The South Africa Model of Open Internet Enabling Policy and Regulation

The Open Internet as cornerstone of digitalisation

Funded by the European Union

Implemented by a consortium led by Stantec

TABLE OF CONTENTS

Abbreviations list

ANIC	African Network for information Commissioners
APNIG	African Parliamentary Network on Internet Governance
AfriSIG	African School of Internet Governance
CC	Competition Commission
CSIR	Council for Scientific and Industrial Research
CIRT	Cyber Incident Response Team
C3SA	Cybersecurity Centre for Southern Africa
ECT Act	Electronic Commerce and Transactions Act
EC Act	Electronic Communications Act
FPB	Film and Publications Board
GDPR	General Data Protection Regulation
HSRC	Human Sciences Research Council
ICASA	European Independent Communications Authority of South Africa
ISPA	Internet Service Providers Association
MMA	Media Monitoring Africa
NCPF	National Cybersecurity Policy Framework
NDP	National Development Plan
NIP	National Infrastructure Plan
PAIA	Promotion of Access to Information Act
POPIA	Protection of Personal Information Act
RICA	Regulation of Interception of Communications and Provision of Communication Related Information Act
SMME	Small, medium, and micro-enterprises
SITA	State IT Association
SABRIC	South African Banking & Risk Information Centre
SANEF	South Africa National Editors' Forum
SADC	Southern African Development Community
SAP	Systems Application Protocol
USAASA	Universal Service and Access Agency of South Africa
WOAN	Wireless Open Access Network
ZADNA	ZA Domain Name Authority
ISPA	Internet Service Providers Association
IXPs	Internet Exchange Points

Executive Summary

Open Internet connectivity is recognised as a promotor of human centric development. Digital technologies and the Open Internet are two distinct concepts that, if they are blended into a consistent policy approach, create a digitization process that maximises the opportunities for social and economic growth.

Key to the success of the Open Internet is its decentralised architecture built on open standards and protocols, underpinned by a multi-stakeholder Internet governance model that involves government and non-government actors in open consensus-driven Internet policy dialogues. At the application level, closest to the internet user, democratically developed principles, regulations, and policies can be put in place regionally or nationally, to ensure fundamental rights and locally driven development.

The realisation of the Open Internet's potential for locally driven growth requires a comprehensive approach, separate but intrinsic to the investment in technology and connectivity and focused on the deployment of Open Internet digital infrastructure, the development of enabling policy and regulatory environments for Open Internet, investment in Open Internet skills and competences, the creation of an Open Internet economy, and participation in Open Internet governance.

This Roadmap elaborates on creating an enabling legal and regulatory environment for the Open Internet and explores South Africa's experience in creating such an environment.

South Africa was an early adopter of the Open Internet, and it has an elaborate and responsive policy environment that has enabled the growth of a dynamic internet sector. **The core strength of the South African model lies in its commitment to the "social openness" of the internet. The South African online environment is characterised by respect for human rights, particularly freedom of expression, association and privacy.** Mechanisms for responding to harmful use, for example hate speech or gender-based violence online, are developed and implemented with care to prevent violation of fundamental rights.

The South African context is also characterised by active engagement of industry and civil society in policy and implementation. Government monitors its own performance, and the institutional ecosystem is one that includes robust oversight at all levels. In terms of challenges going forward, more effective resourcing and capacity of implementation of policy goals is the foremost priority.

Ten factors are found to underpin the South African model for and Open Internet enabling policy and regulation. To maximise their capacity to support internet growth and openness going forward they need to be protected, promoted and strengthened:

- **Constitutional framework and Bill of Rights (1997):** The Constitution provides for an independent regulator, independent oversight institutions and rigorous public participation and, together with the Bill of Rights creates a context which supports internet openness and encourages its use to enable human rights and social and economic equality.
- **Public participation in policy formulation:** Policy development processes that provide for active public participation have resulted in better policy outcomes.
- **Responsive policymaking:** Policy is frequently updated to address emerging challenges and opportunities, and trends in digitalisation.
- **Relatively empowered regulatory institutions:** South Africa's Open Internet model is supported by institutions who, mostly, have clear mandates and can be held accountable. There is room for improvement, where is comes to capacity and independence, but there is a good base to work with.
- **Multistakeholder engagement:** South Africa applies the multistakeholder approach in internet governance at home (even though it is at times critical of this approach when applied to global internet governance processes). The government has a tradition of working with business and civil society locally. Non-state actors do feel this collaboration can be more consistent and comprehensive.
- **Independent oversight by civil society, the media and the research sector:** Not many civil society organisations or research institutions operate in the Open Internet sector, but the few that do play an important role in upholding rights; even when it involves strategic litigation. The South African media is fully independent, and has vibrant online, print and broadcast channels. Political and business media cover internet related policy and regulation in-depth.
- **Private sector engagement:** South Africa has diverse and dynamic internet industry that is well-organised and vigilant when it comes to participating in policymaking and interacting with regulators.
- **Effective national self-regulation and co-regulation:** South Africa illustrates that co-regulation (such as between ISPs and government on unlawful online content) and self-regulation (such as that practised by the media and the advertising industry) works.
- **Parliamentary oversight:** The relevant portfolio committee – Communications - holds government to account.
- **Access to data:** The national statistical agency, the regulator, operators, the revenue service and many other public and private institutions collect and share data that can support Open Internet policy, regulation and implementation.

The South African experience, while linked to the size and strength of South Africa's digital economy, and its historical and political context, presents useful and important lessons of the benefits of an open approach to the internet for other countries in the Global South.

1. The Open Internet as Cornerstone of Digitalisation

Digitisation is an unstoppable process. The Open Internet, which maximises the opportunities provided by digital development, is not and should not be taken for granted.[1]

Digital technologies and the **Open Internet** are two distinct concepts that are often mixed up and confused. Ensuring that the two go intrinsically together in the digitalisation processes of countries and regions is an important policy and investment choice that has an impact on all key drivers for social and economic growth. Communities that embrace Open Internet digitisation are better placed to reap the full benefits of digital development.

Key to the success of the Open Internet is its **decentralised architecture** built on open standards and protocols[2] and underpinned by **multistakeholder Internet governance**. The multistakeholder model involves both government and non-governmental actors in dialogues at the global, regional, and national level, and goes beyond the management of the technical and logical infrastructure.[3] At the application level **democratically developed principles, regulations, and policies** ensure respect for fundamental rights and empower a locally driven development.[4]

The realisation of the Open Internet requires a holistic approach from policy makers and stakeholders that goes further than investing in technology and connectivity. To take the necessary next steps, actions and investments must focus on five areas: the deployment of Open Internet digital infrastructure[5]; the development of enabling policy and regulatory environments for

1 The report 'The Open Internet as cornerstone for digitalisation' demonstrates that the internet's unpredicted spectacular growth and its ability to promote human centric development is underpinned by the current Open Internet model. Digital connectivity technologies as such, while essential, are largely agnostic of what type of Internet they support. If the internet further develops into more closed networks, this risks to lead to a cascade of negative consequences tempering the internet's growth and missing opportunities to drive innovation, investment, socio-political, economic, and cultural development around the world.
Degezelle W., et al. (2022) "The Open Internet as cornerstone for digitalisation. The Global Gateway Partnership Opportunities between the European Union and Africa." Stantec. October 2022.

2 The internet is constructed as one global network of individual networks that exchange data and information, without a centralised authority. Transfer of data between networks, and as such the exchange of information over the internet is possible because of the use of commonly agreed standards and protocols. Ibid p. 20-30.

3 The Open Internet's multistakeholder governance model, its venues, processes, and actors are described in the project's report. Ibid p. 31-34.

4 Examples of Internet-related policy, regulation, and e-government initiatives in Africa and Europa are compiled in the report. Ibid p. 57-65.

Open Internet[6]; investment in Open Internet skills and competences[7]; support for the creation of an Open Internet economy[8]; and participation in Open Internet governance[9]. These five pillars form clusters of investment priorities and partnership opportunities to be refined and scoped in response to national, regional and subnational contexts, local demand and already existing initiatives. A dialogue with local stakeholders on priorities will contribute to a more effective cooperation to create growth and socio-economic development driven by the Open Internet.

