4

South African Digital Sovereignty at the Crossroad of Securitization and Development

Enrico Calandro

4.1 INTRODUCTION

Like many other African countries, South African authorities are designing strategies, policies, and rules and assigning responsibilities to the existing and new agencies to govern emerging digital technologies. Nevertheless, national policy and regulatory directions for the governance of the digital economy and society, on the one hand, are struggling to cope with increasing responsibilities of state actors to protect citizens' rights to data protection and safety and security online. On the other hand, data protection and cybersecurity measures do not always protect citizens' rights to privacy, confidentiality, and freedom of expression. Instead, the increasing body of norms, rules, and regulation on the digital space might increase state control over private communications and online censorship. State and nonstate actors are also conscious of the manipulative power of digital communications and have used various digital platforms to launch sophisticated disinformation and misinformation campaigns to manipulate public opinion (Pretorius, 2021). It exposes the many conflicts that arise when different forms of digital sovereignty analyzed in this book – especially state-led, corporate, postcolonial, and individual digital sovereignty – enter in contact.

To anchor the concept of digital sovereignty in South Africa, the study seeks to answer to the following questions: what are South Africa's national priorities regarding the governance of the digital space? What digital (and offline) processes are impacted? Moreover, to what extent are citizens' rights to privacy and freedom of expression at risk?

To explore the emerging policy position on digital sovereignty in South Africa within the global geopolitical theater on the governance of cyberspace, the chapter first reviews international processes relevant to understanding digital sovereignty positions of South Africa. It reviews the participation

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

of the country in multilateral organizations, including the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) on ICT state security; Third Committee Resolution on Countering the Use of Information and Communications Technologies for Criminal Purposes; the United Nations Office for Disarmament Affairs (UNODA); Intergovernmental Group of Experts (IGE) on Cybercrime; the World Trade Organization (WTO) processes on e-commerce; and the Moratorium on Customs Duties on Electronic Transmissions. By looking at international multilateral processes, South African stance on digital sovereignty and its quest to construct a state-led form of digital sovereignty are explored as a reaction to power dynamics in the international system of the governance of the internet. Nevertheless, the study looks inward to reflect on the national posture of digital sovereignty by highlighting national positions in international *fora* dealing with digital policies.[1] More specifically, at a national level, the policy and regulatory response to the *platformization* of the digital economy (Poell et al., 2019), techno-authoritarianism, and the increase of digital regulation of cyberspace is explored through a critical review of digital policy and regulatory processes related to online content regulation, regulation of bulk surveillance, data policy, and cybercrime. In Section 4.9, the emerging stance of South Africa on digital sovereignty is discussed through the lens of securitization and development.

4.2 SOUTH AFRICA'S ROLE AS A "DIGITAL SWING STATE" IN GLOBAL GEOPOLITICAL LANDSCAPE

Generally speaking, a state-centric approach to digital sovereignty focuses on states' capacity to exert control on digital infrastructures in their territories and datasets relating to their citizens (Couture & Toupin, 2019). Although it is a broad concept, digital sovereignty can be defined as "the right of a state to govern its network to serve its national interests, the most important of which are security, privacy and commerce" (Lewis, 2020). This definition may not seem too problematic when applied to mature economies and democratic countries capable of boosting their economies through competition policy and economic regulation while upholding human rights online. However, serving national interests and governing national networks might have different connotations in small and emerging economies for many reasons. Although developing countries share similar security, privacy, and economic growth objectives, state organizations in emerging economies are poorly resourced to put in place the necessary policy and regulatory mechanisms to effectively

[1] South African statements during the meetings until end of 2021 of the UN OEWG were reviewed. The statements were reviewed across the main themes of the OEWG: International law, cyber norms, confidence building measures, cyber capacity building, and emerging threats in cyberspace. A summary of the statements is available from the Global Partners Digital's Africa OEWG Positions Tracker, available at the following link: https://africa-oewg.org/.

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

counterbalance anticompetitive behavior in digital markets, predatory data extraction practices, and various cyber risks and cyber threats. Besides, democratic assumptions of freedom of expression[2] are often perceived as a threat of established political orders. Lastly, digitalization may result in state control over digital lives and citizens' political positions through misinformation (Pretorius, 2021) and mass surveillance.

In his 1996 *Declaration of the Independence of Cyberspace*, John Perry Barlow, a proponent of a *laissez-faire* approach to the internet's governance, asserted that cyberspace was a new territory that governments should not regulate. Since then, many things have changed. The number of policies and regulatory and legislative initiatives on the governance of the internet has increased dramatically. Different countries and regions have adopted diverging approaches to digital space governance. States have gained greater control of how the internet is used within their borders as a result of growing risks to security and privacy, combined with the erosion of national sovereignty from global connectivity (Lewis, 2020).

Interventions to spur digital competitiveness go beyond regulatory interventions, which can also take the form of new technological standards for digital infrastructure. A growing number of countries discuss plans to recreate national boundaries in cyberspace (Shcherbovich, 2021) through national Domain Name Systems or data localization laws (Lambach, 2019) or by exerting control over their citizens through technology (Shahbaz, 2018). For instance, contrary to the libertarian point of view of Barlow and the multi-stakeholder approach to internet policymaking, there is the recent Chinese proposal to redesign the TCP/IP protocol stack to allow for centralized government control over authentication and internet communication (Gross & Murgia, 2020). Another form of state control over the internet within national borders is shutting down the internet during political elections,[3] a practice implemented by authoritarian or even democratic countries.

[2] Democratic freedom of expression recognizes that everyone's human rights are the same and therefore must be given similar consideration. In a democratic society, the right of freedom of expression is equal for everyone and it comes with the responsibility of respecting everybody else rights. In such a democratic system, the liberty is not arbitrary power, but it is based on accountability. If freedom of expression becomes an act of domination, it infringes the rights of others and therefore a system of justice should hold agents responsible. In this governing system, a democratic state is considered an effective instrument to protect human rights and abolish domination.

[3] In 2019, Access Now documented cases of partial or total internet shutdowns in 25 African countries, compared with 20 in 2018 and 12 in 2017. In October 2020, Tanzania restricted access to the internet and social media during elections. In June 2020, after unrest following the killing of a famous Oromo singer and activist Hachalu Hundessa, Ethiopia forced an internet shutdown that lasted for almost a month. Access Now also documented that Burundi, Chad, Guinea, Mali, Togo, and Zimbabwe also restricted access to the internet or social media at some point in 2020. More recently, in the run-up to the presidential election on January 14, Uganda shut down the internet.

