LEGAL RESOURCES CENTRE

SPYWARE AND SURVEILLANCE TECHNOLOGY IN SOUTH AFRICA

AUGUST 2024

Authors: Devon Turner, Julia Khan and Sherylle Dass

TABLE OF CONTENTS

1.0 QUESTION PRESENTED AND SHORT ANSWERS

Is spyware being used in South Africa?

Spyware is being used by the government, including in the past through the surveillance bill RICA, which was deemed unconstitutional in 2021. However, a new bill to replace RICA was up for public comment and similarly allows for spyware and state sponsored surveillance.

How prevalent is the use of this technology?

This technology seems to be prevalent. From misuse of the technology against journalists, explicitly proven under the past presidency, to ransomware attacks against companies, there is prevalent use of this technology in RSA.

Where, and in what realms, is this technology being used?

Spyware is being, or has been, used within the government and National Intelligence Agency, by individuals, by private companies, and even by international governments in cross-border surveillance. For example, spyware was used by the Rwandan government to bug President Ramaphosa's phone using the notorious Israeli spyware company Pegasus.

2.0

FINDINGS

Government Use

The South African government has used and contributed to spyware. According to information released by WikiLeaks in 2014, the South African government may have provided FinFisher, a surveillance software company marketed by Lench IT Solutions, up to €2-million between 2009 and 2012.[1]

In addition, the South African government has funded VASTech, the spyware company best known for selling its equipment to Muammar Gaddafi, despite calls to stop funding the company.[2] The South African government has also been involved in multiple controversies of illegal use of spyware, resulting in prosecutions of the individuals involved, and its surveillance bill, RICA, was declared unconstitutional by the Constitutional Court in 2021.[3]

Finally, a survey of southern African countries and their surveillance laws revealed governments across the region have been spying on people's communications with insufficient limitations or safeguards and often for anti-democratic purposes.[4]

1 Al Jazeera's The Spy Cables

While limited information exists on the full scope of spyware use by the South African government, it is clear there is surveillance, including mass surveillance, by the state. In 2015, Al Jazeera leaked secret intelligence documents that exposed regulatory loopholes exploited by South African spies to enable domestic surveillance.[5] The cache of secret intelligence papers includes a confidential surveillance policy-and-procedure manual, as well as copies of the application forms used by intelligence and security personnel seeking permission to conduct both physical and electronic surveillance of an individual.

Jane Duncan, author of *The Rise of the Securocrats*, told Al Jazeera that South Africa has seen "an erosion of accountability" that is "extremely worrying" and blames the "wrong decisions" that were taken "at the start of the transition to democracy." As a result, Duncan believes there is an "overextention of the power of the State Security Agency so that intelligence has started to cover itself like a skin and it's become effectively a state watchdog of civil society." Further, Duncan stated that "we don't know effectively what [South Africa's government is] doing with the mass surveillance capacities of the state, but there are certain things that we do know. We know that South Africa has mass surveillance capacity. We know that it's manufacturing mass surveillance capacity. We know that the Department of Trade and Industry has provided funding for at least one company in South Africa to manufacture this mass surveillance capacity. We also know that it's being exported."[6]

---

[1] https://mybroadband.co.za/news/security/110288-did-sa-government-blow-e2-million-on-spyware.html

[2] https://mg.co.za/article/2011-09-02-sa-firm-helped-gaddafi-spy/

[3] 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 Journalism NPC and Others [2021] ZACC 3.

[4] *A Patchwork for Privacy*, May 2020, https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/patchwork_for_privacy_-_communication_surveillance_in_southern_africa.pdf; Allen Munoriyarwa, Admire Mare, *Digital Surveillance in Southern Africa*, 2022, https://doi.org/10.1007/978-3-031-16636-5

[5] Will Jordan, *Spy Cables raise South Africa privacy concerns*, AL JAZEERA, 25 Feb. 2015, https://www.aljazeera.com/news/2015/2/25/spy-cables-raise-south-africa-privacy-concerns

[6] *Supra* note 2.

2

Misuse of Spyware

South Africa has seen a number of concerning reports regarding state spies targeting journalists and misuse of spyware technology. In 2018, the Right2Know Campaign ("R2K"), a nonprofit aimed at reducing state secrecy and increasing access to information, released a report entitled Spooked: Surveillance of Journalists in SA.[7]

R2K formed in opposition to South Africa's infamous "Secrecy Bill": the national security legislation proposed by the former administration of President Jacob Zuma in 2010. Their 2018 report, which investigated 10 case studies of surveillance targeting journalists, noted that while, at the time, there was no explicit evidence that South Africa was a client of Pegasus (discussed in full below), there have been clear attempts to spy on journalists.

In 2012, former criminal intelligence officers were accused of illegally bugging the phones of the former police chief as well as journalists from the Sunday Times.[8]

