ACKNOWLEDGEMENTS

This Discussion Paper forms part of a Southern African Development Community Parliamentary Forum (SADC PF) process of formulating a Digital Economy and Society Model Law. It focusses on the policy and governance considerations for the developing countries within SADC to enable the development of inclusive and sustainable digital economies and societies. Drafted by Research ICT Africa, the paper build on the points of mutual understanding in the SADC Parliamentary Forum-Research ICT Africa Memorandum of Understanding. The objective of such a Model Law on the Digital Economy and Society is to enable the countries to harness the benefits of the digital economy, while safeguarding the rights of citizens and mitigating possible risks associated with such developments.

The paper was authored by Gabriella Razzano with Alison Gillwald, Pablo Aguera, Shamira Ahmed, Enrico Calandro, Cecilia Matanga, Andrew Rens and Anri van der Spuy. It was further peer reviewed by Jonathan Klaaren, Lishan Adam and Hlengiwe Dube. We thank Torbjorn Fredriksson from UNCTAD for his comments. All interpretations, and any errors, however remain those of the authors.

The SADC Parliamentary Forum and Research ICT Africa are grateful to the Canadian International Development Research Centre (IDRC) who have made this research and collaboration possible.
BACKGROUND AND CONTEXT
Introduction

Digitisation on a global scale has been a defining characteristic of socio-economic development in the 21st century. Although the digital economy has been a point of policy reference since the turn of the millennium in reference to the emergence of e-commerce and e-government services, business to consumer (B2C), business to government (B2G), and business to business (B2B), it now describes the wider contemporary economy.

The global trends of digitalisation - and now ‘datafication’ - impact every aspect of social and economic activity. Established technologies that led to the development of the Internet in the latter part of the 20th century, and ultra-highspeed broadband networks at the turn of the century, have been augmented over the last decade by ‘free’ applications running ‘Over-The-Top’ (OTT) of such infrastructure (such as social networks), and the Internet of Things (IOT), which is able to remotely measure, monitor and record information. With the emergence of advanced technologies merging the physical and digital realms, artificial intelligence (AI) and machine-learning technologies enable the collection, use and analysis of vast amounts of digital data arising from personal, social and business online activities.

The digitalisation of production is structurally transforming the world economy. From a business perspective, the transformation of all sectors and markets through digitalisation can foster the production of higher quality goods and services at reduced costs through better coordination of efficiencies and optimisation across supply chains. These changes can be seen in primary areas of production including: the digitalisation and integration of supply chains, design, additive manufacturing, such as 3D printing, and customisation that reduces production times for the ‘mass customisation’ of products, and e-commerce, online search and social media platforms that have opened up new channels to consumers for larger corporations, but also smaller, more informal enterprises (Barnes, Black and Roberts 2019).

However, it has also created entirely new business models and modes of value creation involving ‘platformisation’ (UNCTAD, 2019). Platforms facilitate transactions and networking as well as information exchange. Importantly, these services (which can include cloud services) can lower costs by companies (and government) – whether software, security, or platforms themselves – because they need only pay for what that they use. Aspects of this globalised digital economy are sometimes referred to as the ‘platform’, ‘gig’ or ‘sharing’ economy, because of the reduction of costs through shared services, both in production and consumption (such as in Uber vehicles or Airbnb homes). The advanced technologies used to offer many of these services are based on large scale data collection and new forms of production such as AI, machine learning, advanced robotics, as sometime referred to as the ‘Fourth Industrial Revolution’ (4IR).

But these are all part of the fast-changing process of digitalisation and ‘datafication’ that characterise the contemporary global economy. Some of the developments have been incremental and some disruptive, but they have all been highly uneven. Today, information generation, processing and transmission, critically define who benefits from the transformative potential of digitalisation. Global platforms have been the major beneficiaries and creators of the new value created by these processes. Their dominance of markets through the control of data, as well as their capacity to create and capture value, have resulted in their concentration and consolidation in a very few countries and a handful of companies (UNCTAD 2019).