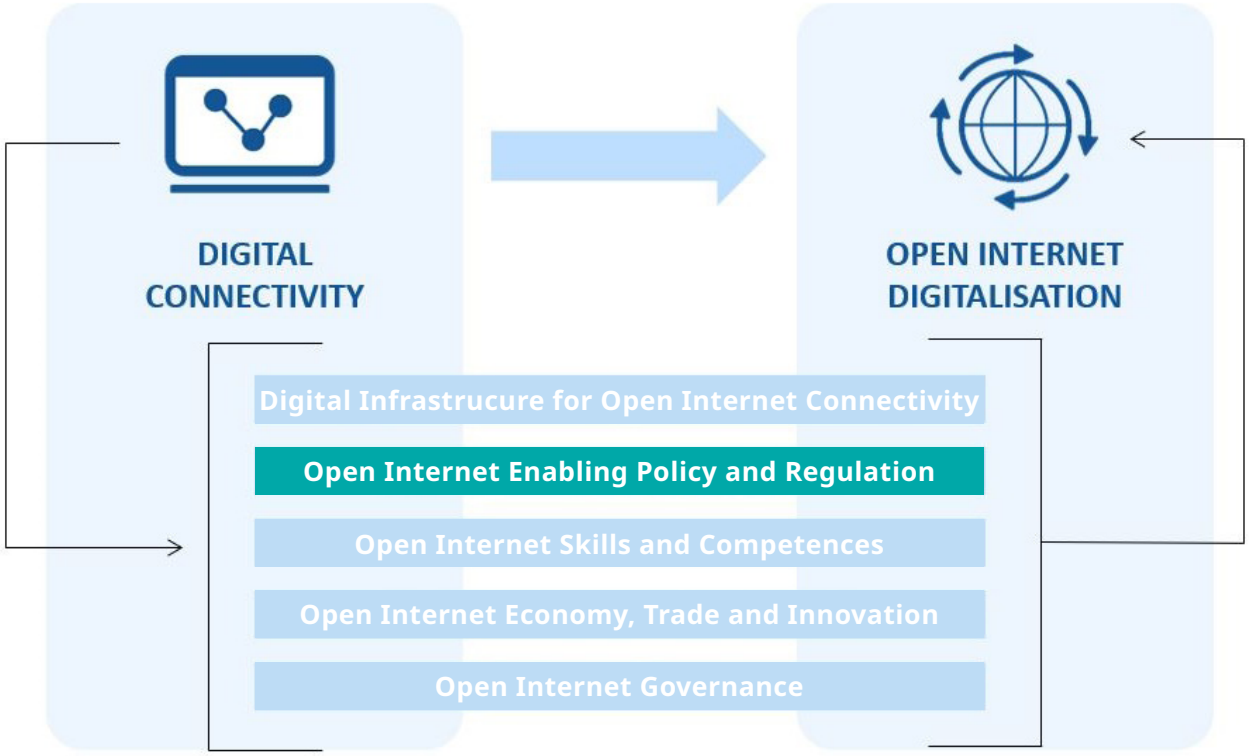

Figure 1. From Digital Connectivity to Open Internet Digitalisation

6 Ibid p. 57-68.
7 Ibid p. 68-74.
8 Ibid p. 74-82.
9 Ibid p. 82-87.

2. Open Internet Enabling Policy and Regulation

2.1 POLICY AND REGULATION ENABLING THE OPEN INTERNET

Policy makers bear the responsibility to make their countries and regions flourish in the new digital era. The digital policy strategies addressing this challenge are growing in substance and sophistication, however, the pressure and urgency of the matter may lead to a one-sided focus on creating connectivity and ill-considered regulation to address perceived or feared ad hoc negative impact of digitalisation. There is a latent risk that policy approaches de facto create more closed internet ecosystems which prove suboptimal in the short and longer term compared to an Open Internet.

As digitalisation and the internet expand so does the range of policy challenges, from closing existing digital gaps to avoiding new ones to occur, from keeping up with the latest digital developments to preparing for the next ones to come. Policy, legislation, and regulation that enable the Open Internet, create an environment for maximising the socio-economic benefits driven by an ongoing digital development. Policies that harm internet openness hamper the dynamics supporting local empowerment and a locally driven socio-economic development.

Policy and regulatory approaches to the Open Internet that encourage[10] access and digitalisation as well as competition, privacy, and respect for people's rights, create the necessary conditions for local digital content and entrepreneurship to thrive. This combined approach allows local economies to grow through innovation in the digital sphere and enables communities to reap the full benefits from the Open Internet as a resource for education and knowledge sharing.

10 The EU Global Gateway, for example, intrinsically combines 'infrastructure investments with country-level assistance on ensuring the protection of personal data, cybersecurity and the right to privacy, trustworthy AI, as well as fair and open digital markets.' European Commission. (2021) "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank, The Global Gateway"

2.2 BUILDING BLOCKS OF OPEN INTERNET ENABLING POLICY AND REGULATION

2.2.1 Opportunities and risks of internet related regulations

Policy and regulation can enable, slow down or even block the availability and use of the Open Internet in all its dimensions (technical, social and economic). Internet related regulations are opportunities to further the Open Internet but can as well pose serious risks to its development. To assess their impact, short- and long-term effects within and across boarders need to be looked at.

Closed internet models are in fact an important part of today's landscape, in particular within autocratic regimes, and they are based on regulations and associated technologies that are superimposed on the global and decentralised internet architecture. Sometimes regulations may pursue legitimate policy goals within democratic or less democratic countries but come with (intended or unintended) far-reaching consequences. For example, intentional government disruptions and shutdowns, generally backed by national or regional laws, may have important economic and technical impacts[11] that go beyond national borders; taxing access or social media use could stifle demand and negatively impact tax revenue from online services[12]; attempts to regulate online content might fail to be effective (e.g., in addressing disinformation) and instead result in stifling freedom of expression and privacy. Freedom of expression and privacy are themselves important building blocks for Open Internet as they stimulate the creation of content online and enable stakeholder participation in the Open Internet's multistakeholder governance.

At the same time, if not designed or implemented properly and accompanied by adequate legal safeguards and institutional capacity, internet-regulations might contribute to increasing bureaucracy, hinder investment and innovation, and violations of human rights.

The next section identifies different types of regulation based on the challenges they address and briefly highlights concrete opportunities and risks.

2.2.2 Types of regulation relevant to the Open Internet

Regulation of digital services and content is necessary to ensure a level playing field for private sector operators and to make sure that the online space is as safe as possible. Such regulation (as is the approach with the European Digital Services Act package[13]) should ensure that consumers are protected, and that online spaces are not used for incitement to violence or the distribution of harmful and illegal content. At the same time such regulation has to take great care that it does not stifle freedom of expression and the free flow of information online.

Privacy and personal data protection is not only a human rights concern but fundamental to the growth of the digital economy and the estab-

11 It is estimated that government internet outages between costed the world economy 42 billion USD between 2019 and 2023. Woodham, Migliano (2023) "Government Internet Shutdowns Have Cost $42 Billion Since 2019."

12 In Uganda, for example, the number of internet users declined by 15.7% after a social media tax was implemented, which in turn reduced tax revenue from online services supported by social media platforms, such as data sales and advertising. Kende, Abecassis (2019) "Impact of taxation on social media in Africa.

13 Digital Services Act: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) http://data.europa.eu/eli/reg/2022/2065/oj
Digital Markets Act: Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), http://data.europa.eu/eli/reg/2022/1925/oj

lishment of more secure and trusted dataflows between countries and continents. While many countries have legal frameworks in place, such laws, and in particular their loopholes and implementation, might provide coverage for effective mass-surveillance techniques deployed by states and companies.

Multi-faceted cybersecurity and cybercrime approaches underpin a secure and trusted Open Internet. Cybersecurity defines a technical approach to securing against attacks and errors.[14] National cybersecurity strategies, the establishment of Cyber Incident Response Teams (CIRTs), and national and international legal frameworks, partnerships and cooperation are pillars to guarantee secure and trusted digital infrastructure. This involves assessing and responding to risks to networks, devices, information, and, importantly, to people and institutions. At the same time, there exists an imminent danger when cybersecurity is being used as a pretext to create more closed and centralised networks that break away from the Open Internet as centralised architectures are more likely to contain single points of failure. Also, ill-designed cybersecurity laws, without enough safeguards and ambiguous scopes that open the door to unwarranted surveillance, are often used to target political dissent.

An effective cybercrime approach creates a secure and trusted online environment and is aimed at preventing, fighting, and punishing unauthorised and criminal behaviour.[15] Cybercrime laws and policies, and cross-border cooperation between law enforcement should reduce the risk and impact of criminal and fraudulent practices, e.g., on e-ecommerce, privacy, or data protection. At the same time, cybercrime strategies may be used for other purposes, including market protection or targeting political dissent.

Effective **copyright legislation** and enforcement protects the rights of creators, stimulates the creation and monetisation of online content and facilitates access to information. When properly designed, they stimulate a locally driven digital content and the proper remuneration of local digital creators vis a vis big digital platforms. Copyright laws can, at the same time, be used for establishing censorship mechanisms and close local digital markets to the inflow of international content and ideas.

e-Government and digital public services strengthen citizen-centred governance and contribute to greater transparency and accountability. while enabling citizens, enterprises and organisations to carry out their interactions with government more easily, more quickly and at lower cost.[16] At the same time, if not designed or implemented properly, for example when missing accompanying organisational changes and legal safeguards, e-government regulations might create more bureaucracy or even be highly problematic in terms of guaranteeing citizens' privacy.