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

Politically driven by digital sovereignty and strategic autonomy (Timmers 2020), Europe has found its digital "third way" (Siebert, 2021) by placing itself as a regulatory superpower by setting rules underpinned by civil rights and self-determination, in opposition to the Chinese techno-authoritarianism (Polyakova & Meserole, 2019; Wang, 2021) and the US surveillance capitalism (Zuboff, 2019b). At the end of 2020, the EU launched a significant regulatory initiative (i.e., the Digital Services Act package) and in November 2022, the Digital Services Act and the Digital Markets Act were adopted by the Council of the European Union, intending to increase innovation, growth, and competitiveness in digital markets (European Commission, 2021). As part of its digital strategy, EU is investing in the "development of digital standards and promot[ing] them internationally" (Aggad, 2021). The new Africa–Europe digital economy partnership of the EU–AU digital economy task force, now advocates for the development of "policies and regulation in areas such as telecom[munications], data economy, data protection and privacy, start-up laws, e-commerce and e-government" (Aggad, 2021). Therefore, regulatory convergence on data use is already quietly happening under the umbrella of "technical assistance," which might have important repercussions on African citizens' privacy (Aggad, 2021). On the other hand, the US has gained an undisputed leadership over operating systems, social media, and cloud computing platforms, posing regulatory challenges to ownership and control of data and related commercial value (Roberts, 2020). Furthermore, as part of a broader US stated effort to address concerns about cybersecurity and data privacy, particularly regarding China's role in the global technology and telecommunications industry, the 2017–2021 US Secretary of State Mike Pompeo's "Clean Network"[4] program aimed to create a more secure and trusted environment for US technology and data with a particular emphasis on countering perceived threats from the Chinese Communist Party.

In response to the Trump administration's position against Chinese tech firms defined as national security threats, in September 2020, China announced its most ambitious contribution to international lawmaking on data governance with the Global Initiative on Data Security (WSJ, 2020). This was done on the one hand to attempt to shift control of the data security narrative away from the US, which, according to China's Foreign Minister Wang Yi, made "groundless accusations" against Chinese tech firms as national security threats and "used security as a pretext to prey on enterprises of other countries who have a competitive edge" (Wang Yi, 2020); and on the other, to set global standards on data security at a multilateral level (Tiezzi, 2020). The Global Initiative on Data Security invites countries to handle data security in a "comprehensive, objective, and evidence-based manner" while emphasizing the importance of a stable supply chain for

[4] The initiative, announced by the UN Secretary of State Mike Pompeo, goes under the name of The Clean Network. See https://2017-2021.state.gov/the-clean-network/index.html.

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

information, technology, and services. This initiative is also an invitation to all countries to consider other countries' approaches in managing their data and internet sovereignty (WSJ, 2020). Considering that affordable devices and networking infrastructures with increased accessibility for the majority of Africans are largely sourced from China (Cascais, 2019; Wilson, 2019), it is expected that national technological standards will be anchored in these suppliers that are supporting the closure of the usage gap. These standards will certainly shape African countries industrial policy and, as a result, its capacity of self-determination on digital sovereignty.

In this virtual space of competing positions on regulatory, technological, and industrial standards, many African governments' plans on digital transformation or on the ambitious Fourth Industrial Revolution (4IR) might increase the reliance of Africa on the US platforms, on regulations modeled after EU, and Chinese networking technologies. African countries are not self-sufficient in terms of technological innovation and development and, like many countries, import a considerable (if not all) portion of these technologies. This high dependence on technological innovation and digital transformation on global powers presents diplomatic challenges (Ndzendze, 2021) for digital sovereignty and self-determination in cyberspace.

Nevertheless, South Africa, as one of the pivotal middle powers in the Global South – together with Brazil, India, Indonesia, Saudi Arabia, and Turkey – stands out as a "swing state" within the BRICS alliance (Kupchan, 2023). This designation positions South Africa in a unique position where it maintains a degree of autonomy and the flexibility to craft its digital policies and navigate complex geopolitical landscapes independently. Unlike nations fully aligned with superpowers, as a "swing state," South Africa straddles the middle ground, allowing it to influence and even reshape emerging power dynamics (Fontaine & Kliman, 2013). As a middle power, South Africa has seized this opportunity to assert its influence in international relations (Kupchan, 2023). One defining feature of the group of "swing states" is the absence of strong ideological affiliations, setting them apart from previous groupings in the Global South, such as the BRICS. This lack of ideological bonds allows these states to adopt a pragmatic, transactional approach to foreign policy, amplifying their collective impact on the global stage. The intensifying rivalry between the United States and China offers a "swing state" like South Africa opportunities to leverage its positions, as both superpowers seek their alignment. This strategic positioning grants South Africa bargaining power with both the US and China vying for their support. However, digitalization might be an exception, particularly when it comes to foundational technologies such as semiconductors, artificial intelligence, quantum technology, 5G telecommunications, and cloud computing. South Africa is primarily a user of such technologies and therefore may need to make strategic choices between trading with the United States or China, as these domains are subject to rigid competition (Kupchan, 2023).

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

The following sections explore the South African approach to digital sovereignty and its evolving digital policy posture. I consider its positions in international processes related to cybersecurity and national development with regard to digital policymaking.

4.3 ICT FOR DEVELOPMENT NARRATIVE IN NATIONAL DIGITAL CONNECTIVITY POLICY

A state-centric approach to digital sovereignty focuses primarily on government strategies and actions to govern digital infrastructures and datasets in their territories. Like many other countries, South African authorities are designing strategies, policies, and rules and assigning responsibilities to the existing and new agencies to govern emerging digital technologies nationally. Differently from mature economies, the international stance of South Africa in the governance of cyberspace does not seem concerned about how to wield cyber power against its rivals (Dunn Cavelty & Egloff, 2019). On the contrary, the country's political priorities and policy objectives related to the governance of digital infrastructures, at least on official papers, emphasize leveraging digitalization to overcome some of the pressing national challenges such as poverty, unemployment, and inequality. Considering that the narrative on ICT development is predominant across all South Africa's main digital policy documents, the emerging model of digital sovereignty needs to be understood within the context of the ICT for development narrative.