The hyper-globalised and uneven nature of these developments have implications for the United Nations (UN) 2030 Sustainable Development Goals (SDGs), a significant number of which are underpinned by global ICT targets that the region is way off meeting, giving rise to fundamental challenges for policymakers in countries at all levels of development. Whether countries and regions are able to create the conditions for the exploitation of these process of digitalisation and datafication to create added value, increase efficiency and productivity, create new jobs and maximise revenue generating trade and taxation, will depend on the policies adopted and implemented, as this is a common institutional challenge for developing countries. "Harnessing its potential for the many, and not just the few, requires creative thinking and policy
experimentation” (UNCTAD 2019:1). While it will present challenges at different levels of government, its globalised nature will nevertheless require greater global cooperation to overcome many of them.

These challenges highlight the need for policymakers in developing countries, while viewing digitalisation in the context of global markets and value chains, to closely consider the implications of their local contexts where the lack of digital readiness will constrain the ability to leverage these new technologies and processes productively. In order to compete in this global market, they will need to prioritise human development, particularly education, the development of advanced digital skills for digital production, access to finance for start-ups, investment in public access and digitalisation of public systems and institutional capacity to create a safe and trusted cyber realm. These will be required to mitigate the risks of rights violations, particularly privacy of private information, to employment and wider economic and social marginalisation.

The digital inclusion of developing countries and critical sectors within developing economies, increases their visibility in the wider value chain ecosystem. This reinforces the need to develop domestic and regional responses to global digital conversations and governance.

It is timely, therefore, that the SADC PF is preparing a Draft Model Law for the regional economic community. The net impact domestically will, however, depend on the level of development and digital readiness of countries and their stakeholders. It will also depend on the policies adopted and implemented at national, regional and international levels.

The next section of Part A locates these national digital economies in the wider global digital ecosystem and systems of global governance. It reflects on the current unevenness of digital development and the digital inequality paradox as one of the most pressing policy challenges of our time. The update on the implications of this in the context of CoVID-19 demonstrates the globalised nature of ‘public goods’ such as the Internet, and the unevenness of peoples’ ability to deploy it to mitigate the negative effects of lockdowns that Governments’ around the world have been forced to institute to contain the spread of the virus.

Part A will then consider the enablers and inhibitors of the digital economy in the context of the Southern African Development Community (SADC) before turning to a discussion of the digital economy more specifically and the emergence of the processes of digitalisation and datafication. Having addressed the socio-political, economic and technological background for the Digital Economy, Part B looks at the legal context and what is required for the domestication of a Digital Economy Law within the SADC. The broader objectives of the Digital Economy Model Law itself are realised through policy. Part C looks at the policy recommendations in three thematic areas:
In line with the international development agenda’s emphasis on digital technologies as enablers of development, ICTs have also been identified by the SADC as critical elements in building a more inclusive society, by eliminating poverty and reducing inequality in the country.¹

However, in this environment, the rules and policies that hope to facilitate development have to respond to a particular reality marked by interconnectedness and globalisation. An essential policy shift is required from a more traditional telecommunications perspective that views digital developments as occurring within the scope of a distinct sector, or even as a national issue, only. Rather, digitalisation occurs within a complex ecosystem that spans the entire economy and society at a national level, while also being inextricably connected to and interlinked with global markets and systems of governance.

In order to identify the necessary points of policy intervention in the complex and adaptive global information system as well as their implications due to the linkages between the different elements within this system, it is useful to conceptualise it as an ecosystem (Figure 1). Rather than focusing on the fast-changing technology, as do many technological determinist and futurist perspectives, it is appropriate for parliamentarians to adopt an approach that places citizens, users and consumers at the centre of the ecosystem. Viewing infrastructure from this perspective, it is not only a matter of availability but of the affordability of the networks, services and applications. Relevant content will also determine the degree to which people are drawn into the ecosystem highlighting, from a policy perspective, the need to weigh both supply and demand side constraints. Affordable access is an outcome of the market structure and the effectiveness of the regulation, which are themselves determined by the national policy and legal structure.