14 Knodel, Kumar, van Hoorenbeeck, Degezelle. 2022. "Mythbusting: cybercrime versus cybersecurity.'

15 Ibid.

16 European Commission. 2022. "Shaping Europe's digital future: e Government and digital public services"

3. The South Africa Model of Open Internet Enabling Policy and Regulation

3.1 SOUTH AFRICA'S DIGITAL CONNECTIVITY CONTEXT

Population	60,6 million in 2023[17]
Internet Users	For 2021 - 72.31 % percent of the population use the internet[18]. 27.7 % of the population remains completely offline
Social media users	For 2022 - 25.80 million social media users in January 2023, equating to 42.9 percent of the total population[19]
Cellular mobile connections	For 2021 - A total of 100,3 million active mobile phone connections with 68,7 million mobile broadband subscriptions [20]
International bandwidth speed	For 2021 - 2405421 megabits per second[21]
Share of web traffic by device	For 2022 - mobile 78.84% - laptop and desktop 19.94% - tablet 1.2% console 0.02%[22]
Network coverage	99.9% of the population[23]
Data centres	For 2023 – 56 data centres – more than a third of the total number of data centres in Africa are located in South Africa[2425]
No. of .za domain names	2,542,613[26]

As can be seen from the above statistics mobile broadband connectivity in South Africa is widely available, but usage is affected by the cost, which is still relatively high in spite of prices dropping in the last 10 years as a result of a more competitive market at the level of international connectivity – undersea fibre – and national fibre backbone.

South Africa was an early leader in Africa in internet penetration and uptake and this is reflected in the policy environment which includes the provisions for the building blocks discussed above: digital services and content, data protection, cybersecurity and cybercrime, copyright, and e-government. The first legislation govern-

17 Statistics South Africa. 2022. "60,6 million people in South Africa"
18 ITU estimates for 2021. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
19 https://datareportal.com/reports/digital-2023-south-africa
20 Ibid ITU data provided by the Independent Communications Authority of South Africa.
21 Ibid
22 https://www.statista.com/statistics/1229072/web-traffic-by-device-in-south-africa/
23 https://datahub.itu.int/
24 Modise. 2023. "Mapping the growth trajectory of South Africa's data centre industry".
25 https://cloudscene.com/market/data-centers-in-south-africa/all
26 https://domainnamestat.com/statistics/tldtype/country

ing internet use and digital transactions, the Electronic Commerce and Transactions Act (ECT Act) came into effect in 2002. In some respects, this positive trend has continued, for example, mobile data coverage is 99.9%, there is a dynamic local domain name industry, strong uptake of social media and dramatic growth in the number of data centres. The South African internet and technology sector remains vibrant, serving as a hub for the Southern African region and beyond. South Africa's leadership has continued in one particular aspect of Open Internet development: "social openness". Social internet openness is defined by the OECD as "respect for human rights, such as privacy, freedom of opinion and expression, freedom to associate, the right to education, and freedom from discrimination".[27]

Since the birth of its democracy in 1994 South Africa has had a strong commitment to human rights and this is reflected in its approach to internet policy and regulation. This has led to the internet playing an enabling role in broader social and political engagement and in media development. South Africa has also demonstrated commitment to public participation in policymaking. Chapter two of the South African Constitution contains the "Bill of Rights"[28] and all policy and regulation need to comply with its provisions. Challenges from business and civil society has frequently sent policymakers back to the drawing board to ensure policy instruments comply with the Constitution.

The Bill of Rights[29] contains rights crucial for an Open Internet with people's empowerment at its centre. Its provisions include equality; human dignity; freedom and security of the person; privacy; freedom of religion, belief and opinion; freedom of expression; assembly, demonstration, picket and petition; freedom of association; political rights; education; language and culture; and access to information. Linked to this solid normative framework is a further strength of the South African model, a robust system of democratic governance and public oversight. South Africa placed 4th in Sub-Saharan Africa in The Economist's 2022 Democracy Index (after Mauritius, Cape Verde and Botswana).[30] This is reflected in the internet environment. Dynamic and independent media and civil society sectors contribute to providing oversight and demanding accountability from government, public institutions and business.[31] Rule of law remains strong and social assistance programmes, such as the social and child support grants provide invaluable support to the poorest of the poor and has been praised by the World Bank.[32] Evidence suggests that people draw on these grants to cover communication costs.

Challenges can be clustered into two linked areas: (1) effective implementation of policies and strategies, and (2) relatively high levels of digital inequality. In spite of good coverage, the cost of communications remains relatively high, and many people can simply not afford to be connected. Challenges related to implementation have multiple dimensions: lack of sufficient institutional capacity, lack of investment in underserved areas, differences of views between regulators and policymakers, low economic growth, policy complexity, and, to a large degree competing priorities at the level of national

27 OECD (2016) "Economic and Social Benefits of Internet Openness". p. 72

28 Constitution of the Republic of South Africa. 1997. "Chapter 2: Bill of Rights"

29 The South African Bill of Rights is a detailed and user-friendly document which addresses a wide range of civil, political, social, cultural and economic rights. South Africa is a signatory of all the major human rights treaties and an active member of the United Nations Human Rights Council, and, at African level, participates in the African Commission on Human and People's Rights.

30 The Economist. 2023. "The state of democracy in Africa and the Middle East: An EIU survey makes for glum reading. But there are some reasons for optimism"

31 Corruption in both the public and private sectors is a serious cause for concern, but at the same time, there are active processes – and responsible institutions - to counter corruption and to bring culprits to justice.

32 Oosthuizen,Morné. 2021. "South Africa : Social Assistance Programs and Systems Review (English)"

development.

Digital inequality is in a large part the consequence of broader economic and social inequities but effective implementation of policies, such as for example South Africa Connect, the national broadband strategy, can help address it. "South Africa remains the most unequal country in the world, and lack of digital access is impacting employment and education, two of the country's best chances at improving equality."[33] Insufficient infrastructure, lack of electricity, high cost of devices and data, and low levels of digital literacy present persist barriers to meaningful connectivity.

In its most recent (2019) ICT Price Basket ranking the ITU placed South Africa in position 117 among the 173 countries ranked from cheapest to most expensive. A fixed-broadband basket with a monthly data usage of a minimum of 5 GB was priced at 6.54% of GNI per capita or $31.18 USD.[34] On average, one gigabyte of mobile internet in South Africa cost 2.04 USD, compared to, in Kenya 0.84 USD.[35] Vulnerable and disadvantaged groups such as women, children, rural populations, and persons with disabilities are disproportionately affected. But so are the millions of South Africans without jobs. In the first quarter of 2023, 32.9% of working age South Africans were unemployed.[36] Youth unemployment -- measuring jobseekers between 15 and 24 years old -- was 62%.[37] Millions of South Africans (an estimate of 47,7% of the population) rely on social grants paid by the government and research indicates that a substantial part of these grants is being used to pay for communications (mobile voice and data).[38]

Government is aware of these challenges and take measures to address them. For example, in 2016 the South African parliament held public hearings on "the cost to communicate" convened by the Telecommunications and Postal Services Portfolio Committee[39] and this group periodically monitors implementation of its recommendations. The recent National Infrastructure Plan (see below) identifies digital as a key pillar.

3.2 THE SOUTH AFRICA MODEL OF OPEN INTERNET ENABLING POLICY AND REGULATION

3.2.1 Policy framework

South Africa has an elaborate human-centric policy and regulatory environment which is generally responsive to trends in digitalisation and internet governance. But it can, at times, make implementation challenging. Translating good policy intentions into effective implementation requires resources and skill. The public sector, in particular, lacks sufficient capacity and medium to small private sector operators struggle to navigate the resulting policy complexity. To understand this context, it is necessary to look at both core documents that lay out an overarching vision, as well as topic-specific policy instruments.

Overarching and infrastructure development policies

Three core documents produced in the last 15 years provide an overview of the principles and goals of South Africa's model for enabling

33 Mlaba. 2021. "How Is South Africa's Digital Divide Making Inequality Worse in the Country?"
34 https://www.itu.int/net4/ITU-D/ipb/
35 https://www.statista.com/statistics/1181015/price-for-mobile-data-in-kenya/
36 https://www.statssa.gov.za/?p=16312
37 https://tradingeconomics.com/south-africa/wages
38 Patel. 2023. "47% of South Africans rely on social grants - study reveals how they use them to generate more income"
39 Parliamentary Monitoring Group. 2016. "Cost to Communicate: public hearings, Telecommunications and Postal Services."

regulation for an Open Internet. They are the National Development Plan (2011), SA Connect (2014), and the National Integrated ICT Policy White Paper (2016).

The National Development Plan (NDP): Completed in 2011 the NDP outlines a vision that includes, by 2030 "...a widespread broadband communication system will underpin a dynamic and connected vibrant information society and a knowledge economy that is more inclusive, equitable and prosperous. "[40] Follow up on implementation of the NDP is located in the Presidency, which is positive in that it receives the attention of the President and cabinet.