There is almost undisputed and general understanding that improving connectivity will facilitate growth and development (UNDP 2015; World Bank 2016; WSIS 2018 in Roberts, 2021). The sustainable development goals (SDGs) include a focused approach for increasing use (target 17.8) and access to ICT; provide affordable and universal access to internet in least developed countries (SDG 9c); enhance regional and international cooperation and access to technology and innovation (SDG 17.6); and promote women's use of ICT for empowerment (target 5b). At an international level and a technical cooperation level, improving internet access and use in Africa[5] has been one of the main priorities of various UN agencies, whose objectives and goals have been translated in digital policy documents at regional and national levels (Calandro, 2015).

Nationally, the 2013 national broadband policy South Africa Connect (SA Connect) was designed to integrate supply- and demand-side approaches to foster a "dynamic and connected information society and a vibrant knowledge economy that is more inclusive and prosperous." South Africa Connect gives expression to South Africa's vision in the National Development Plan (NDP)

[5] Although internet usage figures in Africa are rising, they remain behind world figures. On average, in 2019, only 28.6 individuals out of 100 were using the internet in Africa, according to the ITU (2020).

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

of eliminating income poverty, decreasing inequality, and enhancing employment opportunities. In the problem statement presented in the broadband policy, reference was made regarding proven relationships between investment in the digital infrastructure and improvements in the overall economy. Furthermore, the document describes how making broadband available at competitive rates fosters an increase in broadband penetration, subsequently linked with job creation and overall economic growth.

Comparable goals are outlined in the National Integrated ICT Policy White Paper, which highlights how ICTs play a fundamental role in enabling the National Development Plan to achieve its goal of constructing a more inclusive society that reduces poverty and inequality. In this regard, ICTs play a transformative role, which is acknowledged in the Vision and Principles Chapter of the ICT White Paper. It emphasizes that “the main purpose of this White Paper is to unlock the potential of ICTs to eliminate poverty and reduce inequality in the country by 2030” (DTPS, 2016, p. 10).

More recently, also the 4IR plan expressed similar ambitions to those expressed in SA Connect and in the ICT White Paper. In the Summary Report & Recommendations presented by the Presidential Commission (January 2020), the South African “triple scourge,” that is, unemployment, poverty, and inequality, are the unequal outcomes of a history of exploitation and exclusion and are recognized as the “Grand Challenges” that the 4IR Commission, the State, and all institutional actors and citizens, in their capacity, have to overcome (Presidential Commission on the Fourth Industrial Revolution, 2020, p. 11). The 4IR and the related institutional arrangements, therefore, are about “contemplating solutions to South Africa’s development challenges” (Presidential Commission on the Fourth Industrial Revolution, 2020, p. 14).

Despite good intentions, policy and regulatory outcomes have been suboptimal. The national telecommunications market remains structured around integrated network and service operators, with two incumbents MTN and Vodacom dominating the mobile telecommunications market with a combined market share of 78% (Research ICT Africa, 2020). Many rural areas are still served by one or both incumbent operators where populations remain unable to benefit from the lower prices of smaller operators. Besides, the fiber-optic market has significantly penetrated only urban areas and the main transmission routes, leaving other areas poorly covered. Therefore, while the top-end market is well served, people with low incomes are paying a premium for low-value products. In addition, the proposed strategy of SA Connect to leverage private and public investments to provide connectivity to public buildings in under-serviced areas failed (Research ICT Africa, 2020). Lastly, the inability to release high-demand spectrum, compounded with the separation of the Ministry of Communications into two in 2014, severely undermined digital policy action and operationalization (Research ICT Africa, 2020).

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

All in all, while developmental aspirations underpin these national policy documents, they run short in terms of implementation. From a digital sovereignty perspective, there is little recognition of high dependency on digital supply chain and technological standards. Moreover, risks to human security might jeopardize developmental aspirations. The misuse of digital technology as a weapon, compounded with the risk of escalation of developing cyber offensive capabilities in the absence of shared regulation of how states should behave in cyberspace, could have unintended consequences for human security in South Africa (Allen, 2019).

4.4 A SECURITIZATION AGENDA IN REACTION TO CYBER THREATS

It is well known that in the past few years, and specifically after Snowden's revelations, digital security has received prominence in political security agendas worldwide (Dunn Cavelty & Egloff, 2021), including Africa. In these agendas, online risks become a security issue not always because threats are objectively measurable as such, but because actors define them as threats in political processes (Buzan et al. 1998, Dunn Cavelty & Egloff, 2021) by using the language as a performative act. The narrative of existential risks, sometimes put forward to justify increasing policy and regulatory measures on cybercrime, is often linked to high political stakes and it is a powerful mobilizer to legitimize extraordinary responses and undemocratic procedures (Dunn Cavelty & Egloff, 2021).

In this sense, cybersecurity measures have increased parallel to growing threats and risks emerging from access and use of digital technologies (Dunn Cavelty & Egloff, 2021). Different actors have used different representations of danger to create or change political, private, social, and commercial understandings of security in selected public spheres (Dunn Cavelty & Egloff, 2021). Within this political arena of problems, risks, and threats, cybersecurity policy is shaped at the intersection of "hypersecuritization," "everyday security practices," and "technification" (Dunn Cavelty & Egloff, 2021; Hansen & Nissenbaum, 2009). They do not exclude each other, but they are all present at different times in the cyber-insecurity discourse.

While hypersecuritization refers to the invoking of an imminent status of destruction and existential threats often without linkages to the historical incidents of similar scope, everyday security practices refer to the practice of creating a feeling of insecurity by connecting the hypersecuritization scenarios to the life and experiences of individuals, primarily to ensure compliance and partnership (Dunn Cavelty & Egloff, 2021; Hansen & Nissenbaum 2009). In the technification logic, the technical construction of the cybersecurity discourse is molded by technical knowledge and expert positions that are used to serve a political and normatively neutral agenda (Dunn Cavelty & Egloff, 2021).

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

In its submission on the Cybercrime and Cybersecurity Bill, Research ICT Africa[6] (2015) observed that draconian restrictions and regulations on the internet might be the result also of lack of empirical measurements and assessments of cyber threats and cybercrime. Research ICT Africa (2015) noted that to ensure the penalties are aligned with the crime, it is imperative that cyber-threat representations are fully documented as a means of preventing any (over)reactions that are linked with excessive implementation costs and lack of clarity in terms of the benefits (Research ICT Africa, 2015).