Figure 1: An ecosystemic view of the digital environment
Source: Adapted from Gillwald 2012

¹ See, for instance, recently, in September 2018 SADC Ministers of ICT deliberated that ICT are critical for the sustainable development of the region, and set specific objectives on broadband access, cybersecurity, rural connectivity, and the fourth industrial revolution. Media Statement available at https://www.sadc.int/files/3715/3806/1649/Media_Statement__ICT_Information_Transport_and_Me_.meeting.pdf
framework. Yet as we move to a more advanced digital economy on top of expanded ICT infrastructure, this user-centred approach will need to be balanced against consideration of production (and the consequent extraction risks) that this research considers further in its investigation on the broader inhibitors of the 'good' digital economy.

But the ability of citizens to deploy these technologies and digital services to enhance their livelihoods and wellbeing will be determined not only by affordable access or even their digital literacy to consume the service, but the education and skills to do so productively. Affordable access is an outcome of a policy environment that incentivises infrastructure extension and effective competition regulation of network operator and service providers. For the digital policy to spur employment and innovation, an integrated strategy for investment and human development, including general and specialised skills, entrepreneurialism, together with and enabling financial and trade system, is essential in order to enable innovation.

This requires an enabling state that can crowd-in productive private investments and coordinate public and private delivery of ‘public goods’ such as the Internet, cybersecurity and indeed, data. But outcomes at a national level are increasingly impacted by multi-lateral international governance institutions, such as the International Telecommunication Union (ITU), the World Trade Organisation (WTO), the UN's Commission on International Trade and Law as well as new forms of global governance such as the Internet Corporation for Assigned Names and Numbers (ICANN), a non-member state organisation, responsible for the governance of the Internet. Regional organisations such as the African Union (AU) and regional economic communities, such the SADC and specialist regional organisation such as the SADC PF and the Communications Regulators Association of Southern Africa (CRASA) have an increasingly importantly role in the harmonisation of policies and integration of markets in this globalised environment.

The institutional endowments of the country, including the design and capacity of the institutions, determine the nature and levels of investment as well as the effectiveness of competition regulation to enhance consumer welfare and create the conditions for innovation. Without governance systems able to adapt and deal with the increasing complexity of the digital ecosystem, digital technological development is likely to exacerbate inequality, rather than promote greater opportunity and shared prosperity.

With the scale at which current digital technologies operate, a lack of effective competition regulation (to correctly assess the relevant market in a complex digital ecosystem) is only likely to lead to increased market concentration (especially at the hands of a handful of companies from the Global North).

Considering growing levels of automation, complementary investments are needed in the skills that workers require to leverage technology. Without ensuring the accountability of information producers, brokers and governments responsible for public data, information will increasingly be under the control of and used for the benefit of commercial and political entities.

As ICT moves from being a sectoral issue to one that transects all industries and sectors, the public sector's digital readiness becomes a key determinant of service delivery in finance, health, education, transport, tourism and trade. Modernising the public sector and connecting public offices to cost-saving and more secure technologies will enable e-government to be a first step in meeting the needs of citizens more effectively.

National markets and the networks within them are also overlaid with new innovative global platforms, including cloud services, Big Data applications, DTT services and the IoT. These are creating new cross-border and local policy and governance challenges around cybersecurity, privacy and the safeguarding of other digital rights necessary to create a secure and trusted environment for users. This is a critical condition for uptake of digital services, e-commerce, e-government, online banking, platform work and a vibrant polity.

The extensive collection, storage and analysis of data feeding the algorithms underpinning AI, machine learning, robotics and drones increasingly calls for data governance. These and other technologies of the so-called 4IR (Reyes, Bacani, Horch, Rienstra & Walter, 2016) are entirely dependent on the functioning of the 'Third Industrial Revolution' of computerisation and automation, which is, in turn, intrinsically connected to contemporary forms of the 'Second Industrial Revolution' of energy technology. In fact, network- and data-intensive technologies such as these (especially blockchain) require significant amounts of power to operate, often costing more than the bandwidth they use. This means that stable and high-quality supply of energy is as critical in the digital ecosystem as communication infrastructure.
Data governance

In the era of digitalisation, data has assumed a significant role in socio-economic development, as it is considered a strategic and critical resource for data-driven economies – now referred to as ‘datafication’. But while the socio-economic benefits of big data analysis cannot be ignored, data governance frameworks for transparent and accountable processing of personal information (prior to aggregation) are necessary to safeguard the rights of access to information and privacy. This also has implications for other fundamental rights.