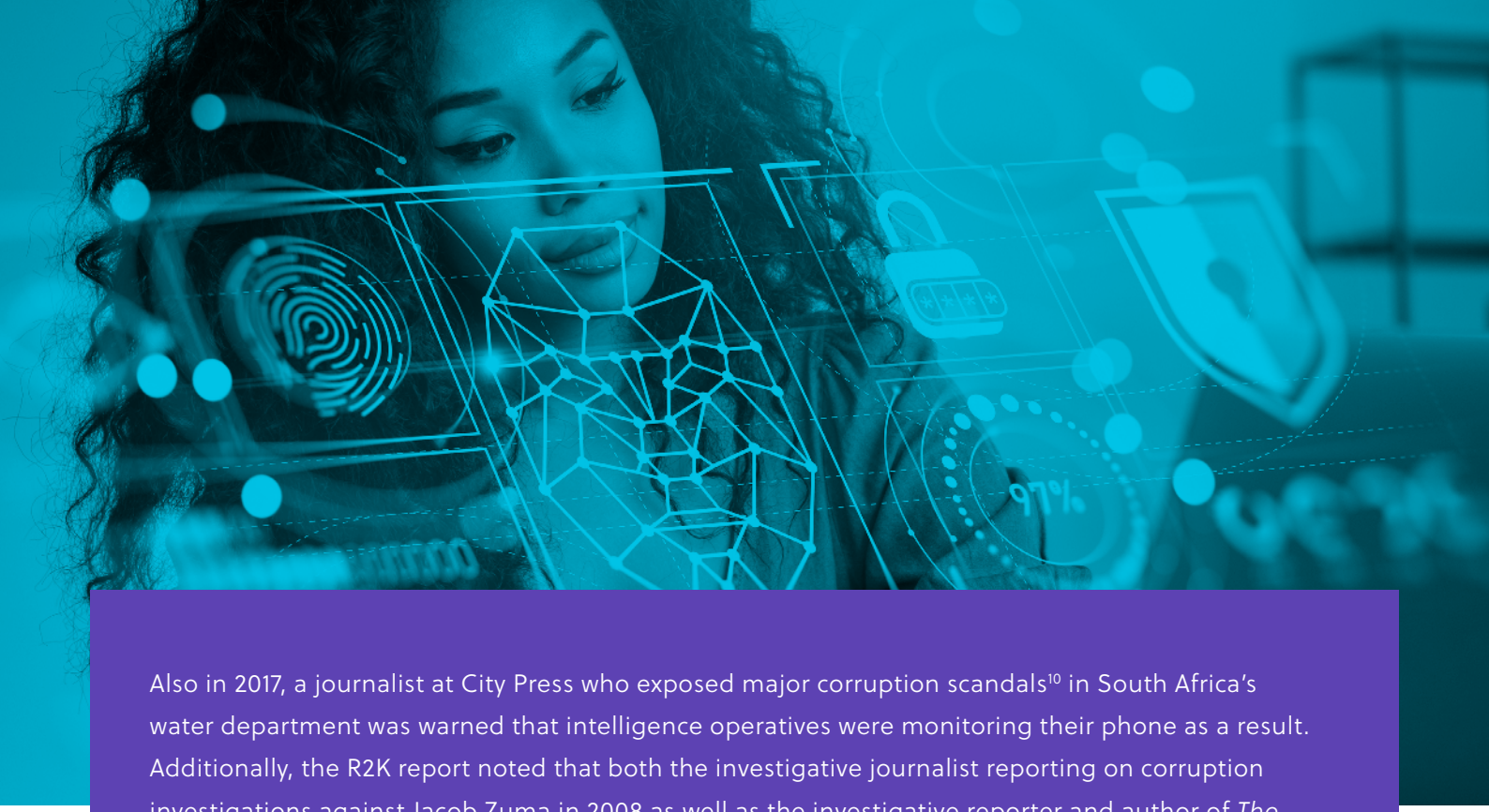
The former KwaZulu-Natal police spy boss and covert intelligence collection officials were suspected of inserting three mobile numbers under false names into a legitimate interception order. In 2017, the former police officer Bongani Cele was convicted in the Pretoria Specialised Commercial Crimes Court of illegally bugging the phones of Sunday Times reporters Mzilikazi wa Afrika and Stephan Hofstatter and sentenced to three years in jail.[9]

---

[7] R2K's website is currently inoperative, https://z-lib.io/book/13693793; see also, Murray Hunter, *South Africa's State of Surveillance: How Journalists Are Targets for Spying*, Global Investigative Journalism Network, GLOBAL INVESTIGATIVE JOURNALISM NETWORK, 24 July 2018, https://gijn.org/stories/south-africas-state-of-surveillance-how-journalists-are-targets-for-spying/

[8] Sapa, *Police illegally tapped journalists phones: report*, TIMES LIVE, 18 Aug. 2013, https://www.timeslive.co.za/news/south-africa/2013-08-18-police-illegally-tapped-journalists-phones-report/

[9] Athandiwe Saba, *Cops illegally bugged Sunday Times calls*, SUNDAY TIMES, 30 July 2017, https://www.timeslive.co.za/sunday-times/news/2017-07-29-cop-illegally-bugged-sunday-times-calls/



Also in 2017, a journalist at City Press who exposed major corruption scandals[10] in South Africa's water department was warned that intelligence operatives were monitoring their phone as a result. Additionally, the R2K report noted that both the investigative journalist reporting on corruption investigations against Jacob Zuma in 2008 as well as the investigative reporter and author of *The President's Keeper* were both spied on by Pegasus's technology.[11]

Further, in 2015 R2K published an investigation[12] of state spying on community organisations and unions. Despite laws requiring service providers to store logs of everyone's communication activity, in 2017 R2K discovered those logs got handed over to state agencies more often than was previously thought. R2K warned that journalists in South Africa have long been a target for state spying, and more recently have also become the target of private spying. Part of the problem is that most reporters are left to deal with the risks on their privacy and safety on an individual basis; however, the *AmaBhungane* case (discussed in full below), provides hope, and further legal protections, that bulk interceptions and spyware can be more seriously targeted.

With regard to unethical practices used by the South African government to obtain information of journalists, one of the contributors to R2K's report – data privacy expert Murray Hunter – stated, "The South African government has shown that it will resort to dirty tricks to try to get into journalists' communication, not for any legitimate public safety or national security reasons, but because they want to figure out who the sources are, and they want to clamp down on damaging or embarrassing reporting."[13] Evidence indicates that South Africa's state security structures increase their political intelligence gathering before elections. Additionally, while there was supposed to have been a crackdown on the surveillance issues and abuses exposed by the Zondo Commission and the President's expert panel on state security, it still has not materialized.