National broadband strategy: "SA Connect", the country's national broadband strategy was published in 2013 in terms of section 3(1) of the Electronic Communications Act 36 of 2005 and formalised in the 2014 amendment of this Act. The inclusion of broadband targets in the NDP and the eventual development of SA Connect was a response to pressure from the South African Broadband Forum.[41] This campaign, led by civil society, the Association for Progressive Communications and its South African member, SANGONet, and industry through a coalition called "South Africa Connect" also benefited from collaboration with the World Bank. It was a response to debilitating shortages of broadband capacity, which, at the time, was stifling efforts to realise the potential of the internet for economic and social development.[42]

SA Connect provides a long-term vision, strategy, and roadmap for catalysing national broadband connectivity. It identifies responsible government departments and agencies and emphasises the need for multistakeholder collaboration. The roadmap was designed so that implementation could start immediately while also enabling enterprise and innovation and ensuring social and economic inclusion. A significant element was its emphasis on the development of an **open access national broadband network** built by harnessing both public and private sector contributions. In the amendment of the EC Act related to South Africa Connect a provision was made for the Minister of Communications to establish a multistakeholder broadband council to guide implementation of the framework. Invitation letters were issued to a diverse group of individuals from business, the research sector, civil society and public agencies. However, before they could have their first meeting, a cabinet reshuffle took place, a new minister was appointed, and after a few months of operating without clarity of engagement from the new minister, the council's chairs resigned in frustration.[43]

In retrospect this leadership change stands out as a watershed moment in South Africa's Open Internet development, marking a shift away from the responsible government department showing substantive commitment to a multistakeholder approach. In spite of these stumbling blocks SA Connect continued to be considered a priority and government recognised the lack of progress. In an effort to address this, the Department of Public Works and Infrastructure published the **National Infrastructure Plan 2050**[44] in 2022 with the following goals:

- High-speed broadband is universally accessible;
- Government services and buildings are digitally enabled;
- Regulation enables competitive and universally accessible broadband;
- Public sector capacity is strong and can drive

40 Research ICT Africa. 2017. "State of ICT South Africa"
41 Song. 2009. "South African National Broadband Forum".
42 Otter. 2009. "Broadband on agenda for new government"
43 Van Zyl, Gareth. 2016. "Exclusive: Tech experts quit govt broadband council"
44 https://www.gov.za/sites/default/files/gcis_document/202203/46033gon1874.pdf

the required policy agenda;
- Private sector participation in achieving universal broadband access is prevalent;
- Partnerships are strong and there are centres of digital excellence promoting a growing knowledge base of delivery and innovation;
- The ICT skills base is robust.

National Integrated ICT Policy White Paper (2016)[45]: In 2012 the Minister of Communications initiated a sector policy review. The review was done by a panel of independent experts who invited public comment, and based on that, issued a set of recommendations in 2015. When the final outcome of the review was published 18 months later as a White Paper, it met with some surprise and concern as the document differed from the 2015 recommendations and included the controversial decision to create a "super regulator". The White Paper announced that the existing statutory bodies regulating the sector would be abolished and replaced by a new "super" economic regulator with both content and market regulation mandates that would take over the functions of the communications regulator ICASA, the Films and Publication Board, the ccTLD, ZADNA, and the Universal Service and Access Agency of South Africa (USAASA). This "super regulator" would report to the Department of Telecommunications and Postal Services. Also controversial was the proposal to create a wireless open access network (WOAN) and to change the spectrum management policy in a way that would make it harder for operators to gain access.

But the White Paper also reflects the commitment in the South African model to open access and an Open Internet. For example, it increases competition in the delivery of national broadband objectives, which was previously allocated to a single state-sponsored operator. Research ICT Africa, in its assessment of the Paper, praised it and pointed out that the "explicit introduction of spectrum trading, as well as the 'use it or lose it' principle, displays recognition of the market's power to allocate this valuable resource more efficiently".[46] One of the specific Open Internet related topics addressed in the White Paper is network neutrality. It outlines the government's commitment to promoting net neutrality and includes a stipulation for a sector regulator to make recommendations on how it can best be achieved. This has not yet been done and there is ongoing discussion on the matter. The South African Internet Service Providers Association (ISPA) is strongly in support of network neutrality and has urged the regulator to take this into account.[47]

In August 2022 the then Minister of Communications and Digital Technologies stated in a briefing to the Parliament's Portfolio Committee on Communications that the merger of regulators had been abandoned.[48] Also in 2022, the Cabinet scrapped the WOAN, which was expected to increase competition in the mobile market dominated by two large players, MTN and Vodacom. The decision came as large operators continued to resist and a similar model in Mexico, the Red Compartida, filed for bankruptcy.[49]

Together with the documents discussed above, South Africa's Open Internet regulation is shaped by a set of legislative instruments that address specific aspects of the Open Internet and digital markets on a day-to-day basis. The integration – and increased competition - that the White Paper tried to achieve remains elusive,

45 https://www.gov.za/documents/electronic-communications-act-national-integrated-ict-policy-white-paper-3-oct-2016-0000
46 Gillwald. 2018, "The State of ICT in South Africa" p.38.
47 Cupido. 2021. "Is net neutrality legislation needed in South Africa?"
48 Mzekandaba. 2022. "Government abandons move to merge ICASA, FPB".
49 McLeod. 2022. "Government shelves the Woan".

but, on the other hand, many of these specific policies have been honed over time through being used, implemented, challenged, and, from time to time, amended in a manner that creates a relatively stable and enabling – even if imperfect -- policy environment.

Digital services and content

The **Electronic Communications and Transactions (ECT) Act** 25 of 2002[50] came into force during the World Summit on the Information Society's Geneva phase, and it reflects South Africa's early adoption of ICTs for development.[51] The ECT act has been amended on several occasions to stay up to date and provides for:

- Facilitation and regulation of electronic communications and transactions;
- Development of a national e-strategy;
- Promotion of universal access to electronic communications and transactions and the use of electronic transactions by SMMEs;
- Human resource development in electronic transactions;
- Prevention of the abuse of information systems; and
- Encouraging the development and use of e-government services.

The **Electronic Communications (EC) Act** 36 of 2005[52] repealed South Africa's first post-Apartheid ICT legislation, the Telecommunications Act of 1996. It has been amended twice, most recently in 2014[53] to include the national broadband strategy developed in 2013. This amendment included other ambitious goals, such as redefining use of the Universal Access Fund and establishing an e-rate, a discounted internet broadband rate for educational institutions; goals linked to South Africa's commitment to enabling Open Internet access and use.

The **Consumer Protection Act** 68 of 2008[54] along with the ECT Act and the Protection of Personal Information Act (see below) govern various aspects of doing business on the internet in South Africa. The provisions of the Act explicitly apply to any marketplace including the digital marketplace. Therefore, in the enabling internet context it provides for:

- Recourse against false or deceptive online advertising or advertising via social media;
- Promotion of a fair, accessible and sustainable online marketplace for consumer products and services and establishing of national norms and standards relating to consumer protection;
- Improved standards of consumer information in the online context;
- Promotion of responsible consumer behaviour (which addresses, for example, forwarding of misleading information in some contexts);
- Establishing the National Consumer Commission.

Many aspects of consumer protection are supported by self-regulation. For example, the advertising industry's self-regulatory body, the Advertising Regulatory Board,[55] developed a Social Media Code[56] which provides a clear set of rules for marketing via social media with a view to protecting consumers and promoting ethical conduct by marketers and advertisers. The Code addresses misleading advertising, including deceptive claims or offers.

50 https://www.gov.za/documents/electronic-communications-and-transactions-act

51 The ECT Act has since been amended by the Cybercrimes Act 19 of 2020 and the Consumer Protection Act 68 of 2008. A 2012 amendment of the ECT act fell away when POPIA – discussed below -- came into force.

52 "Electronic Communications Act 36 of 2005"

53 "Electronic Communications Amendment Act 1 of 2014"

54 https://www.gov.za/documents/consumer-protection-act

55 https://www.arb.org.za/

56 https://www.arb.org.za/assets/appendix-k-social-media-(2022).pdf

Draft National Policy on Data and Cloud[57] was tabled in 2021 to create an enabling environment for the provision of data and cloud services in an effort to move towards for a data intensive and data driven South Africa. It has provoked some controversy because of proposed data localisation requirements.

The **Film and Publications Amendment Act**[58] commenced on 1 March 2022 and gives the Film and Publications Board (FPB) more power to enforce provisions related to online content control with respect to managing harmful content. Some stakeholders have argued that these amendments make the previously straightforward online content control environment more complex and the implications for non-commercial content distributors is not clear.[59] Policy complexity is also a factor here as some of the provisions in this act overlap with those in the Cybercrimes Act.[60]

Privacy and personal data protection

The **Regulation of Interception of Communications and Provision of Communication Related Information Act** 70 of 2002 (RICA)[61] provides for:

- Regulation of the interception of certain communications;
- Mandatory sim card registration;
- Monitoring of certain signals and radio frequency spectrum and the provision of certain communication-related information;
- Prohibiting the use of telecommunication services which cannot be intercepted.