Within the South African context, the country adopted a human-centered approach to national security in its 1996 Constitution, distinguishing it from the conventional state-centered approach. As Duncan (2018) observed, in light of South Africa's history of apartheid, a more refined definition that treats state protection as a higher priority over citizens could lead to a situation in which the government can abuse its power and shield itself from any criticism while simultaneously failing in its objective to address the underlying issues that put society at risk. A human security approach, on the other hand, deals with seven fundamental security threat domains[7]: food security, economic security, health security, personal security, environmental security, political security, and community security (UNDP, 1994). This human-centered approach to national security is perceived to be more democratic than a state-focused approach. However, Duncan highlights the need to put checks and balances in place to prevent excessive levels of scrutiny in aspects of public and private lives (Duncan, 2021). If national security achieves a "freedom from fear and want" (UNDP, 1994), such a broad framework might entail a strategic and operational expansion of intelligence (and, thereby, surveillance) to increasing "insecurities" and risks. As observed in South Africa, discourses related to securitization can serve to legitimize surveillance in ways not unlike the apartheid police state that preceded it (Kuehn, 2018).

4.5 SOUTH AFRICAN POSITIONS ON ICT STATE SECURITY IN UN PROCESSES

South Africa has been involved with the UN GGE on advancing responsible state behavior in cyberspace in the context of international security since the beginning in 2004 and 2005, although that process failed to produce a consensus report. Subsequently, it served as the only African representative in the second GGE in 2009 and 2010, and the result of which was a consensus report A/65/201 (2010). It did not take part in the third, fourth, and fifth GGE, but it had a seat in the recently concluded sixth GGE together with

[6] Research ICT Africa is a digital policy and regulation think tank based in Cape Town, South Africa. The author of this chapter is a senior research associate with the think tank.

[7] The seven threats to security are based on those identified by the 1994 UNDP Human Development Report.

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

Kenya, Mauritius, and Morocco from Africa, and with all BRICS countries, which were all represented in the recent GGE. South Africa has been not only an active member of the GGE but also one of the most active African countries during the substantive meetings of the OEWG, sponsored by the Russian Federation and established with resolution A/RES/73/27 in December 2018.

During these meetings, South Africa suggested several inputs including the consideration of gender disparities in ICT access and use and the recommendation of conceptual and practical clarification on the notion of a "human-centric approach." It also suggested that exchanges within the Southern African Development Community (SADC) and the AU could effectively function as Confidence Building Measures[8]. In its comments to the predraft of the UN OEWG report, South Africa has expressed concerns about stockpiling of ICT-related vulnerabilities by state actors[9] and has also called for a "long-term view" that includes binding instruments of international law "to hold Member states accountable and assist in the arbitration of grievances." In May 2020, at the United Nations Security Council (UNSC) held in an Arria-formula meeting[10] to discuss "cyber stability, conflict prevention, and capacity building," South Africa expressed concerns about malicious cyber acts aiming at damage or impairing health infrastructure or responses to the COVID-19 crisis (Pytlak, 2020b). Lastly, South Africa abstained on the UN L.8/Rev.1 (UNGA, 2020) on the extension of the mandate of the OEWG for another five years, tabled by Russia at the end of October 2020. During the meeting, South Africa stressed that although it supports the idea of extending the OEWG in general by two years, it would like to focus on the implementation of existing norms instead of developing new ones (Pytlak, 2020a).

From its statements, it is clear South African positions on international law are leaning toward the support for the creation of a new instrument in international law in the form of legally and politically binding norms under the aegis of the UN.[11] This is also quite clear in the BRICS context, considering that since the *eThekwini Declaration* (2013) on Partnership for Development,

[8] https://front.un-arm.org/wp-content/uploads/2020/04/south-africa-inputs-of-oewg-predraft.pdf

[9] A similar position was expressed by Digital Europe (2017), when it shared its concerns of governments exploiting vulnerabilities instead of reporting them to be fixed.

[10] An Arria-Formula Meeting is an informal meeting of the UN Security Council that is convened at the initiative of member or of a group of members of the Security Council to discuss various issues within the competence of the Security Council. The Arria-Formula Meeting mentioned in this chapter took place online under the presidency of Estonia to discuss issues related to cyber stability, conflict prevention, and capacity building.

[11] This might be also one of the reasons why in the United Nations General Assembly subsidiary committees, South Africa through the UN Third Committee that deals with human rights, humanitarian affairs, and social matters, voted in support of a resolution on countering the use of ICT for criminal purposes that will elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

Integration and Industrialisation, the discussions and initiatives on cyber-BRICS have intensified. BRICS countries have shared common interests and enhanced cooperation in the area of science, technology, and innovation, with the aim of designing a legal framework within which the various areas of this cooperation and partnership can grow and develop (Belli, 2021b). More recently, in September 2021, cybersecurity was a priority at the 13th BRICS summit, when BRICS leaders reiterated their willingness of "advancing practical intra-BRICS cooperation in this domain, including through the implementation of the BRICS Roadmap of Practical Cooperation on ensuring Security in the Use of ICTs and the activities of the BRICS Working Group on Security in the use of ICTs" (BRICS India, 2021, p. 7).

At the same time, during the third substantial meeting of the UN OEWG, South Africa stressed the importance of reaffirming that a universal cybersecurity framework can only be grounded in the existing international law, including the *Charter of the United Nations* in its entirety, and respect for human rights and fundamental freedoms (DigWatch, 2019). Therefore, it seems that South Africa is cognizant that despite the intention to work (also with BRICS) toward a UN cybersecurity framework, the country is already a signatory of a binding instrument of international law on cybercrime: *The Convention on Cybercrime of the Council of Europe* (better known as the Budapest Convention). While the two international efforts are not mutually exclusive, the envisaged UN Treaty on cybercrime probably will not create a different framework than the one already established under the Budapest Convention (for South Africa and for any other Budapest Convention's signatory).

The importance of addressing developmental issues has emerged when South Africa voiced the concern of developing states related to the increasing sophistication of malicious ICTs and the need to bridge the digital and gender divides. South Africa has stated the need to implement existing norms and their role in identifying capacity building and warned of strain on resources (DigWatch, 2021).