The increasing availability of digital data is driving a shift in policymaking worldwide from being data-informed to being data-driven (Taylor, 2017). On the other hand, the collection and processing of massive amounts of personal data has become an increasingly contentious issue, because the computing-analysis of this ‘big data’ allows researchers, private and public sector organisations alike to infer people’s movements, activities and behaviour, presenting ethical, political and practical implications for the way people are treated and seen (Taylor, 2017). However, these developments are also central activities within the emerging economic activities of all countries.

New technological developments such as AI, blockchain, cloud computing, drones, and the IoT produce, store and analyse an unprecedented amount of data, adding urgency to the need for policy options to regulate a data-driven environment. For instance, the use of AI and machine learning for behavioural profiling for tailored products and services is challenging the global principles on data protection related to the collection of data for specific purposes, minimality, and limitations on further processing. Cloud computing has quickly risen to prominence, disrupting traditional models related to data storage and distribution, having repercussions in various areas such as law, business and society.

The connection of devices to the Internet, and systems such as the IoT, AI, machine learning and other emerging technologies, have a direct implication in terms of data storing, processing and management, considering that data can be now be produced, stored and analysed by machines without human interventions.

A framework that facilitates making data available while respecting privacy rights, data integrity and availability, is central to building a trusted and secure digital environment and is a pre-condition for the adoption and absorption of emerging technologies in Africa. Although the concept of industry 4.0 is really pertinent to more industrialised economies and many of the technologies and processes identified in the graphic below are not evident in many SADC economies, the globalised nature of these industrial developments mean they impact on local economies directly and indirectly, requiring policymakers to consider a number of data-related aspects to enable a digital economy.

The emerging digital economy is fundamentally underpinned by data and analytics as a core capability. This necessarily means that considering the statutory and regulatory options for countries hoping to optimise the outcomes of development globally in their countries would involve data governance and justice considerations very strongly – all within an economic context that seeks to leverage ‘digital dividends’ and incorporate broader considerations of digitalisation. While data may be underpinning much of the digital economy, digitisation occurs across the value chain of activities for a business.

Digital inequality

The interconnections between different components of the ecosystem highlight the need for policymakers in developing countries to view digitalisation in the context of global markets’ value chains, but also in their local contexts where the lack of digital readiness will constrain their ability to leverage these new technologies and processes and to mitigate the risks related to employment, data governance and access to finance.

Fundamental to this is the importance of digital inclusion and equality. Paradoxically, as more people are connected, digital inequality is increasing. This is not only the case between those online and those offline (as is the case in a voice and basic text environment), but also between those who have the technical and financial resources to use the Internet optimally, and those who are ‘barely’ online. The latter includes those who only have partial access to poor-quality or expensive data services that do not permit them to be ‘always on’ or to use data-intensive services. The gap between those who passively consume a limited number of basic services and those able to put technology to full and productive use, with some even enhancing their prosperity, is widening.
Similarly, as more people who do not have the awareness or skills to exercise their rights come online, they are more vulnerable to the risks that accompany their use of new applications (apps) and services that collect personal information and use algorithms to target their advertising or to the ways in which governments can survey them, than those who have the knowledge or skills to mitigate such risks.

Rising shifts of income from labour to capital and a drop in mid-level jobs in many countries, commonly referred to as wage polarisation by economists, suggest that the gains from greater use of technology will not be equitably shared without significant policy interventions (Van Reenen, 2019).

This digital-inequality paradox, together with global governance to mitigate the risks of increased digitalisation and datafication, is arguably the biggest policy challenge for nations in an increasingly fractured global, digital economy and society.