RICA has been controversial for making SIM card registration mandatory, and for enabling abuse by law enforcement and political interest groups of the provisions for lawful interception of communications. Mandatory SIM card registration was justified as a measure to combat cybercrime but has wholly failed in this respect. Pre-registered SIM cards can be bought on any street corner in South Africa.[62] [63] In 2021, in what is seen as triumph for Rule of Law, a group of South African and international civil society organisations won a challenge against RICA in the Constitutional Court.[64] The complaint centred on the Act not making provisions for the subject of a surveillance order being informed at any time that he or she had been under surveillance, not even after the fact. The Court also upheld the earlier High Court hearing which found that "RICA also failed to provide sufficient safeguards for the appointment of a designated judge to ensure the correct investigative procedures have been applied – creating space for executive interference, notes the court papers."[65]

The **Protection of Personal Information Act** 4 of 2013 (POPIA)[66] is considered as one of the best data protection laws in the world. It is based on the EU Data Protection Directive 95/46/EC but includes several stricter provisions. As a result, once the EU's 2018 General Data Protection Regulation (GDPR) came into force, POPIA was considered as "adequately protective". It is one

57 https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf
58 Films and Publications Amendment Regulation. 2022.
59 Majavu. 2022. "Films and Publications Amendment Act leaves online content producers hot under the collar"
60 Bowmans. 2022. "South Africa: Films and Publications Amendment Act Comes into Operation".
61 https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13
62 Roberts. 2022. "Why millions of Africans are right to resist mobile SIM card registration"
63 Privacy International. 2019. "Africa: SIM Card Registration Only Increases Monitoring and Exclusion".
64 Thakur. 2021. "Advocacy release: AmaB wins battle against spying abuse as ConCourt declares bulk surveillance unlawful, Rica surveillance provisions unconstitutional".
65 Malinga. 2021. "ConCourt RICA ruling will prevent abuse of Internet surveillance powers".
66 https://www.gov.za/documents/protection-personal-information-act

of the few data protection laws in the world that affords protection to individuals as well as to juristic persons such as companies and trusts.[67] POPIA provides for:

- Promotion and protection of personal information processed by public and private bodies and establishing minimum requirements for the processing of personal information;
- Establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of both POPIA and the earlier Promotion of Access to Information Act of 2000;
- The obligation to report data breaches to the Information Regulator and in Some cases also to data subjects;
- the rights of persons regarding unsolicited electronic communications and automated decision making;
- Regulating the flow of personal information across national borders.

Cybersecurity and cybercrime

The **National Cybersecurity Policy Framework (NCPF)** was gazetted by the State Security Agency in 2015 Its purpose was to "create a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of critical information infrastructure whilst strengthening shared human values and understanding of Cybersecurity in support of national security imperatives and the economy". This was intended to enable the development of an information society which takes into account "the fundamental rights of every South African citizen to privacy, security, dignity, access to information, the right to communication and freedom of expression." It mentions, explicitly, different stakeholder groups, stating that the "the NCPF seeks to ensure that Government, business, and civil society are able to enjoy the full benefits of a safe and secure cyberspace" and that to achieve this they "will need to work together to understand and address the risks, reduce the benefits to criminals and seize opportunities in cyberspace to enhance South Africa's overall security and safety including its economic well-being."[68]

The NCPF provides for:

- Measures to address national security in terms of cyberspace;
- Measures to combat cyber warfare, cybercrime and other cyber ills;
- The development, review and updating existing substantive and procedural laws to ensure alignment;
- Measures to build confidence and trust in the secure use of ICT.

Emerging from this was the *Cybercrimes and Cybersecurity Bill of 2015* which was challenged during the public participation process by civil society and internet service providers for being difficult to implement and risking human rights abuses because of using vague definitions. In response the Bill was redrafted as the *new Cybercrimes Bill of 2018*. Another round of extensive public comment and proposed changes resulted in the *2020 Cybercrimes Bill*, and it has since been signed into law by the President of South Africa. The **Cybercrimes Act 19 of 2020**[69] provides for:

- Creating and defining offences which have a bearing on cybercrime;
- Criminalising the disclosure of data messages which are harmful;
- Interim protection and further regulation of jurisdiction in respect of cybercrimes, the powers to investigate cybercrimes and aspects relating to mutual assistance in respect of the investigation of cybercrimes and the Executive to enter into agreements with foreign States to promote measures aimed at the detection, prevention, mitigation and investigation of cy-

67 Bowan. 2020. "After 7-year wait, South Africa's Data Protection Act enters into force"

68 "National Cybersecurity Policy Framework of 2015", Section 3, p. 14.

69 https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000

bercrimes;
- Imposing obligations to report cybercrimes;
- Capacity building.

The active engagement of diverse stakeholders from business, think tanks, human rights defenders and civil society in the drafting and finalising of this Act, resulting in stronger more implementable legislation, is another demonstration of the strength of the South African model. However, continued efforts are needed to effectively implement and strengthen South Africa's cyber resilience. Some sectors, particularly the financial services and fintech sectors[70] are well organised in terms of preventative measures, collaboration and access to human and technical capacity. They respond to threats proactively but micro crimes involving small amounts that target poor consumes still fall through the cracks. However, general awareness and response to cyber threats remains a challenge. South African citizens and institutions from all stakeholder groups lag behind many other countries in the world. Overall, both the South Africa public and private sectors are not coping well with cyber threats. Kaspersky currently ranks South Africa as 82nd in the world listing of countries ranked by cyber threats with Kenya ranked 35th (in other words more exposed to threats). What both countries have in common is that there is extensive adoption of ICTs by the private and public sectors, but lack of robust cybersecurity strategies and capacity. According to the Kaspersky report South Africa experienced 106,000 attempted backdoor and spyware attacks in the first quarter of 2023.[71] In January 2023 Fibre infrastructure company, Seacom, said that "South Africa remains the most targeted African country in terms of ransomware and business email compromise". In 2022 "more than half of South African firms were impacted by ransomware".[72]

The **South African Cyber Incident Response Team (CIRT)** was established by the NCSPF and is located in the Council for Scientific and Industrial Research (CSIR). Known as the South African Cybersecurity Hub[73] its mission is to "be the central point of contact for the private sector, civil society and citizens in order to enhance collaboration and promote a coordinated approach to cybersecurity including *inter alia* incident coordination, information dissemination, awareness building, sector CIRTs establishment, creation and promotion of national standards."[74] It operates with a fair amount of secrecy and perhaps suffers from lack of sufficient political leadership and support from the ministry it falls under, the Department of Digital and Communications Technology. As discussed elsewhere in this document the frequent leadership changes in South Africa's ministry of communications (not to mention frequent name changes) has, and continues to, impact on implementation.

As recently as June 2023 millions of Rands was stolen in a cyber-attack targeting the Department of Justice (the third time in recent years).[75] Ironically this attack occurred just as South Africa's Information Regulator found the Department guilty of negligence for not renewing security and virus checking software licenses. The resulting security breaches compromised the security of 1000s of citizens' personal information. In an unprecedented action in South Africa the Regulator fined the Department for an amount of

70 The South African Banking & Risk Information Centre (SABRIC) is an active in national and regional cybersecurity discussions providing information and support to the banking sector and to consumers. https://www.sabric.co.za/

71 Etike. 2023. "Nigeria, South Africa, and Kenya rank among top 100 for global online threats".

72 https://seacom.co.za/business-insights/sa-has-highest-number-of-ransomware-and-email-attacks-in-africa/

73 https://www.cybersecurityhub.gov.za/

74 Website of the Cybersecurity Hub https://www.cybersecurityhub.gov.za/ (Accessed on 3 July 2023).

75 Skiti. 2023. "Justice department loses millions in yet another cyber attack".

R5 million (Euro 245,000) on 4 July 2023.[76]

While this illustrates South Africa's weakness in terms of cybersecurity implementation, it also points to the strength of the South African legal and regulatory framework when it comes to the protection of privacy and the right to access information.

Copyright and intellectual property

The **Copyright Amendment Bill** B 13B-2017 (amending the South African Copyright Act of 1978) is another example of the effectiveness of public participation in policymaking in South Africa. The Bill includes an expansive "fair use" provision intended to enable use of the Open Internet to share and grow knowledge. The Bill does not use the term "fair use" but explicitly exempts a range of everyday research, education and information sharing uses of works and performances from copyright[77]. For example:

- Research, private study or personal use, including the use of a lawful copy of the work at a different time or with a different device;
- Criticism or review of that work or of another work;
- Reporting current events;
- Scholarship, teaching and education;
- Comment, illustration, parodie, satire, caricature, cartoon, tribute, hommage or pastiche;
- Preservation of and access to the collections of libraries, archives and museums.

Open Internet advocates have praised this legislation. But it has also provoked push back, including from, among others, the entertainment industry.

e-Government and digital public services

The **National e-Government Strategy and Roadmap of 2017**[78] has as purpose to guide the digital transformation of public services in South Africa to establish an "inclusive digital society where all citizens can benefit from the opportunities offered by digital technologies to improve their quality of life".