The commitment of South Africa in international cybersecurity is evident not only at the UN First level but also at the UNODC level, in particular with the open-ended intergovernmental expert group (IEG) to conduct a comprehensive study on cybercrime.[12] The IEG is a process particularly relevant for South Africa, considering that it has played a diplomatic role as Chair of the Bureau of the IEG. The country has occupied this role since 2011, making its most significant diplomatic stance in 2017 when it facilitated the adoption of a multi-year plan for delegations to interrogate the findings of the draft report on cybercrime matters affecting UNODC Member States.

[12] The UN Commission on Crime Prevention and Criminal Justice (CCPCJ) has been the main venue for discussing cybercrime within the UN context. The CCPCJ established an IEG based in Vienna, tasked with conducting a Comprehensive Draft Study on Cybercrime. The study, presented in 2013, is still subject of discussion among states (EU Cyber Direct (2021)).

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

In 2020, South Africa chaired the sixth session of the IEG on Cybercrime that deliberated on two important issues namely: (1) international cooperation and (2) prevention (UNODC, 2020). This was the last substantive meeting of the IEG, followed by a stocktaking exercise in April 2021 aimed at putting together a list of recommendations for submission to the CCPCJ. This session was also a platform for delegations from the United States (Nemroff, 2018) and its allies to contest Russia-led third committee resolution.[13] The contestation was to preempt the call of the IEG[14] on active participation of all Member States in the work of the ad hoc committee[15] to develop a new cybercrime convention (UNODC, 2021).

4.6 PROMOTING INCLUSIVE DEVELOPMENT IN WTO PROCESSES ON ELECTRONIC TRANSMISSION

Another perspective worth to explore to understand South Africa's approach to digital sovereignty is the country's position on electronic international trade. At that level, South Africa and India have argued in favor of suspension of the WTO Moratorium on Electronic Transmission.[16] Both countries have suggested a multilateral dialogue to promote an inclusive development-oriented approach to e-commerce. Such a dialogue, they argue, should include the examination of the challenges experienced by developing countries and least developed countries (LDCs) in relation to e-commerce and explore ways of enhancing the participation of such countries in digital transmissions. They have argued that the Moratorium has several implications for developing countries, including tariff revenue losses, and it has impacts on industrialization, the use of digital technologies such as 3D printing in manufacturing, and the losses of other duties and charges (IISD, 2020).

Since 1998, this Moratorium has been renewed biannually (except for 2003–2005 when the members failed to reach consensus in Cancun). The debate however on whether this Moratorium on custom duties on electronic

[13] Ad hoc committee established by General Assembly resolution 74/247.

[14] Concept note, Seminar on International Cybersecurity, cohosted by DIRCO and Research ICT Africa, January 2020.

[15] In December 2019, a significant development took place within the United Nations General Assembly when resolution A/RES/74/247 was adopted. This resolution set in motion a parallel process with the mandate to create an Open-ended Ad Hoc Intergovernmental Committee of Experts, comprising representatives from all regions. The primary objective of this committee was to work on the development of a comprehensive international convention aimed at addressing "the misuse of information and communications technologies for criminal purposes." This process commenced in August 2020.

[16] The WTO moratorium bans countries from imposing customs duties on electronic transmissions. It was adopted in 1998 during the Second Ministerial Conference that ended with the Declaration on Global Electronic Commerce. Since then, at every Ministerial Conference, WTO members have agreed "to maintain the current practice of not imposing customs duties on electronic transmissions."

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

transmissions should be done away with or made permanent has not been decided upon yet even after 20 years of discussions in the WTO (Roberts, 2020). Tariff revenue losses for South Africa are estimated at USD 37 million using bounded or most favored nation (MFN) duties and USD 25 million when using effectively applied duties (UNCTAD, 2019 in Roberts, 2020). This is due to the fact that South Africa and other developing countries and emerging economies (with the exception of China) are highly dependent on foreign digital networks and services such as telecommunications networks, cloud computing, social networks, and data centers. The bounded duties equal Rand 542 million or 1% of South Africa's tax revenue in 2017 (Roberts, 2020). Although these might not seem big amounts, the proportion of electronic transmissions in trade is expected to increase with the growth of the digital economy. Therefore, according to Roberts (2020), a permanent moratorium on customs duties essentially means an increasing loss of customs revenue for developing countries because of their position as large and growing net importers of electronic transmissions in trade. Further, the moratorium makes it virtually impossible to rebalance the current dependency on foreign services. Lastly, the Moratorium may impede countries from adopting rules for the access to data and appropriate incentives for transnational investments in local capabilities.

4.7 EMERGING NATIONAL REGULATION ON DIGITAL SOVEREIGNTY

Before delving into some of the policy and regulatory measures adopted to secure network infrastructures and citizens' data, it is important to contextualize these measures in the worrisome reality of increasing national vulnerability in cyberspace.

4.7.1 Cyber Vulnerabilities

Recent cyber incidents make it clear that South Africa is facing an undoubtedly real wave of unrelenting cyberattacks and incidents, which is affecting many economic sectors. Kaspersky (2023a) has reported that ransomware attacks in South Africa increased by 10% in the second quarter of 2023 in comparison to the first quarter of the same year, as well as phishing attacks, which grew by 7% between 2022 and 2023 (Kaspersky, 2023b). Not only do individuals and consumers fall victims of cybercrimes, but also public and private organizations alike. In the past few years, South Africa experienced a sharp increase in cyberattacks on all fronts that hit banks, internet service providers (ISPs),[17] utilities, and e-commerce platforms (Accenture, 2020), with smaller and less

[17] See, for instance, the cyberattack that in February 2023 hit RSAWEB, a nation-wide ISP (Smith, 2023).

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

resourced actors being the most vulnerable (Calandro & Berglund, 2021). According to SEACOM (2023), a private operator of Africa's first broadband submarine cable system along the continent's Eastern and Southern coasts, South Africa has the highest number of ransomware and email attacks in Africa, with over 220 million email threats detected in 2021, costing the country billions in losses. In 2022, there was a surge in ransomware attacks, including a particularly damaging form of malware called "Agenda," which targeted healthcare and educational institutions, while the average ransom payout for South African institutions is estimated to be around R3.2 million. Regarding attacks to critical infrastructures, in May 2023, the Development Bank of Southern Africa (DBSA) experienced a ransomware attack by a threat actor believed to be the Russian group Akira (DBSA, 2023). While the extent of the breach is still under investigation, DBSA reported that servers, logfiles, and documents were encrypted and suspects that various categories of stakeholders' personal information may have been unlawfully accessed or acquired (DBSA, 2023). In 2021, two incidents were particularly concerning. First, in September 2021, the Department of Justice and Constitutional Development's IT system was interrupted due to a security breach through a ransomware. While all information systems were encrypted and unavailable to the Department's employees and member of the public, the Office indicated that data was not compromised (Ngqakamba, 2021). Second, Transnet SOC Ltd., South Africa's port and rail company was attacked with a ransomware that encrypted terabyte of personal data, company files, financial reports, and other documents, forcing the operation to switch to manual processing of cargo (Gallagher & Burkhardt, 2021).