---

[10] Sipho Masondo, *Watergate: Noose tightens around Nomvula Mokonyane*, NEWS24, 3 Aug. 2016, https://city-press.news24.com/News/noose-tightens-around-nomvula-20160730

[11] *Supra* note 3.

[12] https://www.r2k.org.za/wp-content/uploads/R2K-Surveillance-of-Journalists-Report-2018-web.pdf

[13] Aarti Bhana, *Pegasus: The real enemy of free speech and journalism*, FRAY INTERMEDIA, 2024, https://www.frayintermedia.com/post/pegasus-the-real-enemy-of-free-speech-and-journalism/

Private Company Use

1 Pegasus

Electronic devices infected with Pegasus, a notorious spyware program sold only to governments, have been discovered in South Africa.[14] The spyware, developed by Israeli cyber warfare firm NSO Group, has been used to target journalists and human rights activists across the world.[15]

Similar to other spyware programs, Pegasus works by insinuating itself into smartphones; however, it gives the infiltrator particularly free reign of the device, including access to its microphone and camera, all files or photos stored on the phone, network connections, contact information, message and browsing histories, passwords, email accounts, recordings and so forth. The purchaser can listen to conversations – even ones that take place over encrypted messaging apps like Signal – all without the owners' knowledge.

In July 2021, the Pegasus Project found phone numbers of more than 180 journalists on a list of what appear to be potential targets of Pegasus spyware that could turn their mobile phones into listening devices.[16] While the NSO Group denied connection with the list and said it only sells its product to vetted governments with the goal of preventing crime or terrorism, this was not the first time reports of misuse of spyware had come out against Pegasus.

In late 2018, Citizen Lab published a report that also found evidence of Pegasus throughout Africa, including Côte d'Ivoire, Togo, Uganda, Kenya, Rwanda, Zambia, South Africa, and most North African countries.[17] The report identified that 45 countries had infected devices which were being traced as well as multiple instances of cross-border surveillances.[18] According to The Guardian, which was part of the Pegasus investigation project, President Cyril Ramaphosa's personal mobile phone seemed to have been selected by Rwanda for targeting in 2019.[19]

---

[14] Simon Allison, *South African phones targeted by notorious 'governments only' spyware*, MAIL & GUARDIAN, 2 Oct. 2018, https://mg.co.za/article/2018-10-02-south-african-phones-targeted-by-notorious-governments-only-spyware/

[15] Bill Marczak et al., NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains, THE CITIZEN LAB, 18 Apr. 2023, https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/#:~:text=NSO%20Group's%20Pegasus%20spyware%20remains,attack%20surfaces%20on%20the%20iPhone.

[16] *Spyware reform critical as at least 180 journalists revealed as potential Pegasus targets*, COMMITTEE TO PROTECT JOURNALISTS, 19 July 2021, https://cpj.org/2021/07/spyware-reform-critical-180-journalists-potential-pegasus-targets/; Journalists Selected for Targeting, ORGANIZED CRIME AND CORRUPTION REPORTING PROJECT, 2021, https://cdn.occrp.org/projects/project-p/#/professions/journalist

[17] *Special report: When spyware turns phones in weapons*, COMMITTEE TO PROTECT JOURNALISTS, 13 Oct. 2022, https://cpj.org/reports/2022/10/when-spyware-turns-phones-into-weapons/

[18] Bill Marczak, et al., *Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, THE CITIZEN LAB, 18 Sept. 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[19] Shannon Ebrahim, Nefarious use of Pegasus spyware exposes governments, INDEPENDENT ONLINE, 6 Aug. 2021, https://www.iol.co.za/news/politics/opinion/nefarious-use-of-pegasus-spyware-exposes-governments-7c68bac2-0971-4903-bde1-37513e20d7ac; see also, Nicole McCain, *Ramaphosa one of 14 world leaders targeted in Pegasus spyware case – report*, NEW24, 21 July 2021, https://www.news24.com/news24/southafrica/news/ramaphosa-one-of-14-world-leaders-targeted-in-pegasus-spyware-case-report-20210721, ("... Ramaphosa's cellphone number was listed as a potential target for surveillance in the Pegasus spyware case. He was reportedly among 14 heads of state to be targeted, including Pakistani Prime Minister Imran Khan and French President Emmanuel Macron.")

2

Circles

Circles is a spyware company that is also affiliated with the NSO Group responsible for Pegasus spyware. Like Pegasus, Circles is only sold to nation-states.

However, unlike Pegasus, Circles' tools do not require targets to click on a malicious link. It works by exploiting flaws in Signalling System No.7 (SS7), the set of protocols that allows networks to exchange calls and text messages between each other. SS7 is predominantly used in 2G and 3G systems, which in 2019 became the leading mobile technology in sub-Saharan Africa, accounting for over 45% of all connections.