3.2.2 Institutional arrangements

Oversight and implementation of complex policy and regulation requires well-developed institutional arrangements and institutional capacity. This is implicit in the South African model and the responsibility for implementation of the policies discussed above is generally made clear in the documents themselves. In practice establishing, resourcing and maintaining effective institutional arrangements remains enormously challenging. The South African economy in general lacks human capacity. Nowhere is this felt more strongly than in the public sector where lack of human resource capacity is generally seen as a key factor in South Africa's struggle implementation of politics and delivery of services.[79]

A particular challenge has been the lack of continuity in the structure and leadership of the ministry and government department responsible for internet and digital development. In 2014, the Department of Communications was split into two: the Department of Telecommunications and Postal Services that dealt with postal services and old-style telecoms, and the Department of Communications that dealt with digital technologies. This changed yet again and currently there is one department that deals with both: the Department of Communications and Digital Technologies. Continuity at the level of leadership remains a challenge as the minister has changed at least 10 times in the last 10 years.[80]

76 Vermeulen. 2023. "Information Regulator tests its teeth — slaps Department of Justice with R5 million fine".
77 Library of Congress. 2018. "South Africa: National Assembly Passes Copyright Amendment Bill, Adopts Expansive Fair Use Exception"
78 https://www.gov.za/documents/electronic-communications-and-transactions-act-national-e-government-strategy-and-1
79 Mle, Ngumbela. 2020. "Building a capable state through proper human resource management"
80 https://en.wikipedia.org/wiki/Minister_of_Communications_and_Digital_Technologies

In spite of capacity constraints, the institutional context of South Africa's enabling policy environment is nevertheless a strength of the model. These constraints also indicate an entry point for filling some of the gaps discussed below.

Firstly, at an overarching level there are institutions that support South Africa's commitment to human rights, inclusion and democracy. Most of them deal with internet issues on a regular basis. Public institutions that support South Africa's democracy and Bill of Rights include:

- The South African Human Rights Commission;[81]
- Independent Communications Authority of South Africa (ICASA);[82]
- The Commission for the Promotion and Protection of the Rights of Cultural, Religious and Linguistic Communities;[83]
- The Commission for Gender Equality;[84]
- The Auditor-General;[85]
- The Independent Electoral Commission;[86]
- The Public Protector.[87]

Most of these institutions, including the communications regulator, ICASA, are identified in the Constitution which also prescribes that they should be independent from government and political influence. In practice their reputations, and independence from political influence vary. The Public Protector, for example, has been challenged repeatedly, and successfully, in court for political bias and problematic findings in her reports. On the other hand, in 2021 the World Bank ranked the South African Auditor General as one of only two fully independent such agencies in the world.[88]

ICASA issues licenses to telecommunications and broadcasting service providers and monitors their compliance with rules and regulations. Its mandate is outlined in the ICASA Amendment Act of 2012.[89] Councillors are appointed by the Minister on the recommendation of Parliament who vets them.

The Electoral Commission and the SA Human Rights Commission have both been proactive in Open Internet related matters. The SAHRC developed, in a consultative manner, the Social Media Charter in 2023 in an effort to support co- and self-regulation of social media[90]. It engages international and national internet companies on a regular basis on matters related to online expression, harmful content and mis and dis information.

As recently as July 2023 the Independent Electoral Commission announced that for the upcoming national election of 2024 it would partner with Google, Meta and TikTok, and a South African civil society organisation, Media Monitoring Africa (MMA) to prevent and respond to election-related disinformation.[91]

The National Assembly, South Africa's legislature, includes a multi-party parliamentary

81 https://www.sahrc.org.za/
82 https://www.icasa.org.za/
83 https://nationalgovernment.co.za/units/view/51/commission-for-the-promotion-and-protection-of-the-rights-of-cultural-religious-and-linguistic-communities
84 https://cge.org.za/
85 https://www.agsa.co.za/
86 https://www.elections.org.za/pw/
87 https://www.pprotect.org/
88 Omarjee. 2021. "World Bank ranks SA's Auditor-General as one of two in the world that has 'full independence'"
89 https://www.gov.za/sites/default/files/gcis_document/201409/35901gen970.pdf
90 SAHRC. 2023. "Social Media Charter: SHINE - Social Harmony through National Effort"
91 Electoral Commission. 2023. "Electoral Commission partners with social media giants to combat disinformation in 2024 National and Provincial Elections"

Portfolio Committee on Communications and Digital Technologies[92] that holds the executive and public sector institutions in the ICT sector accountable.

Other institutions that are part of the internet regulation context include:

- The Information Regulator[93] is an independent body established in terms of POPIA. It is subject only to the law and the constitution and it is accountable to the national assembly even though its budget is covered through the Department of Justice. It is empowered to monitor and enforce compliance by public and private bodies with the provisions of PAIA and POPIA.
- .ZA Domain Name Authority (ZADNA)[94] is a state-owned entity reporting to the Minister of Communications and Digital Technologies. The ECT act designates it as the regulator of the domain name industry in the country and its board members are appointed by the minister.
- Internet Service Providers Association (ISPA)[95] is the recognised internet industry body in terms of the Electronic Communications and Transactions Act (Act 25 of 2002). ISPA operates the South African unlawful internet content take-down notice process on behalf of its members. As long as they support and participate in this process, ISPA's members have special limitations on liability for content. ISPA also established and operated South Africa's Internet Exchange Points (IXPs)
- The Film and Publication Board[96] was historically responsible for the age-related classification of films and video games. Recently, after a long and contentious lobbying process, it has been mandated to take responsibility for aspects of online content regulation.
- The Competition Commission[97] (CC) has proven to be an effective watchdog and defender of consumer interests. Currently it is assessing whether there is anticompetitive or exploitative behaviour by online shopping and service platforms operating in South Africa. The study looks at both national and global players.
- State IT Association (SITA)[98] is the designated lead ICT service provider to government and in general the public sector. All procurement by the public sector takes place through SITA.

3.2.3 Access to statistical data including open telecom data

Enabling Open Internet policy and regulation depends on access to data, and in this respect the South African model is definitely a good-practice example. Freedom of information legislation (the Promotion of Access to Information Act, discussed below) compels both the private and public sectors to comply with requests from the public. The national statistical agency, Statistics South Africa[99] and the communications regulator ICASA are considered reliable sources of data. Nevertheless, there is a need for more "open telecom data" in the country as private operators are not always forthcoming with making information about infrastructure its usage available in the public domain; information which could be of assistance to smaller and regional first/last mile operators.

92 https://www.parliament.gov.za/committee-details/142
93 https://inforegulator.org.za/
94 https://www.zadna.org.za/
95 https://ispa.org.za/
96 https://www.fpb.org.za/
97 https://www.compcom.co.za/
98 https://www.sita.co.za/
99 https://www.statssa.gov.za/

3.3 SUCCESS FACTORS OF THE SOUTH AFRICAN MODEL FOR OPEN INTERNET ENABLING POLICY AND REGULATION

Ten main factors underpin the success of the South African model for Open Internet enabling policy and regulation. It should be noted however that they are not equally robust, and their capacity to support internet openness cannot be assumed to be sustainable. They are:

- **Constitutional framework and Bill of Rights:** Of particular relevance is that the Constitution provides for an independent regulator, independent oversight institutions and rigorous public participation. That, together with the Bill of Rights, creates a context which supports internet openness and encourages its use to enable human rights and social and economic equality. Moreover, the South African Constitution is not just a piece of paper. It is protected and promoted by rule of law, and the highest court in the land, the Constitutional Court.
- **Public participation in policy formulation:** Policy development processes that provide for active public participation have repeatedly resulted in better policy outcomes in South Africa.
- **Responsive policymaking:** Policy is frequently updated to address emerging challenges and opportunities, and trends in digitalisation. This strength, however, has a negative side-effect as efforts and capacity channelled into making new policy can serve as a distraction from implementing existing policy. It can also result in unnecessary policy complexity.
- **Relatively empowered regulatory institutions:** Many of them lack capacity, and political influence limits their effectiveness and independence. Nevertheless, South Africa's Open Internet model is supported by institutions who, mostly, have clear mandates and can be held accountable. There is room for improvement, there is a good base to work with.
- **Multistakeholder engagement:** South Africa has been a critic of the multistakeholder approach in global internet governance, but it applies it at home. Even though government's commitment to working with business and civil society can be inconsistent, the tradition remains. Carrying forward engagement that takes place during policy formulation into implementation would be a further improvement.
- **Independent oversight by civil society, the media and the research sector:** Not many civil society organisations or research institutions operate in the Open Internet sector, but the few that do play an important role in upholding rights; even when it involves strategic litigation. Research ICT Africa based at the University of Cape Town is a vital source of critical analysis for policymakers. The South African media is fully independent, and has vibrant online, print and broadcast channels. Political and business media cover internet related policy and regulation in-depth.
- **Private sector engagement:** South Africa has diverse and dynamic internet industry. It is also well-organised and very vigilant when it comes to participating in policymaking and interacting with regulators.
- **Effective national self-regulation and co-regulation:** South Africa illustrates that co-regulation (such as between ISPs and government on regulating unlawful online content) and self-regulation, such as that practised by the media and the advertising industry works.
- **Parliamentary oversight:** The relevant portfolio committee does try to hold government to account.
- **Access to data:** The national statistical agency, the regulator, operators, the revenue service and many other public and private institutions collect and share data that can support Open Internet policy, regulation and implementation.

