister, acting under section 6(2) of the IC Act, ordered a nationwide internet shutdown on 14 January 2019 stopping all forms of internet and network communications.[112] On 16 January 2019, Econet wireless sent a message to its subscribers indicating that it had received a warrant from the Minister of State in

109 Secs 208(2)(a)-(d) Constitution of Zimbabwe.
110 Sec 210 of the Constitution of Zimbabwe establishes the Zimbabwe Independent Complaints Commission Act 5 of 2022.
111 *Azer Ahmadov v Azerbaijan* ECHR (22 July 2021) App 3409/10.
112 A Mare 'State-ordered internet shutdowns and digital authoritarianism in Zimbabwe' (2020) 14 *International Journal of Communication* 4244-4263.

the President's Office for National Security through the CIO Director-General to suspend all networks and internet service.[113] Despite this bold disclosure, Econet enforced the patently defective warrant. This decision was challenged in court, resulting in an order for suspending the decision.[114] The IC Act does not provide for internet shutdowns, and a minister or even the President, who administers the IC Act, cannot issue such a directive or warrant.[115]

The courts in Zimbabwe have previously dealt with wide surveillance powers in the *Law Society of Zimbabwe v Minister of Transport and Communications*.[116] In this case, the Law Society of Zimbabwe objected to sections 98(2) and 103 of the Postal and Telecommunications Act which authorised bulk interception of communications.[117] The Supreme Court ruled that this Act had granted wide powers to the President and violated common law practice of lawyer-client confidentiality.[118] This Act authorised the President to order interception of communications, if the President thought it was necessary in the interests of national security or necessary for the maintenance of law and order.[119] The President was empowered, after consultation with the minister, to issue general directives to service providers 'as appear to the President to be requisite or expedient in the interests of national security or relations with the government or territory outside Zimbabwe'.[120] Once issued, the service provider was required to comply, 'notwithstanding any other duty imposed on him by or under this Act'.[121] While this case dealt with lawyer-client confidentiality, the Court observed that lawyers did not have an absolute right to privacy of their communications, but there must be oversight and safeguards against such interception as they could violate the rule of law.[122] This executive unaccountability continues under the IC Act in that interception warrants are authorised by the minister, after advice from an *ad hoc* committee constituted of representatives from the executive members of an Act administered by the President.[123]

113 'Zimbabwe's biggest mobile operator Econet says ordered to shut down internet' *Reuters* 18 January 2019.
114 *Zimbabwe Lawyers for Human Rights v Minister of State for National Security* HC265/19. The order did not address the merits or otherwise of the shutdown.
115 MISA Zimbabwe statement, https://zimbabwe.misa.org/2019/01/21/high-court-sets-aside-internet-shut-down-directives/ (accessed 16 January 2023).
116 Law Society of Zimbabwe (n 12).
117 As above.
118 As above.
119 Sec 98(2) Postal and Telecommunications Act.
120 Sec 103(1) Postal and Telecommunications Act.
121 Sec 103(3) Postal and Telecommunications Act.
122 Law Society of Zimbabwe (n 12).
123 Statutory Instrument 212 of 2018 (n 47).

The second form of surveillance is bulk surveillance, carried out constantly with or without a warrant of interception. The IC Act clearly enables wide and vague surveillance powers going beyond targeted 'certain communications'[124] to permanent interception through real-time and full-time monitoring facilities installed in service providers' systems, and permanent capacity to direct internet disruption.[125] The prospects of interception at all times and full-time monitoring render meaningless the application of a warrant with a time duration. The authorities can request communications records, which are supposed to be available at the full-time monitoring facilities. Of course, the interpretation of these provisions on bulk surveillance might be read as ordinary interception with a warrant authorisation, but safeguards will still be required. Section 9 of the IC Act authorises 'interception at all times', meaning that this might be carried out even when there is no reasonable suspicion of an offence being committed. This provision allows for what the United Nations (UN) called 'just in case' data collection, which is not necessary and certainly disproportionate.[126] Admittedly, bulk surveillance can be conducted as a preventative measure rather than for the investigations of specific criminal activity, as noted in the *Big Brother* case.[127] This notwithstanding, the law must provide clear indications on when bulk surveillance can be conducted; the circumstances for conducting bulk surveillance; a clear authorisation and supervision procedure; how the information is safeguarded during collection; time limits for the interception; *ex post facto* review and remedial powers in competent bodies.[128] The IC Act fails to provide oversight on bulk surveillance powers.