While South Africa was not on the list in 2021 when the report was published, at least twenty-five countries, and at least seven other African governments, have been confirmed as using Circles in a comprehensive report published in Dec. 2020.[20]

3

VASTech

VASTech, a South African company founded in 1999, which operates similarly to the US's PRISM surveillance program offers multiple tools under what it calls "communication intelligence extraction solutions."[21]

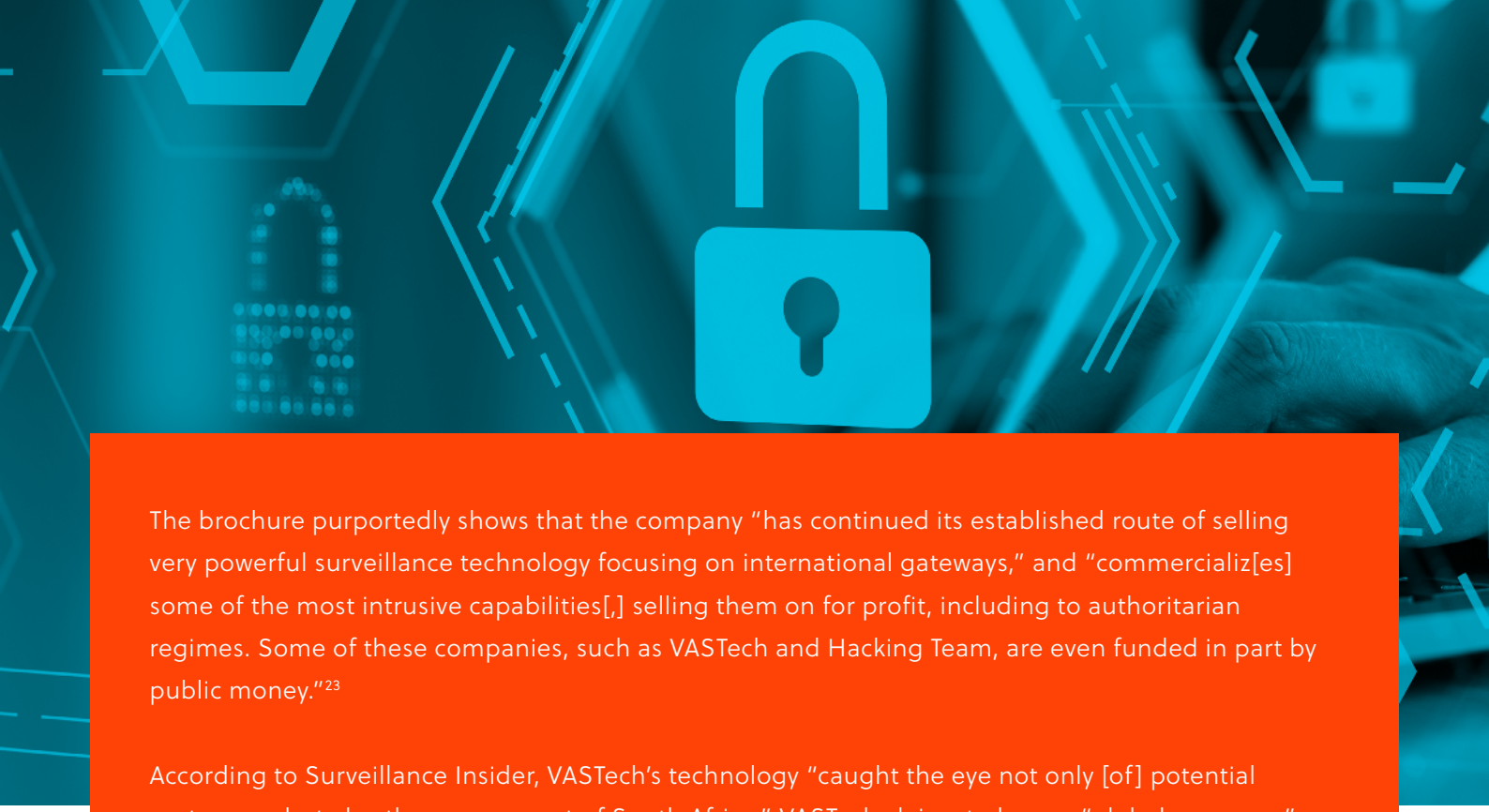
In 2016, the company produced a pamphlet in which they outlined their capabilities for governments, militaries, and law enforcement agencies to conduct "passive detection" of communications transmitted through satellites, phones, and fiber optic cable.[22]

---

[20] Bill Marczak, et al., *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*, THE CITIZEN LAB, 1 Dec. 2020, https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

[21] https://www.vastech.co.za/

[22] Jenna McLaughlin, *South African spy company used by Gadaffi touts its NSA-like capabilities*, THE INTERCEPT, 31 Oct. 2016, https://theintercept.com/2016/10/31/south-african-spy-company-used-by-gadaffi-touts-its-nsa-like-capabilities/



The brochure purportedly shows that the company "has continued its established route of selling very powerful surveillance technology focusing on international gateways," and "commercializ[es] some of the most intrusive capabilities[,] selling them on for profit, including to authoritarian regimes. Some of these companies, such as VASTech and Hacking Team, are even funded in part by public money."[23]

According to Surveillance Insider, VASTech's technology "caught the eye not only [of] potential customers, but also the government of South Africa." VASTech claims to have a "global presence," with offices in Dubai and Switzerland and offers "current solutions" in "the Middle East, Europe, Africa, Asia, and the Americas" for "protecting sovereign interests," according to the 2016 pamphlet.

The company's capabilities, which include intercepting and recording international phone calls, texts, and social media messages, have been exposed by The Wall Street Journal, Wikileaks, and research by nonprofit organizations.[24]

VASTech markets three systems to intercept communications: "PORTEVIA," which gathers information straight from the fiber cables of the Internet, "STRATA," which monitors mobile devices, and "GALAXIA," which collects communications from satellites. The South African government has funded VASTech, despite calls from Privacy International to stop the funding.[25] This funding would be provided by the now-called Department of Trade, Industry and Competition, however, information on shareholding and the amount of funding is uncertain.

4

Small Companies

In additions to larger, international companies producing spyware software and equipment, smaller companies within South Africa also seem to be using spyware in one-to-one surveillance.[26]

---

[23] *Supra* note 19.