3.4 RESULTS OF THE SOUTH AFRICA MODEL OF OPEN INTERNET ENABLING POLICY AND REGULATION

Overall, the South African model has had positive results, and these can be expanded through more effective implementation. The local ICT sector has a robust legal and regulatory framework that is suited to supporting an Open Internet. The public and private sectors and ordinary South Africans support an Open Internet. Even government supports an Open Internet. The challenge lies in leadership in implementation, addressing inequality, and strengthening sector and self-regulation.

In terms of economic openness, as already pointed out, South Africa was an early adopter of ICT for development and the work put into enabling policy and regulation in the first five years of the new millennium contributed to it having one of the largest ICT markets on the continent. MTN South Africa was the first mobile operator in Africa to introduce pre-paid mobile services; the model that has since become the norm across the continent.[100] A positive result of having an Electronic Commerce and Transaction Framework in place early on in the digital revolution (2002) is that it enabled online commerce in South Africa. The ECT Act tried to ensure compliance with OECD model law and EU directives which contributed to facilitating cross-border transactions.[101] Online shopping has continued to grow in South Africa, with local retailers competing very successfully with large global companies. By the end of 2022 the South African online retail market reached above $3 billion USD (R55 billion). It is expected that e-commerce will continue to grow with, for the first time, online retail exceeding 5% of the total value of retail in South Africa.[102] The biggest online retailers are wholly owned South African companies.[103]

Areas where South Africa has and continues to show leadership include mobile software, mobile payment and online banking apps and security software. Innovation frequently responds to the needs of small, medium and micro enterprises. While it is not considered to be sufficient, financial support provided by the South African government plays a positive role in enabling innovation in the tech sector and South Africa has a thriving start-up market. Through its ICT small, medium, and micro-enterprises (SMME) Development Strategy the government provides support capacity development, partnerships and incubation.

Bigger players also do well. "As an increasingly important contributor to South Africa's GDP, the country's ICT and electronics sector is both sophisticated and developing. Several international corporates operate subsidiaries from South Africa, including IBM, Cisco, Unisys, AWS, Microsoft, Intel, Systems Application Protocol (SAP), Dell, Novell, and Compaq. It is seen as a regional hub and a supply base for neighbouring countries."[104]

In their assessment of the South African ICT sector the US Government's International Trade Administration says that "South Africa's ICT products and services industry is penetrating the fast-growing African market. South African companies and locally based subsidiaries of international companies have supplied most of the

100 MTN introduced pre-paid mobile phone services as early as 1996. Initially applied to voice, the model extended to mobile data once it became available. https://en.wikipedia.org/wiki/Prepaid_mobile_phone

101 Gereda. 2006. «The Electronic Communications and Transactions Act»

102 TMO. 2023. "The changing face of e-commerce for South African retailers."

103 https://ecommercedb.com/ranking/stores/za/all?page=1&pagesize=50&specialist=all&currency=USD

104 International Trade Administration. 2023. "South Africa - Country Commercial Guide"

new fixed and wireless telecoms networks established across the continent in recent years."[105] They predict that consumption in the sector (including purchasing of devices) will rise but be affected by the economic downturn and the depreciation of the Rand's decreasing household purchasing power.

Another result of the enabling policy framework in South Africa is its thriving data centre sector. The early investment in IXPs by ISPA at a time that connectivity was in short supply contributed to this. Using cloud-based systems has become popular in South Africa – around 60% of large local companies in the country have implemented cloud computing - particularly because many South African companies are keen to expand services into African and global markets.[106]

In terms of social openness, the results have been extremely positive. South Africans are active users of social media, and according to a recent study, they spend more time online than people in any other country in the world. South Africans are connected for an average of 9 hours and 38 minutes daily on any device. "This is far higher than the global average of 6 hours and 37 minutes – and over 2 hours more than the USA – making us the biggest internet addicts in the world."[107] That internet speeds are slow might contribute to this, but the same study indicates that South African use of social media is above average[108].

Media freedom is an important result of South Africa's human rights framework, and media sustainability has benefited from Open Internet development. While online platforms pose a threat to viability of traditional media's business models, they also create opportunities for smaller, diverse, and local language media, including community radio, many who use internet-based streaming to reach their audiences.

Social media is used for political debate, marketing, connecting friends and family and even education. Freedom of expression and opinion is definitely an enabler of this. A positive result of the institutional arrangements of South Africa's enabling model is that when race or gender-based hate speech occurs on social media, the South African Human Rights Commission has been proactive in taking proportionate action to address it. Dangerous online speech remains a problem, and along with mis and disinformation one that needs to be addressed in the future.[109]

105 Ibid

106 Ibid

107 Businesstech. 2023. "South Africans are the biggest internet addicts in the world".

108 South Africans and average of 3 hours and 44 minutes each day on social media, compared to the global average of 2 hours and 31 minutes. On the extreme end of the spectrum users in the Philippines spending over 4 hours.

109 Allen. 2022. "Social media vigilantism is alive and trending in South Africa".

4. Conclusion: Is the South Africa Model applicable to other Countries?

The core strengths of the South African model derive from its broader context of constitutionalism, respect for human rights and rule of law, and oversight provided by a strong independent media and by civil society. Also important is active engagement from a vibrant national internet business sector and technical community. South Africa also has a diverse institutional Open Internet ecosystem – with policy documents mandating implementation to specific entities.

These are the outcomes of South Africa's historical and political development and are not easy to replicate. But there are some strengths that can serve as a helpful model for other countries:

- Having the same regulator be responsible for freedom of information legislation and protection of personal information has worked very well. Also, having the information regulator report to parliament rather than a government department has enabled it to hold government accountable for protection citizen's personal information.
- Self and co-regulation of content, the media and advertising bodies is effective and does not have to disempower the State or rely on taxpayers' money to uphold national laws and universal human rights.
- Public participation in policy formulation builds legitimacy and capacity and help ensure policy coherence.
- Evidence and data strengthen enabling policy and regulation – governments need to invest in national statistical agencies having the capacity and direction needed to collect Open Internet-related data.
- Freedom of expression drives social media use – South Africa has one of the highest levels of social media in the world. The fact that freedom of expression and opinion is protected by the Bill of Rights contributes to this.
- Critique from independent media and civil society builds confidence and legitimacy including among investors.

5. Acknowledgments

This document was developed by Stantec for the European Commission and is based on research by Stantec experts and interviews with local stakeholders. We warmly thank the interviewed stakeholders for their availability and time, in particular:

- Justine Limpitlaw - Electronic Communications Law Consultant/Link Centre, University of the Witwatersand.
- Mukelani Dimba - Head of Education and Communication at the South African Information Regulator.
- Izak Minnaar – South Africa National Editors' Forum (SANEF) and South Africa Press Council.
- Avani Singh - Attorney of the High Court of South Africa and digital rights specialist - board member of Media Monitoring Africa.
- Nthabiseng Pule - Project and Outreach Manager for the Cybersecurity Centre for Southern Africa (C3SA).
- Alison Gillwald, Executive Director, Research ICT Africa, University of Cape Town.
- Palesa Banda - Chair of the South African ccTLD, ZADNA.

6. References

- Allen, K. Lancaster, L and Machabaphala, T. "Social media vigilantism is alive and trending in South Africa". ISS Today, 12 July 2022. https://issafrica.org/iss-today/social-media-vigilantism-is-alive-and-trending-in-south-africa

- Bowan, N. 2020. "After 7-year wait, South Africa's Data Protection Act enters into force" International Association of Privacy Professionals. July 2020. https://iapp.org/news/a/after-a-7-year-wait-south-africas-data-protection-act-enters-into-force/

- Bowmans. 2022. "South Africa: Films and Publications Amendment Act Comes into Operation". https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/

- Businesstech. 2023. "South Africans are the biggest internet addicts in the world". 4 March 2023. https://businesstech.co.za/news/lifestyle/666999/south-africans-are-the-biggest-internet-addicts-in-the-world/

- Constitution of the Republic of South Africa, 1996 - Chapter 2: Bill of Rights. https://www.gov.za/documents/constitution/chapter-2-bill-rights

- Cupido, Carmen. 2021. "Is net neutrality legislation needed in South Africa?" TechCentral. https://techcentral.co.za/is-net-neutrality-legislation-needed-in-south-africa/170904/

- Degezelle, W. et al. 2022. "The Open Internet as cornerstone for digitalisation. The Global Gateway Partnership Opportunities between the European Union and Africa." Stantec. October 2022. https://fpi.ec.europa.eu/system/files/2022-10/The%20Open%20Internet%20as%20cornerstone%20of%20digitalisation%20DIGITAL.pdf

- The Economist. 2023. "The state of democracy in Africa and the Middle East: An EIU survey makes for glum reading. But there are some reasons for optimism" In the edition of 3 April 2023. https://www.economist.com/graphic-detail/2023/04/03/the-state-of-democracy-in-africa-and-the-middle-east

- Electoral Commission. 2023. "Electoral Commission partners with social media giants to combat disinformation in 2024 National and Provincial Elections" https://www.elections.org.za/pw/News-And-Media/News-List/News/News-Article/Electoral-Commission-partners-with-social-media-giants-to-combat-disinformation-in-2024-National-and-Provincial-Elections?a=AISDGvpz75ps1usOfX7oimHCQG6/AToNAzCQK374oSg=

- Electronic Communications Act 36 of 2005 https://www.gov.za/documents/electronic-communications-act (Accessed on 1 July 2023).