There are many interconnected factors that make South Africa an attractive target by cyber-threat actors. First, many South African internet users are novices and therefore inexperienced and less digitally literate than users in other more developed nations. A significant portion of the South African population is not always able to recognize different kinds of cyberattacks and may unintentionally fall victim of cybercrime. Second, lack of investment in cybersecurity inhibits South Africa's ability to put in place measures to prevent and mitigate advanced threats. Third, the development, implementation, and adoption processes of policies and mechanisms that combat cybercrimes are lengthy. Fourth, the South African Police Service (SAPS), which is now legally mandated to act against such crimes, lacks cybercrime training and is not knowledgeable in handling cybercrime-related cases (Dlamini & Mbambo, 2019) in addition to not having adequate resources to investigate, detect, and combat cybercrime. Finally, cybersecurity awareness is a challenge as well, increasing the risk of negligent use of ICT among citizens, consumers, public officials, and small and medium enterprises (Dlamini & Mbambo, 2019). These factors do not affect only South Africa, but are common to most countries and are particularly evident in most developing countries.

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

4.7.2 Data and Cloud Policy

To respond to increasing threats and risks to data security, one of the most significant policy developments indicating a possible emerging approach of South Africa on digital sovereignty is the Draft National Policy on Data and Cloud, published on April 1, 2021 by the Minister of Communications and Digital Technologies. The Draft Policy covers a number of areas such as access to data and cloud services, data protection, localization and cross-border data transfers, and cybersecurity measures. The Draft policy seeks to promote "data sovereignty"[18] and recognizes data as a "tradable commodity" (DCDT, 2021, p. 29) and a critical element for the digital economy, although it does not clearly define what these terms mean. Additionally, while the developmental spirit of the data and cloud policy is clear from its key objectives,[19] the document seems more concerned with how to address the lack of data ownership and control. According to the Draft Policy, most of the data centers and cloud computing infrastructure hosting data generated in South Africa are under foreign ownership.

The developmental spirit of the Draft policy is evident in the inception as it aims at enabling South Africans "to realise the socio-economic value of data" (Department of Communications and Digital Technologies, 2021, p. 13) and to ensure socioeconomic development for inclusiveness. The policy aspires to foster a digital economy that is data driven and data intensive. Explicitly, the Draft Policy places attention on leveraging the socioeconomic value of data through relevant policies and law that support access, reuse, and publication of data while also ensuring adequate privacy, protection, security, and confidentiality in line with the South African Constitution.

From the perspective of securitization, one of the biggest issues associated with this policy concerns the nationalistic elements and government's heavy control over data. Specifically, the Draft policy attempts to position the government at the center of data ownership,[20] control, and distribution in South Africa (Cohen, 2021). It states that "data generated in South Africa shall be the property of South Africa, regardless of where the technology company is domiciled. Government shall act as a trustee for all government data generated within the borders of South Africa." The plan contains clear characteristics of a state-led approach that will ultimately serve to establish

[18] The Policy explicitly refers to data sovereignty and its connection to security: "The Data and Cloud Policy seeks to strengthen the capacity of the State to deliver services to its citizens, ensure informed policy development based on data analytics, as well as promote South Africa's data sovereignty and the security thereof." Draft National Policy on Data and Cloud, p. 11.

[19] Some of the objectives of the draft data policy include "to ensure socio-economic development for inclusivity, promote connectivity and access to data and cloud computing, remove regulatory barriers and enable competition, and ensure the implementation of effective cybersecurity, privacy, data and cloud infrastructure protection measures," among others.

[20] Although ownership is not explicitly defined in the policy, the document refers to data ownership in a few sections in relation to data control (p. 30), to localized data storage and acquisition (p. 9) and to data ownership as a critical element for the digital economy (p. 20).

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

a High-Performance Computing and Data Processing Centre, which will act as a repository for "[all] data generated from South African natural resources [which] shall be co-owned by government and the private sector participant/s whose private funds were used to generate such."

In its written submission in the response to the draft policy, Research ICT Africa (2021) warned on the positions on sovereignty and localization of the Draft policy, stating that this does not support data flows required to increase trade under the African Continental Free Trade Agreement (AfCFTA),[21] arguing that in its current form the Draft policy prevents cross-border data flows. The document adopts a Russian approach to data storage in that it describes that a copy has to be maintained within South African borders in addition to storing copies for law enforcement purposes. Nevertheless, it states that citizen data[22] may be kept outside South Africa and cross-border transfer can be executed in line with the Protection of Personal Information (POPI) Act. This is markedly distinct from the European Union's General Data Protection Regulation, which emphasizes the need to maintain data security regardless of where it is stored (Cohen, 2021).

As such, to some extent, the Draft National Policy on Data and Cloud appears to adopt an approach that is relatively different to South Africa's POPI Act 4 of 2013, which is based on the EU's personal data protection model, specifically Directive 95/46/EC of the European Parliament and the Council of October 24, 1995. For example, cross-border transfers are not forbidden in South Africa unless they are not aligned with certain requirements, emphasizing the need for adequate legal protection, consent, performance of a contract, or the data subject's interests or benefit.[23] In this sense, adequacy

[21] The Agreement establishing the African Continental Free Trade Area (CFTA) was signed in March 2018 by the 54 Member States of the AU. Since then, 30 countries have deposited their instruments of ratification with the AU Commission. The Agreement lays the foundations for the future establishment of a Continental Common Market. Trading under the CFTA started on January 1, 2021.

[22] The Draft Policy refers to citizen's data in the section related to localization and cross-border data transfers. Nevertheless, it does not provide a clear definition of the term "citizen data."

[23] Regarding "data sovereignty," section 72 of POPI Act provides that:

(1) A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless any ONE of the following conditions/considerations exist –
  (a) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement that provide an adequate level of protection that reflects the principles of POPI;
  (b) the data subject consents to the transfer;
  (c) the transfer is necessary for the performance of a contract between the data subject and the responsible party;
  (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject; or
  (e) the transfer is for the benefit of the data subject.