6.3 Oversight of surveillance

Surveillance oversight constitutes various ways of holding any intelligence gathering practices publicly accountable, and it takes different forms, such as internal oversight, parliamentary oversight and external independent oversight.[129] Given the significant role of the executive in issuing warrants, providing advice on warrants, and the lack of a judicial role in the IC Act, this article contends that judicial oversight is the most effective means of preventing abuses

124 IC Act Purpose as amended.
125 Secs 9(1)(a)-(c) & (g) IC Act as amended.
126 Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014) para 26.
127 *Big Brother Watch* (n 77) Application para 59.
128 *Big Brother Watch* (n 77) para 361; *Centrum för rattvisa v Sweden* ECtHR, (25 May 2021) para 262.
129 Mavedzenge (n 2).

in surveillance laws. The first instance of oversight is the exercise of power to issue warrants of interception.

The IC Act contains limited judicial involvement in the issuance of warrants.[130] This should not be the case. Interception warrants must be issued by a court of law. The IC Act involves the Administrative Court in adjudicating on *ex parte* renewals of warrants after the first initial six months.[131] This is insufficient to cure any maladies in the first warrants. If oversight on warrants of interception is effective, then an independent entity must authorise the interception of warrants. To constitute sufficient oversight, I believe that the independence required for oversight is a body independent of the executive and is one that enables verifying that reasonable suspicion existed for the issuing of a warrant of interception. This position was reinforced in *Liblik & Others v Estonia* where the European Court of Human Rights ruled that the authority empowered with authorising the use of secret surveillance must be 'capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures'.[132]

In my view, the minister is functionally incapable of certifying the existence of a reasonable suspicion. This, however, is not to rule out that ministerial oversight might in some instances be effective. For Zimbabwe, however, there are grounds for apprehension as ministers do not follow consistent judicious interpretation of each of the terms of the warrant, nor are they capable of legally verifying if sufficient reasons exist to institute a warrant of interception. The IC Act requires all these processes to be done secretively, which minimises the demand for accountability from the subject of surveillance and from other accountability platforms such as Parliament.[133] The oversight of secretive processes is difficult.

The second stage of oversight is during the interception of communication. Section 7(1) of the IC Act provides that targeted interception warrants are initially valid for three months and bulk interception is both ongoing and real-time as there are no time limits. The minister will be unable to evaluate the volume of information gathered over the three months or determine whether it is adequate

130 The only time a court is involved in the issuance of a warrant is during the renewal of a warrant which can be done before the Administrative Court as an *ex parte* application in terms of IC Act secs 7(2)(b), 7(3), 7(4).
131 Secs 7(2)-(4) IC Act as amended.
132 *Liblik & Others v Estonia & 5 Others* ECHR App 173/15 (28 May 2019).
133 Secs 9(1)(j)-(k) IC Act.

to support investigations and the prosecution of a criminal offence. If the IC Act had provisions such as more regular reporting to a court or a judge on the carrying out of the interception warrant and specific information being collected, this would reduce the propensity to abuse surveillance powers. Once the warrant under section 6 of the IC Act expires, it can be renewed by the minister for another three months or by the minister in consultation with the Attorney-General in terms of sections 7(1)(a)(i) and 7(1)(a)(ii) of the IC Act. Upon expiration of six months, the authorised person needs to seek extension in terms of section 7(2)(a) of the IC Act, again before the minister in consultation with the Attorney-General, for specified purposes of addressing criminal groups; gathering information concerning an actual threat to national security or economic interests; and information concerning potential public safety threats or national security. These are two executive offices and cannot reasonably be considered independent in any sense. The Administrative Court, upon showing good cause through an *ex parte* application by the authorised person, can extend the warrants in terms of sections 7(2)(b), 7(3) and 7(4).