[24] *VASTech Passive surveillance in support of LI*, WIKILEAKS, https://wikileaks.org/spyfiles/docs/vastech/ 41_passive-surveillance-in-support-of-li.html

[25] *South African Government still funding VASTech, knows previous financing was for mass surveillance*, PRIVACY INTERNATIONAL, 20 Jan. 2014, https://privacyinternational.org/blog/1308/south-african-government-still-funding-vastech-knows-previous-financing-was-mass

[26] *See e.g.* Private Investigator Cape Town, https://privateinvestigatorcapetown.com/cell-phone-spy-software/; The 10 Best Private Investigation Services in Johannesburg, https://johannesburg.infoisinfo.co.za/search/private-investigation

Organisations Calling for Embargo Against Israeli Spyware Companies

Given the prominence of Israeli spyware internationally, organisations have called for two-way embargos against Israel in the wake of Israel's recent violence against Palestine. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies encourages governments to take the human rights and fundamental freedoms of the recipient countries into account before exporting to them, and not just focus on not exporting to countries subjected to sanctions. South Africa has been shown to be open to business for Israeli spyware as evidenced by the survey of communication surveillance laws in 12 southern African countries in 2020 and updated in 2022.[27]

Israeli surveillance tools, including spyware, have been critical to the occupation and it is at least plausible that they have become critical to the most recent military operations in Gaza too. Activists have stated that, as such, the companies that provide these tools could be complicit in the commission of genocide. As a result, over 170 organisations have demanded governments which use military assistance, including spyware, from Israel enter into an embargo against Israel and cease the use of these technologies.[28]

2023 Proposed RSA Spying Law

In early 2021, the South African Constitutional Court found that the country's State Security Agency, through its intelligence agency, the National Communication Centre, was conducting bulk interception of electronic signals unlawfully. As a result, in November 2023, the General Intelligence Laws Amendment Bill was introduced in the National Assembly to respond to the gap created by *AmaBhungane*.[29] This bill primarily deals with how the surveillance centre should be regulated. The amendment bill provides for the proper establishment of the National Communication Centre and its functions. This includes the collection and analysis of intelligence from electronic signals, and information security or cryptography. A parliamentary ad hoc committee set a deadline of 15 February 2024 for public comment. The bill says, in vague terms, that the centre shall gather, correlate, evaluate, and analyse relevant intelligence to identify any threat or potential threat to national security. However, it doesn't provide any of the details the court said it would be looking for. The bill states that the surveillance centre needs to seek the permission of a retired judge, assisted by two interception experts, before conducting bulk interception, which experts believe to be a strength of the bill. The judge will be appointed by the president, and the experts by the minister in charge of intelligence.

---

[27] *Supra* note 1.

[28] *Ending complicity in international crimes: A two-way arms embargo on Israel*, INTERNATIONAL SERVICE FOR HUMAN RIGHTS, 8 Nov. 2023, https://ishr.ch/latest-updates/ending-complicity-to-international-crimes-a-two-way-arms-embargo-on-israel/; Jane Duncan, *Embargo against invasive Israeli spyware essential after International Court of Justice ruling*, DAILY MAVERICK, 15 Feb. 2024, https://www.dailymaverick.co.za/article/2024-02-15-embargo-against-invasive-israeli-spyware-essential-after-icj-ruling/

[29] B 40—2023, General Intelligence Laws Amendment Bill, https://static.pmg.org.za/B40-2023_General_Intelligence_Laws.pdf

Experts have also identified dangers of the bill,[30] including the mere fact that it allows for bulk identification, which puts large numbers of people under surveillance regardless of whether they are suspected of threats to national security. In RSA specifically, around 2005, rogue agents in the former National Intelligence Agency misused bulk interception to spy on senior members of the ruling African National Congress, businesspeople, and civil servants. This was despite the agency's mandate to focus on foreign threats. These rogue agents were able to abuse bulk interception because there was no law controlling and limiting how these capabilities were to be used. A 2008 commission of inquiry called for this law to be enacted.