- Electronic Communications Amendment Act 1 of 2014 https://www.gov.za/documents/electronic-communications-amendment-act-0 (Accessed on 1 July 2023).

- Etike, E. "Nigeria, South Africa, and Kenya rank among top 100 for global online threats" https://technext24.com/2023/06/07/nigeria-south-africa-kenya-cyber-threats/ (Accessed on 4 July 2023).

- European Commission. 2021. "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank, The Global Gateway". https://ec.europa.eu/info/sites/default/files/joint_communication_global_gateway.pdf

- European Commission. 2022. "Shaping Europe's digital future: eGovernment and digital public services". https://digital-strategy.ec.europa.eu/en/policies/egovernment

- Films and Publications Amendment Regulation. 2022. https://www.gov.za/sites/default/files/gcis_document/202209/46839gon2432.pdf

- Gereda, S. 2006. «The Electronic Communications and Transactions Act,» in Thornton, Carrim, Mtshaulana and Reburn (eds.) Telecommunications Law in South Africa, Johannesburg, STE Publishers. http://thornton.co.za/resources/telelaw12.pdf. (Accessed on 10 July 2023)

- Gillwald A., Mothobi O., Rademan B. 2018. "The State of ICT in South Africa" Research ICT Africa. p.38. https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report_04.pdf

- International Trade Administration. 2023. "South Africa - Country Commercial Guide: Information Technology" May 2023. https://www.trade.gov/knowledge-product/south-africa-information-technology

- Kende M. & Abecassis D. 2019. "Impact of taxation on social media in Africa." Analysis Mason. https://www.analysysmason.com/consulting-redirect/reports/impact-of-taxation-on-social-media-africa-may2019/ (Accessed 12 April 2023).

- Knodel, Kumar, van Horenbeeck, Degezelle. 2022. "Mythbusting: cybercrime versus cybersecurity." IGF Best Practice Forum Cybersecurity. https://www.intgovforum.org/en/filedepot_download/56/24126

- Library of Congress. 2018. "South Africa: National Assembly Passes Copyright Amendment Bill, Adopts Expansive Fair Use Exception" https://www.loc.gov/item/global-legal-monitor/2018-12-21/south-africa-national-assembly-passes-copyright-amendment-bill-adopts-expansive-fair-use-exception/

- Malinga, S. 2021. "ConCourt RICA ruling will prevent abuse of Internet surveillance powers". ITWeb. 5 February 2021. https://www.itweb.co.za/content/xA9PO7NZj1e7o4J8

- McLeod, D. 2022. "Government shelves the Woan". Tech Central. https://techcentral.co.za/breaking-government-shelves-the-woan/208654/

- Mlaba. 2021. "How Is South Africa's Digital Divide Making Inequality Worse in the Country?" In Global Citizen, August 2021. https://www.globalcitizen.org/en/content/south-africa-digital-divide-makes-inequality-worse/

- Mle, T.R. & Ngumbela, X.G., 2020, 'Building a capable state through proper human resource management', Journal of Local Government Research and Innovation 1(0), a15. Accessed on 9 July 2023. https://www.parliament.gov.za/storage/app/media/Pages/2022/5-may/05-05-2022_Parliamentary_State_Capability_Conference/General_Resource_Documents/Building_a_capable_state_through_proper_human_resource_management.pdf

- Modise, E. 2023. "Mapping the growth trajectory of South Africa's data centre industry". Techcabal, 20 February 2023. https://techcabal.com/2023/02/20/south-africa-data-centre-industry/

- Mzekandaba. 2022. "Government abandons move to merge ICASA, FPB". ITWeb, August 2022. https://www.itweb.co.za/content/KA3WwqdzDDQ7rydZ (Accessed on 9 July 2023).

- "National Cybersecurity Policy Framework of 2015". https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf (Accessed on 5 July 2023).

- Noxolo Majavu And Palesa Dlamini. 2022. "Films and Publications Amendment Act leaves online content producers hot under the collar". News24. 5 March 2022. https://www.news24.com/citypress/news/films-and-publications-amendment-act-leaves-producers-hot-under-the-collar-20220305

- OECD. 2016. "Economic and Social Benefits of Internet Openness". https://one.oecd.org/document/DSTI/ICCP(2015)17/FINAL/En/pdf

- Omarjee, L. 2021. "World Bank ranks SA's Auditor-General as one of two in the world that has 'full independence'" News24. https://www.news24.com/fin24/economy/world-bank-ranks-sas-auditor-general-as-one-of-two-in-the-world-that-has-full-independence-20210805

- Oosthuizen,Morné. 2021. "South Africa : Social Assistance Programs and Systems Review (English)". Washington, D.C. : World Bank Group. http://documents.worldbank.org/curated/en/238611633430611402/South-Africa-Social-Assistance-Programs-and-Systems-Review

- Otter. 2009. "Broadband on agenda for new government" Published in My Broadband, April 2009. https://mybroadband.co.za/news/broadband/7732-broadband-on-agenda-for-new-government.html

- Parliamentary Monitoring Group. 2016." Cost to Communicate: public hearings, Telecommunications and Postal Services". September 2016. Day one: https://pmg.org.za/committee-meeting/23304/ and Day two: https://pmg.org.za/committee-meeting/23322/

- Patel (2023) "47% of South Africans rely on social grants - study reveals how they use them to generate more income" Published in The Conversation, May 2023. https://theconversation.com/47-of-south-africans-rely-on-social-grants-study-reveals-how-they-use-them-to-generate-more-income-203691

- Privacy International. 2019. "Africa: SIM Card Registration Only Increases Monitoring and Exclusion". https://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion

- Research ICT Africa. 2017. "State of ICT South Africa" report. https://researchictafrica.net/wp/wp-content/uploads/201robe8/10/after-access-south-africa-state-of-ict-2017-south-africa-report_04.pdf

- Roberts, T and Oloyede, R. 2022. "Why millions of Africans are right to resist mobile SIM card registration" Published by Thompson Reuters Foundation. https://news.trust.org/item/20220503084813-z74ni/ (Accessed on 9 July 2022).

- Skiti, S. 2023. "Justice department loses millions in yet another cyber attack" In TimesLive June 2023. https://www.timeslive.co.za/news/south-africa/2023-06-01-justice-department-loses-millions-in-yet-another-cyber-attack/

- Song. 2009. "South African National Broadband Forum". https://manypossibilities.net/2009/03/south-african-national-broadband-forum/ (Accessed on 6 July 2023

- South African Human Rights Commission. 2023. "Social Media Charter: SHINE - Social Harmony through National Effort". https://www.sahrc.org.za/home/21/files/SAHRC%20Social%20Media%20Charter%20FINAL.pdf

- Statistics South Africa. 2022. "60,6 million people in South Africa" 2022 Census results. https://www.statssa.gov.za/?p=15601 (Accessed on 3 July 2023)

- Thakur. 2021. "Advocacy release: AmaB wins battle against spying abuse as ConCourt declares bulk surveillance unlawful, Rica surveillance provisions unconstitutional". AmaBhungane, February 2021. https://amabhungane.org/advocacy/210202-release-amab-wins-battle-against-spying-abuse-as-concourt-declares-bulk-surveillance-unlawful-rica-surveillance-provisions-unconstitutional/

- TMO. 2023. "The changing face of e-commerce for South African retailers." https://themediaonline.co.za/2023/02/the-changing-face-of-e-commerce-for-south-african-retailers/

- Van Zyl, Gareth. 2016. "Exclusive: Tech experts quit govt broadband council" Published in News24 on 14 January 2016 https://www.news24.com/fin24/exclusive-tech-experts-quit-govt-broadband-council-20160114 (Accessed on 6 July 2023).

- Vermeulen.2023. "Information Regulator tests its teeth — slaps Department of Justice with R5 million fine". In My Broadband, 4 July 2023. https://mybroadband.co.za/news/security/498859-information-regulator-tests-its-teeth-slaps-department-of-justice-with-r5-million-fine.html

- Woodham S. & Migliano S. 2023. "Government Internet Shutdowns Have Cost $42 Billion Since 2019." TOPVPN. https://www.top10vpn.com/research/cost-of-internet-shutdowns/ (Accessed 12 April 2023).