The last stage of oversight is data management and when surveillance is terminated. The data storage arose in *AmaBhungane* and references to other global practices were made.[134] This stage shows the importance of enforcing data safeguards throughout the surveillance cycle. If the data is retained, there should be sufficient safeguards that the information is not used for other purposes, especially as the IC Act allows for simultaneous interception and sharing of data among authorised persons.[135] The UN Human Rights Committee made this observation on RICA in 2016 prior to *AmaBhungane*. The Committee was concerned about the wide scope of the data retention regime and recommended that South Africa consider revoking or limiting the requirement for mandatory retention of data by third parties.[136]

Considering that the IC Act holds secrecy of the interception essential, at the very minimum, if the information is destroyed, there must be notification of the subject of surveillance. Notification

134 *AmaBhungane* (n 5) para 107 citing *Weber v Germany* (2008) 46 EHRR 5, [2006] ECHR 1173 para 95.

135 The Zimbabwe Electoral Commission allegedly shared the entire voter's roll information with the ZANU PF ruling party, in the run-up to the 2018 elections, resulting in ZANU PF sending indiscriminate messages. This confirmed unofficial sharing of data between government agencies and ruling party; *News Day*, https://www.newsday.co.zw/2018/07/zanu-pf-breaks-into-zec-database/ (accessed 14 September 2022).

136 Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016).

is required as a measure of accountability, except in cases where a court determines that there are security risks. If notification is not provided, another level of accountability is that the law must provide for standards on safeguarding the integrity and confidentiality of the data, even if destroyed. In *AmaBhungane*, RICA was found to contain limited safeguards to ensure that personal data obtained through interception is lawfully managed and not abused.[137] This finding is relevant for the IC Act, as a reading of its provisions indicates limited, if not non-existent, safeguards and guarantees on data handling.

While other laws such as the Cyber and Data Protection Act, section 18, might cure this limitation through technical and organisational measures, the Cyber and Data Protection Act is a 2021 development, and the IC Act of 2007 needs to pronounce itself on this subject.[138] There is ample guidance from other jurisdictions. For instance, the Court of Justice of the European Union (EU) resolved that rules relating to the security and protection of data retained by providers of electronic communications services must take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data.[139]

In summary, every surveillance law must provide for oversight allowing for a measure of foreseeability to protect against arbitrary interference.[140] The law must be clear giving citizens 'adequate indication of the conditions and circumstances in which the authorities are empowered to engage in secret surveillance'.[141] Statutory provisions should include safeguards that restrict the scope and duration of surveillance to prevent mission creep and the misuse of personal data.

6.4 Remedies in case of unlawful surveillance

In the event that the authorised persons conduct surveillance, which does not meet the standards of restrained powers and there is no oversight, one might contend that such surveillance becomes unlawful. For these reasons, any law authorising the restriction of

137 *AmaBhungane* (n 71) para 108.
138 Sec 18 of the Cyber and Data Protection Act of 2021 in Zimbabwe requires technical and organisational measures to be adopted by data controllers and data processors. Technically, service providers are processors, and the data controller would be the monitoring centre.
139 *Tele2 Sverige AB v Post-och telestyrelsen* (C-203/15); *Secretary of State for the Home Department v Tom Watson & Others* (C-698/16), CJEU (21 December 2016) para 122.
140 *Centrum for rattvisa* (n 128).
141 *Malone v United Kingdom* 82 ECHR 10 para 67.