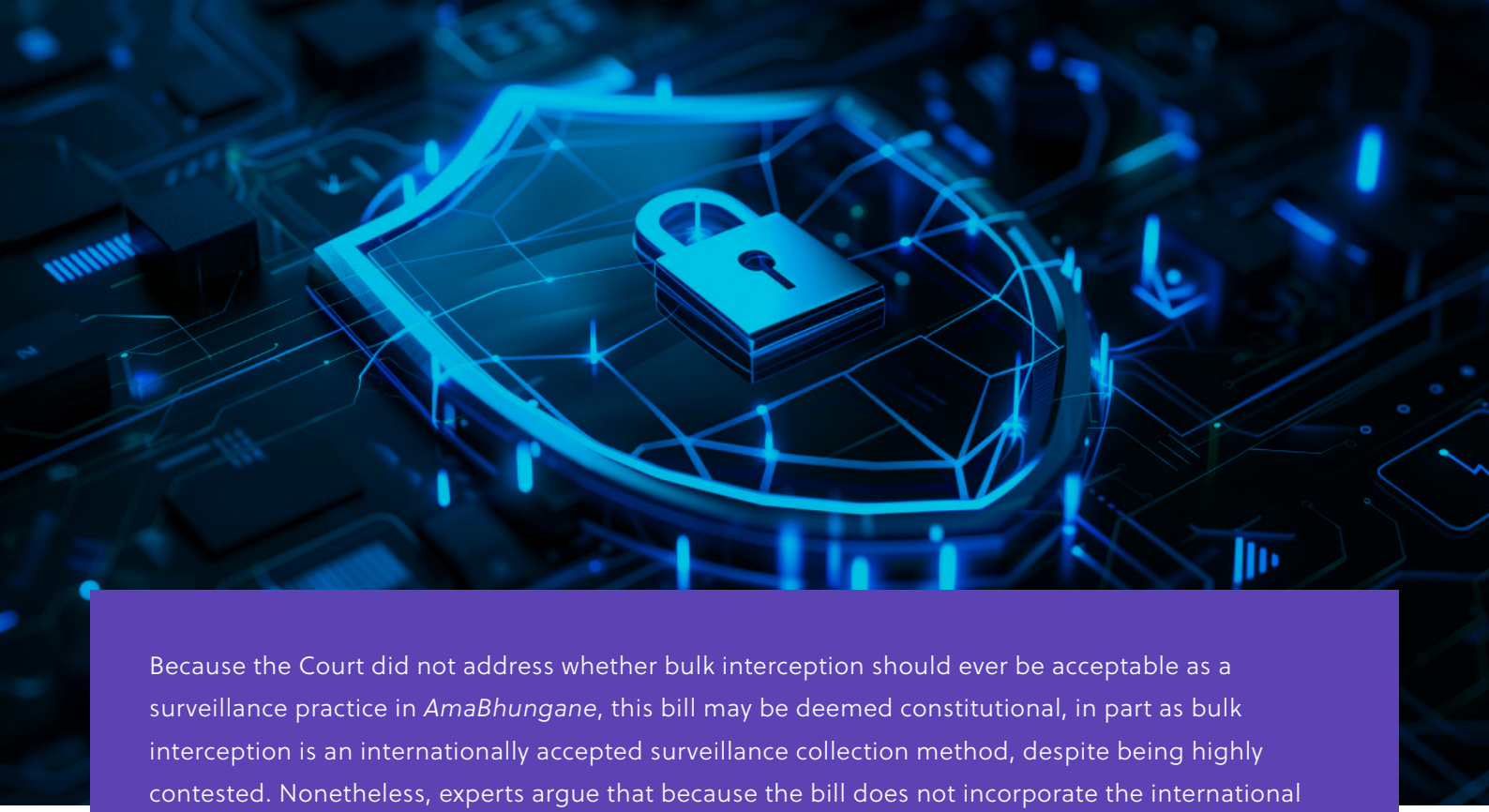
The government refused to do so until it was forced to act by the Constitutional Court ruling in *AmaBhungane*. The government justified its refusal to act by claiming that the National Communication Centre was regulated adequately through the National Strategic Intelligence Act. The court rejected this argument because the act failed to address the regulation of bulk interception directly.

The bill also fails to incorporate international benchmarks on the regulation of strategic intelligence and bulk interception in a democracy. These require that a domestic legal framework provide what the European Court of Human Rights has referred to as "end-to-end" safeguards covering all stages of bulk interception.[31]

---

[30] Jane Duncan, Surveillance and the state: South Africa's proposed new spying law is open for comment – an expert points out its flaws, THE CONVERSATION, 5 Feb. 2024, https://theconversation.com/surveillance-and-the-state-south-africas-proposed-new-spying-law-is-open-for-comment-an-expert-points-out-its-flaws-222165

[31] *Supra* note 27, ("The European Court has stated that a domestic legal framework should define, (1) the grounds on which bulk interception may be authorized, (2) the circumstances, (3) the procedures to be followed for granting authorization, [and] (4) [the] procedures for selecting, examining and using material obtained from intercepts. The framework should also set out (1) the precautions to be taken when communicating the material to other parties, (2) limits on the duration of interception, (3) procedures for the storage of intercepted material, (4) the circumstances in which such material must be erased and destroyed, (5) supervision procedures by an independent authority, [and] (6) compliance procedures for review of surveillance once it has been completed.").



Because the Court did not address whether bulk interception should ever be acceptable as a surveillance practice in *AmaBhungane*, this bill may be deemed constitutional, in part as bulk interception is an internationally accepted surveillance collection method, despite being highly contested. Nonetheless, experts argue that because the bill does not incorporate the international benchmarks and because the bill gives the intelligence minister too much power to set the ground rules for bulk interception, the bill is dangerous and should not be approved. Currently, the Bill has passed through the National Assembly but has faced many objections and is yet to be adopted into law.[32]

Spyware and Ransomware Attacks

A 2023 report by a cyber security company stated that spyware attacks in South Africa increased by 18.8% between the last quarter of 2022 and first quarter of 2023.[33] Moreover, a 2022 report showed that 51% of South African organisations surveyed were hit with ransomware in 2021; forty-nine percent of the organisations that had data encrypted paid the ransom to get their data back, even if they had other means of data recovery, such as backups.[34] According to Interpol's African Cyber Threat Assessment Report,[35] almost 220 million email threats were detected in South Africa in 2021. The South African state bank has reportedly received over 100,000 fraudulent emails resulting in more that R400 million in loses necessary to recover its IT systems.[36]

---

[32] https://intelwatch.org.za/2024/04/08/despite-important-gains-the-new-general-intelligence-laws-amendment-bill-fails-to-safeguard-against-a-second-*state*-capture/

[33] Mandisa Ndlovu, *Spyware attacks in South Africa increase by 18.8%*, MAIL & GUARDIAN, 19 May 2023, https://mg.co.za/article/2023-05-19-spyware-attacks-in-south-africa-increase-by-18-8/?amp=

[34] *Ransomware hits more than half of SA companies*, IT-ONLINE, 9 May 2022, https://it-online.co.za/2022/05/ 09/ransomware-hits-more-than-half-of-sa-companies/

[35] *INTERPOL report identifies top cyberthreats in Africa*, INTERPOL, 21 Oct. 2021, https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa (Postbank, for example, lost more than R18 million over three months in such attacks).