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

mechanisms can be seen as a form of data sovereignty that does not preclude cross-border data flow. A data sovereignty's approach that recognizes adequacy mechanisms does not evoke necessarily data localization, but rather the possibility to transfer personal data freely as long as equivalent jurisdictional guarantees are applied.

4.7.3 Online Content Classification and Emergency Regulation against Disinformation

In the review of the policy posture of South Africa with regard to digital sovereignty, online content regulation provides an example on how state-centric and securitization trends are emerging in the governance of the digital space nationally. The Films and Publications Amendment Act 11 of 2019 (FPAA)[24] was highly criticized by human rights observers and termed as the "Internet Censorship Bill" (Mungadze, 2019) as it is overhauled for infringing on freedom of speech. While the objective of the law is to regulate the development, ownership, creation, and distribution of films, publications, and games with the underlying objective of protecting young people from any harmful material, the underlying definition of what is harmful and disturbing is somewhat vague. Its broad lexicon may engender a situation in which constitutional rights to privacy and freedom of expression are infringed (Mungadze, 2019).

In summary, while the Act appears to protect people against revenge porn or fake news and enables them to consult the Film and Publication Board (FPB) for remedy (ITweb, 2017), the Act requires ISPs[25] to block access to any sites that host repudiated classification content. After it has been enacted, the FPAA will give the FPB the power to demand that any content that is deemed to be prohibited is taken down. However, the Association of ISP (ISPA) has criticized the amendment on the basis that it goes beyond the FPB's mandate and creates an environment in which the FPB can censor content as a quasi-governmental department. This would be contrary to the existing arrangements, which give the courts the power to adjudicate defensible limitations to the freedom of expression (Freedom House, 2020).

A further regulation that could impede the rights of freedom of expression is intermediary liability. ISP's liability was limited by the Electronic Communications Act 2002, which required them to cooperate with takedown notices. However, the existing provisions fail to provide immunity to

[24] The Act was signed into law by the President and published in the Government Gazette on October 3, 2019.

[25] The FPB published draft regulations to implement the Act in 2020. Within these regulations, website owners are classified as "internet service providers." This significantly increases the costs associated with hosting websites and mandates that all online content providers submit content to the FPB for its oversight (Freedom House, 2020).

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

all forms of communications providers. The takedown process does not provide the individual who uploaded the material the right to argue against any claims. Nor does it allow people to seek recourse for false claims (Comninos, 2012, in Razzano et al., 2020). As such, in practice, the takedown process may represent an indefensible infringement of people's rights to freedom of expression. One proposed modification, which was designed to address the current lack of appeal process, did not improve the situation; it gave the complainant the right to decide on the validity of the response to the complaint. According to Rens (in Razzano et al., 2020), a notice process may address many issues that arise on notice and takedown. This process would give the intermediary the obligation to share the notice that was received with the subscriber to attempt to strike a balance between the competing interests (Razzano et al., 2020).

In more recent times, false information about COVID-19 spread throughout South Africa via the internet. This false information has impeded the nation's COVID-19 response (Kazeem, 2020) and provoked the government to put in place emergency regulations in an attempt to fight the "infodemic" (WHO, 2021). Essentially, spreading any false information[26] related to COVID-19 became a criminal offense.[27] Although the enactment of the regulation resulted in multiple arrests in the early stages of the pandemic, there was no evidence of government abuse of this power (Wild, 2020). Rather, the state collaborated with technology companies and fact-checkers to diminish any proliferation of false information (South African Government, n.d.). The strong response may have helped reduce the spread of hoaxes and rumors concerning COVID-19.

4.7.4 Downsized Mass Surveillance

To supplement the evolving national approach to the regulation of online content, the national regulation of surveillance provides a further case of securitization in the governance of the digital sphere. Surveillance is perceived to be illegitimate or unconstitutional if it fails to sufficiently delineate the process by which an individual is informed that their information has been intercepted or fails to make it clear what processes need to be followed by officials who examine, replicate, share, or sort any data that they access as a result of intercepting communications. In South Africa, the Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA) outlines the legal requirements associated with the interception

[26] The focus is on information that is purposefully rather than unconsciously false – disinformation, not misinformation.

[27] See COVID-19 regulations issued in terms of Section 27(2) of the disaster management act, 2002 (https://cdn.24.co.za/files/Cms/General/d/8296/998082c0829846979a52f11933b621bd.pdf). Specifically, "any statement, through any medium, including social media, with the intention to deceive any other person about COVID-19; COVID-19 infection status of any person; or any measure taken by the Government to address COVID-19."

of communications. Regulation of Interception of Communications and Provision of Communication Related Information Act mandates that communication companies provide interception-capable networks. It also demands that intelligence agencies seek an interception direction (or warrant) from a certified judge prior to performing any type of communication surveillance. However, the Act was endorsed in a rushed response to the global panic observed in the aftermath of the September 11, 2001, terrorist attacks (Duncan, 2021). It has not undergone any modification since that period and has fallen behind any international developments on democratic oversight. The South African Constitutional Court questioned the constitutionality of the RICA in 2019 when it issued a judgment that temporarily halted the country's foreign signals intelligence (SIGINT) capabilities (Duncan, 2021). In the case of *AmaBhungane Centre for Investigative Journalism NPC and Another* v *Minister of Justice and Correctional Services and Others* [2019], the Court, after being informed of mass surveillance by state security entities, ordered: "It is declared that the bulk surveillance activities and foreign signals interception undertaken by the National Communications Centre are unlawful and invalid." This emerged in the absence of any express empowering legislation to do so. Legislation for mass surveillance needs to take into consideration necessity and proportionality of such a law. However, in light of the nature of proportionality requirements within international law, it is challenging to delineate what is a justifiable and lawful permission for this type of activity (Razzano et al., 2020).

4.7.5 Cybercrime Legislation

From a cybercrime perspective, as observed earlier, it is undisputed that cyberattacks have costed South Africa billions of Rands and that they have posed real risks to the well-functioning of governments, critical infrastructures, and affected confidentiality, integrity, and availability of individuals' data. That might be the reason why Hlase (2018) observed that due to the need of putting in place appropriate measures to protect information systems and critical infrastructures otherwise vulnerable to infiltration and sabotage, "securitization may be unavoidable" in South Africa (2018, p. 62).