a right must provide for effective judicial remedies. Remedies must ordinarily be of a judicial nature, such that they constitute effective and not illusory remedies. This is not to discount non-judicial remedies as long as they provide the needed relief and guarantee non-recurrence. However, informed by Zimbabwe's experience, any remedy must be judicial in nature. In addition, oversight must also be of a judicial nature. If non-judiciary oversight is adopted, these must be 'independent of the authorities carrying out the surveillance' and 'vested with sufficient powers and competence to exercise an effective and continuous control'.[142]

The IC Act in section 18(1) provides for judicial appeal against anyone aggrieved by a warrant or directive. This provision is insufficient. First, the IC Act operates on executive decrees, and a service provider is unlikely to challenge this directive. The authority (POTRAZ) responsible for the registration part supervision of interceptions is also responsible for the licensing of services providers. This licensing is susceptible to cancellation, revocation and variation by the President in consultation with the minister.[143] Therefore, non-judicial remedies from service providers are unlikely, as they are unlikely to challenge government directives. That notwithstanding, service providers must adopt procedures to enable their users to seek remedies, including attending to data breaches, and informing users when the government demands access to data or issues directives.[144] A grievance mechanism can complement the judicial oversight mechanism.

The proposed appeal under section 18(1) is merely superficial, as it is unclear how an individual would become aware of the warrant or directive, given that the IC Act criminalises any disclosure of the surveillance process. Section 16(7)(a) of RICA is similar to section 16(2) of the Zimbabwean IC Act, which denies disclosure. To its credit, the IC Act anticipated some form of disclosure or knowledge of interception warrants as section 18(1) provides that anyone aggrieved by the interception warrant can appeal to the Administrative Court within 'one month of being notified or becoming aware of it'. This raises the question as to whether a whistle-blower or technology

142 *Klass v Germany* ECHR (6 September 1978) Series A 28 para 56.

143 Sec 26(1) Postal and Telecommunications Act [Chapter 12:05]. The minister, after consultation with the President, is of the view on reasonable grounds that any decision or action of the board is not in the national or public interest or the interests of consumers or licensees as a whole; the minister may direct the board in writing to reverse, suspend or rescind such decision or to reverse, suspend or rescind such action.

144 CA Parsons 'Do transparency reports matter for public policy? Evaluating the effectiveness of telecommunications transparency reports' 13 January 2015, https://ssrn.com/abstract=2546032 (accessed 14 July 2023).

tools constitute notification.[145] This represents a half-hearted effort to provide remedial action, fully aware that an appellant must first become aware of the warrant before challenging it – and even then, must demonstrate how they obtained that knowledge. In a very secretive regime such as Zimbabwe, all those likely to disclose are afraid of punitive measures. This malady can only be cured by a post-notification regime as part of safeguards and access to justice.

In *AmaBhungane* the Court emphasised the importance of post-surveillance notification as it minimises abuse and removes a perpetual state of secrecy.[146] This notification is foundational to invoking remedies as provided under section 18(1) of the IC Act. Without becoming aware and without confirmation of surveillance, access to courts and enforcement of rights becomes illusory.[147] In the absence of a post-notification regime, there are limited 'adequate and effective guarantees against abuse'.[148]

International human rights treaties, such as ICCPR (article 2(3)) reiterate the importance of an effective remedy even during the implementation of a secret surveillance scheme.[149] While non-judicial authorities can undertake surveillance supervision, this certainly is not adequate and requires judicial oversight. The levels of executive interference and complicity demand a more robust legislatively enabled judicial approach to surveillance supervision. As far back as 1998, the UN Human Rights Committee's Concluding Observations on Zimbabwe recommended that any interception of communications must be subjected to judicial oversight and be in accordance with ICCPR.[150]

Despite the passage of time, the Human Rights Committee's recommendation to Zimbabwe remains relevant, and has been repeatedly overlooked, despite numerous opportunities to implement