[36] *Supra* note 29.

3.0 ANALYSIS OF CASE LAW

AmaBhungane

South Africa's courts have recognized that protecting the identity of journalists' sources is an "essential" part of media freedom. In this recent journalist-protective case, the Court ruled in favor of *AmaBhungane* where they challenged the constitutionality of South Africa's surveillance law, the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 ("RICA"). In *AmaBhungane* v Minister of Justice, the South African Constitutional Court declared various elements of the legislation authorizing interception of communications unconstitutional and invalid.[37]

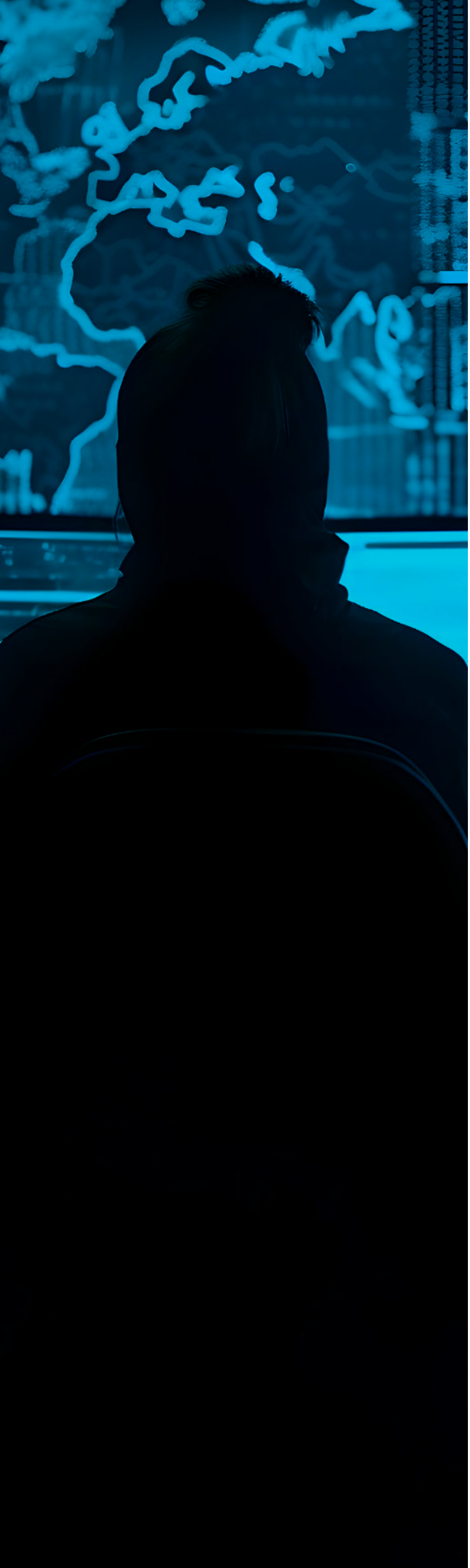
AmaBhungane Centre for Investigative Journalism launched a court case after an affidavit revealed South African journalist Sam Sole's communications had been intercepted in 2008. Sole, who was instrumental to the reporting of the corruption investigation against Jacob Zuma had been spied on by the National Intelligence Agency for a period of months wherein government agents listened in on his confidential discussions with sources as well as his personal calls.[38]

In *AmaBhungane*, the applicants argued that RICA, which declares that citizens must link their SIM card, landline, and internet account to their identity so any communications from their SIM card or account can be traced back to them is constitutionally flawed and must be amended. Specifically, *amaBhungane* argued that the RICA is unconstitutional because (1) the person targeted for surveillance is never informed of the warrant to intercept their communications, even when the interception has ended and any investigation has concluded; (2) RICA required private companies to store information on their users and whom they communicate with without providing any oversight mechanisms; (3) RICA is silent on the necessary procedures for officials examining, copying, sharing, and storing the intercepted data and the procedures for destroying intercepted data irrelevant to investigations; (4) RICA fails to provide extra protections for persons with special legal duties to protect the confidentiality of those they speak with, such as lawyers and journalists; (5) the oversight system is insufficient because the RICA judicial system fails to include a "public advocate" to represent the interests of people who have been targeted by the surveillance systems; and (6) RICA fails to regulate South Africa's "bulk interception" programmes wherein mass surveillance practices are employed to collect and analyse massive flows of data on large groups of people.

---

[37] *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 Journalism NPC and Others* [2021] ZACC 3, https://collections.concourt.org.za/bitstream/handle/20.500.12144/36631/%5bJudgment%5d% 20CCT%20278%20of%2019%20and%20279%20of%2019%20AmaBhungane%20Centre%20for%20Investigative%20Journalism%20v%20Minister%20of%20Justice%20and%20Others.pdf?sequence=42&isAllowed=y; *see also South Africa's spy law declared unlawful*, IFEX, 16 Feb. 2021, https://ifex.org/south-africas-spy-law-declared-unlawful/; Juniour Khumalo, *Surveillance abuses: How spies target SA journalists who uncover corruption*, NEWS24, 4 July 2018, https://www.news24.com/citypress/news/surveillance-abuses-how-spies-target-sa-journalists-who-uncover-corruption-20180704; Jane Duncan, Top court ruling on South Africa's spy law is a victory for privacy, but loopholes remain, THE CONVERSATION, 14 Feb. 2021, https://theconversation.com/top-court-ruling-on-south-africas-spy-law-is-a-victory-for-privacy-but-loopholes-remain-154865

[38] *Supra* note 33.