The protracted process associated with establishing jurisdictional clarity on cybercrime concluded in June 2021 when it was passed as law. The President proclaimed that certain sections of the law to commence on December 1, 2021 (Sheik, 2021). As a result of the Cybercrimes Act 19 of 2020, the relationship between law enforcement bodies and electronic communications service providers (ECSPs) has been revamped, leading to the introduction of several new mechanisms for the SAPS to access and to maintain the preservation of any evidence held by ECSPs.

Particularly, Section 54 outlines several reporting obligations and the maintenance of evidence to be imposed on ECSPs and financial institutions,

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

which may help SAPS during the process of any investigations of an offense. However, the Act also specifies that these measures must not be misused to enforce obligations on electronic service providers or financial institutions to monitor any data that the ECSP or financial institution stores or transmits; or proactively seek circumstances or facts that are indicative of unlawful activity.

Despite these positive developments, a challenge associated with the Cybercrime Act concerns the operationalization of the law because resource limitations and competing policy priorities have culminated in a serious lack of personnel who have the skills required to establish defense against cybercrimes (Allen, 2019).

4.8 DISCUSSION

Based on the earlier discussions, it is possible to argue that national policy and regulatory directions for exerting sovereignty in the digital domain in South Africa are informed by developmental aspiration linking digital transformation to socioeconomic development. However, institutional failures due to the delayed implementation of digital policies extensively undermined policy and regulation actions on improving digital connectivity. Besides, existing and newly established state entities are struggling to cope with increasing responsibilities to protect citizens' rights to privacy, safety, and security online.[28] On the other hand, the country is facing an unprecedented wave of cyberattacks and incidents resulting from competing policy priorities and inadequate investment in cybersecurity and, more recently, from criminals capitalizing on COVID-19, which is affecting many economic sectors. From a geopolitical point of view, the high dependence on digital services from the US, technological equipment from China, and regulatory standards from the EU (McKenzie Baker, 2022) place the country also in a position of diplomatic pressure from diverging global powers and different approaches in the governance of the digital realm, undermining self-determination on digital sovereignty.

As a result, securitization trends are permeating an increasing number of areas of digital governance. It can be understood almost as a protectionist reaction to the fear of losing control over national digital assets and the benefits of digitalization. At the same time, however, the increasing use of surveillance and the use of social media for disinformation and misinformation campaigns are expression of the need of exerting control through manipulation of information.

Internationally, at the UN First Committee level, developmental ambitions are expressed in several inputs at the OEWG, those for instance related to the consideration of the digital divide and gender disparities in ICT access and

[28] On this note, South Africa's information regulator is struggling with lack of funding while it is battling to cope with rising incidents of data breaches (eNCA, 2020).

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

use amid a securitization agenda spurred by increasing threats of cybercrime. The position of vulnerability in cyberspace of South Africa emerged from its concerns on stockpiling of ICT-related vulnerabilities by capable state actors and not by the country's concerns with growing cyber offensive and defensive capabilities of adversary states.

At the level of international digital trade, South Africa has advocated for an inclusive and development-oriented approach to transnational e-commerce in the WTO process related to the moratorium on electronic transmission. While the ban from imposing customs duties on electronic transmission is perceived as a loss of tariff revenue and duties, in an international digital trade system, developing countries might become rent seekers considering that most of e-commerce would be incoming. Therefore, in addition to advocating for the removal of the ban on tariffs, a bigger effort should be placed on creating favorable conditions for outgoing e-commerce to grow.

Nationally, with the recent Draft National Policy on Data and Cloud, the country took a predominantly state-centric position on data sovereignty, stating that data generated in South Africa shall be the property of South Africa, with the government acting as a trustee for all government data generated within the borders of South Africa. While the ambition of the policy document is to realize the socioeconomic value of data and to ensure socioeconomic development for inclusiveness, the outcome may restrict data flows necessary to increase trade under the AfCFTA. Similarly, the approach to online content regulation is shaped by securitization forces through a state-centric vetting approach for the classification of digitally distributed content. On the other hand, the takedown procedure that gives expression to limited liability for ISPs (Parliament of the Republic of South Africa, 2022) has an impact on the rights of freedom of expression, because it does not provide a right to respond to claims made by a complainant, nor imposes adequate penalties for false claims. More recently, as a result of the infodemic related to disinformation on COVID-19, alongside emerging regulation to fight against the pandemic, disinformation on COVID-19 became a criminal offence. Lastly, practices of mass surveillance by state security agencies have been fought in court, which acknowledged them as unlawful and invalid.

4.9 CONCLUDING POLICY OBSERVATIONS

The South African state stance to digital sovereignty is at the intersection of a digital transformation for development and securitization agenda. Nevertheless, in a national context of cyber vulnerability, institutional failure to effectively implement inclusive digital connectivity and transformation policies and lack of personnel, skills, and capacity to deal with increasing cyber threats and cyber risks, balancing the need to securitize elements of the critical infrastructures and to protect data while respecting fundamental rights of privacy and freedom of expression is a major challenge for South African policy makers.

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press

In South Africa, cyber threats and vulnerabilities are growing in parallel with responsibilities of state actors to protect citizens' rights to privacy, safety, and security online. The public sector response is putting human and constitutional rights under pressure with increasing government control over various elements of the digital infrastructure. To improve developmental outcomes of digitalization while protecting privacy, safety and security online of South Africa citizens, policy options for digital sovereignty should consider elements of proportionality as the most important requirement that must be satisfied in the limitation of human rights. The four major elements of this principle are legitimacy, adequacy, necessity, and proportionality *stricto sensu* (Anđelković, 2017). At the same time, emerging digital policy regimes on data, cybersecurity, and online content governance should be human-centric to deal with the underlying factors that make society vulnerable, instead of abusing national security narratives to protect state actors from criticism. In this way, self-determination in cyberspace would respect human rights and would promote the human security approach to national security as enshrined in the 1996 Constitution. Lastly, in order to implement a positive digital sovereignty agenda for South Africa, existing digital policy regimes and legislation on data protection and cybercrime should be effectively implemented. This can be done only if the necessary skills and capacity in public sector institutions are in place, so that public authorities can tackle emerging threats and risks, leverage digital transformation for socioeconomic development, while protecting citizens' rights to privacy and freedom of expression.

https://doi.org/10.1017/9781009531085.006 Published online by Cambridge University Press