145 See sec 31 of the Cyber and Data Protection Act which provides for whistle-blowers, and various technologies make it possible to establish that one's communication is being intercepted as evidenced by the Circles Report (n 16).
146 *AmaBhungane* (n 5) paras 46-48.
147 Sec 85 of the Constitution of Zimbabwe on the enforcement of fundamental human rights and freedoms; compared with sec 38 of the Constitution of the Republic of South Africa and the enforcement of rights.
148 *Klass* (n 142) para 42.
149 *Klass* (n 142) para 69.
150 Concluding Observations on the First Report of Zimbabwe, ICCPR Committee (6 April 1998) UN Doc CCPR/C/79/Add.89. Similarly, the Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016) recommended that South Africa 'should refrain from engaging in mass surveillance of private communications without prior judicial authorisation'.

this recommendation. A similar recommendation was made to the South African government by the Human Rights Committee.[151]

In summary, the IC Act grants broad executive powers without oversight mechanisms, offers no avenues for remedy, and lacks comprehensive safeguards throughout the surveillance process.[152] As the Supreme Court held in *Law Society of Zimbabwe*:

> The net effect of the failure to provide statutory mechanisms to control or limit the exercise of the power conferred by the Act on the President leads to an unfettered discretion to intercept … communication … The Act provides no legal recourse or safeguard for the innocent. The Act does not provide any mechanisms for accountability. Similar legislation in other jurisdictions provides or is required to provide, for prior scrutiny, independent supervision of the exercise of such powers and effective remedies for possible abuse of the powers. The Act provides for no such safeguards.

These safeguards constitute an assessment of interception powers, oversight capabilities and remedies at each stage of interception, and for processes with higher threshold of violations such as bulk surveillance, independent authorisation at the outset is necessary as well as *ex post facto* review.[153]

7 Conclusion

As observed in *AmaBhungane*, the 'indiscriminate tentacles of interceptions reach communications of whatever nature, including the most private and intimate'.[154] If unbridled powers of surveillance, weak oversight mechanisms and illusory remedies for surveillance exist, the government will visit [your] bedrooms as proclaimed by the government minister. The reasonable suspicion threshold for surveillance in Zimbabwe is low. The interception targets are identifiable and belong to the same group – political opponents of the regime. The oversight mechanisms and reviews are a sham, making the remedies illusory if not non-existent. In a secretive state, there is no likelihood of being aware that one is under surveillance as suspicion alone will not suffice.

That notwithstanding, the IC Act is ripe for constitutional challenge, as there are grounds that fundamental rights are being or are likely to be infringed by virtue of the IC Act's provisions when contrasted

151 Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016) paras 42, 43.
152 Law Society of Zimbabwe (n 12).
153 *Centrum för rättvisa* (n 128) para 264.
154 *AmaBhungane* (n 5) 31.

against international standards.[155] Its ripeness is accentuated by the uncanny similarities to RICA and the decision in *AmaBhungane*. Furthermore, the earlier Supreme Court decision in *Law Society of Zimbabwe* affirms the conclusion that the IC Act is unconstitutional for both omissions and commissions in its provisions.

A range of amendments to IC Act are required, namely, authorisation of interception warrants by an independent court; the authorisation of bulk interception by a court; a post-surveillance notification regime; data protection measures for storage and destruction consistent with the Cyber and Data Protection Act of 2021; service provider transparency reports disclosing the number of interception warrants received; and the provision of a user grievance mechanism. Access to information through post-surveillance notification facilitates the constitutional accountability of public officials.[156] The amendments can also include a parliamentary intelligence and oversight committee. As the IC Act stands, the government or state can visit your bedroom with impunity, fulfilling the description of Zimbabwe as a pariah and surveillance state.

155 Sec 85 Constitution of Zimbabwe.
156 *Hitschmann v Mutare City & Others* (2016) ZWHHC 211.