In 2019, the High Court ruled in favor of amaBhungane holding that RICA was unconstitutional. The High Court upheld the following challenges: (1) RICA makes no provision for a subject of surveillance ever to be notified that she or he has been subjected to surveillance (notification issue); (2) RICA permits a member of the Executive unfettered discretion to appoint and renew the term of the designated Judge (the functionary responsible for issuing directions for the interception of private communications), and thus fails to ensure the independence of the designated Judge (independence issue); (3) RICA lacks any form of adversarial process or other mechanism to ensure that the intended subject of surveillance is protected in the ex parte application process (ex parte issue); (4) RICA lacks adequate safeguards for examining, copying, sharing, sorting through, using, destroying and/or storing the surveillance data (management of information issue); and (5) RICA fails to provide any special circumstances where the subject of surveillance is a journalist or practising lawyer (practising lawyers and journalists issue). RICA was accordingly declared unconstitutional to the extent of these failures. The declaration of invalidity was suspended for two years to allow Parliament to cure the defects. Interim relief, in the form of reading-in, was granted in respect of the notification issue, the independence issue and the practising lawyers' and journalists' issue.

In 2021, following an appeal by authorities, the Constitutional Court upheld the High Court's decision. The Constitutional Court wrote RICA "fails to provide adequate safeguards to protect the right to privacy" as buttressed by the rights of access to courts, freedom of expression and the media, and legal privilege.

The Constitutional Court held that interception and surveillance of an individual's communications under RICA is a highly invasive violation of privacy, and thus infringes section 14 of the Constitution. The Court next considered whether this limitation was reasonable and justifiable under section 36(1) of the Constitution.

The Court acknowledged the constitutional importance of the right to privacy, as tied to dignity, versus the importance of state surveillance, in order to investigate and combat serious crime, guarantee national security, maintain public order and thereby ensure the safety of the Republic and its people; the Court ultimately held that the collection of Sole's communications was "egregiously intrusive" in nature thus necessitating the question 'is RICA doing enough to reduce the risk of unnecessary intrusions?' and, as such, providing safeguards to mimise the infringement on the right to privacy in order to meet the reasonableness and justifiability standard.

Accordingly, the Court ordered that post-surveillance notification to the owner of the device(s) should be the default position and RICA was unconstitutional to the extent that it failed to provide for notifying the subject of surveillance of the surveillance as soon as would be possible without jeopardising the purpose of the surveillance. The Court further held that RICA was unconstitutional to the extent that it fails to ensure adequate safeguards for an independent judicial authorisation of interception as RICA failed to allow the designated RICA judge an "adequate level of structural and operational autonomy secured through institutional and legal mechanisms designed to ensure that it 'discharges its responsibilities effectively.'"[39]

Regarding the management of information, the Court held that RICA's provisions did not prescribe the relevant procedures and allowed the Director of the Office for Interception Centre unacceptably broad discretion to regulate the management of information. Thus, RICA allowed for unnecessarily egregious intrusions into the privacy of the subjects of interceptions.

The Court therefore declared RICA unconstitutional to the extent that it fails adequately to prescribe procedures to ensure that data obtained pursuant to the interception of communications is managed lawfully and not used or interfered with unlawfully. Finally, the Court also found RICA unconstitutional in its dealings with lawyers' and journalists' heightened privacy needs as protected by the rights to fair trial and fair hearing and the rights to freedom of expression and the media, respectively.

[39] *Supra* note 33 at 49.

These rights were found to weigh in favour of special consideration being given to the importance of the confidentiality of lawyer-client communications and journalists' sources, in order to minimise the risk of infringement of this confidentiality, and, as such, RICA's failure to do so rendered it unconstitutional.

With regard to bulk interception, the Constitutional Court held that bulk interception was unlawful and invalid. While the Minister of State Security argued bulk communication surveillance should be viewed as constitutional, the Court held that section 2 of the National Strategic Intelligence Act 39 of 1994 is ambiguous and should thus be interpreted in a manner that best promotes the right to privacy and does not contradict RICA's prohibition of communication interceptions without interception directions. Accordingly, the Court stated that the broad terms of section 2 do not authorise the practice of bulk surveillance, and the practice is therefore unlawful and invalid.

Having declared RICA unconstitutional, the Court limited the retrospectivity of its declaration of invalidity. It further suspended its declaration of invalidity for three years, as requested by the Minister of Justice, to allow Parliament adequate time to proceed with its investigations and develop suitable remedial legislation. Since the infringement of the privacy right is egregiously intrusive, and the period of suspension is relatively long, the Court deemed it necessary to grant interim relief in respect of the notification issue, and the lawyers' and journalists' issue.

4.0 CONCLUSION

In sum, the use of spyware seems to be widespread, even with the full scope of its use remaining unknown. Journalists, non-profit organisations, and WikiLeaks have revealed pertinent information about its use, namely its misuse leading to unlawful surveillance.

While *AmaBhungane* indicates the Court's willingness to protect people's privacy rights, even where national security concerns are raised, the state has demonstrated its disregard for people's privacy rights through persisting with the proposed surveillance bill in its current form.

WE LOOK FORWARD TO CONNECTING WITH YOU.

www.lrc.org.za

info@lrc.org.za

LRCSouthAfrica

lrcsouthafrica

LRCSouthAfrica

Legal Resources Centre

LRCSouthAfrica

JOHANNESBURG/NATIONAL OFFICE
Tel: +27 11 038 9709

CAPE TOWN OFFICE
Tel: +27 21 879 2398

DURBAN OFFICE
Tel: +27 31 301 7572

MAKHANDA OFFICE
Tel: +27 46 622 9230

LRC LEGAL RESOURCES CENTRE