COVID-19

The impact of COVID-19 on the digital economy both globally, and regionally, has highlighted the urgency for understanding the legislative and regulatory priorities of the digital economy. Globally, there have been surges in the amount of data created through expanded digitalised interaction, which includes work and social interactions (QTS, 2020).

The pandemic has led to state-sanctioned mass quarantines across the globe which, though of varying extremity, have resulted in rapid shifts in behaviour and practice referred to as the ‘new normal’. This ‘new normal’ is dominated by increased digital dependency. The necessity for reducing individual interaction to curb the spread of disease has also led to the disruption of business models and workflows, with a higher demand for digitalisation of work processes to facilitate this kind of ‘out of office’ work environment (QTS, 2020). And necessarily then, there have also been increases in the demand for data collection functions and storage, for businesses (QTS, 2020). However, the pandemic has also highlighted the vulnerability of gig and platform workers functioning outside domestic labour protections in the face of a contracting labour market.

Regionally, with the notable exception of South Africa, Africa has so far been spared the significant direct infection and death rates of the disease that other regions have suffered. However, the economic impacts have been increasingly severe, with the African Development Bank predicting that contracting economies resulting from COVID-19 will push between 28.2 million and 49.2 million more Africans into extreme poverty (AfricaNews, 2020). The emphasis on digital economic, political and social engagement brought by COVID-19, has highlighted the urgent need for expanding digital infrastructure across the region (Melhelm et al., 2020; Razzano, 2020).

The low level of digital beneficiation being experienced in Africa may be a challenge to economic resilience in the face of the pandemic, with decreased capacity across the continent to reap the benefits of expansion in the digital economy (Razzano, 2020). Existing digital inequalities in the region, which include the differential levels of access and use, mean that the inequality of negative impacts will be exacerbated across services like education, health care provision and labour (Ahmed, 2020). Vitally, the crisis has reinvigorated the call to deal with the challenge of digital taxation and the extraction of value in the face of contracting tax sources in the region (challenges around digital and e-taxation will be dealt with in more detail later) (AfricaNews, 2020).
3 Preconditions for the Take-off of the Digital Economy

Enablers of a digital economy

- **DIGITAL AND DATA AFFORDABILITY.** Economic regulation can enable the digital economy by improving competition at different levels of the supply-chain infrastructure of the Internet. Optimal market conditions to enable access to ICT are facilitated by increasing investment in infrastructure by the private sector and by reducing the cost to communicate. From a supply-side perspective, this can be achieved by:
  - undertaking the necessary market reviews on market dominance and anti-competitive practices, including their impact on prices;
  - ensuring service-based competition through access to wholesale networks;
  - relieving rollout bottlenecks that affect pricing, such as spectrum assignment; and
  - prioritising the roll-out of public Wi-Fi in all public buildings, especially in the rural areas to connect the unconnected (Mothobi, Chair & Rademan, 2017).

- **DIGITAL INFRASTRUCTURE AND REAL ACCESSIBILITY.** There is extensive evidence that while considerable progress has been made in terms of supply-side measures, demand side measures are the greatest challenge. While broadband network extension remains an issue in several countries, coverage is not the only factor determining connectivity and use of the Internet. In Lesotho, Rwanda and South Africa, to name but a few African countries, broadband coverage stands at over 98% and yet significant portions of the population remain unconnected (Gillwald & Mothobi, 2019). South Africa is the only country in sub-Saharan Africa, in 2018, to have an Internet penetration rate above 50% (Gillwald & Mothobi, 2018). The barriers to use for many people is therefore not that they are not covered by a signal, but that people do not have the resources to get online – the primary barrier being the cost of devices as well as the price of data. At the same time in Ghana and Nigeria, 43% and 40%, respectively, of those who do not use the Internet, also do not know what the Internet is (Gillwald & Mothobi, 2019). While human development in Africa remains a challenge more broadly in dealing with digital inequality, alternative strategies to extend affordable access to communications as practical, short-term interventions remain urgent. We simply cannot carry on doing things the way we have and expect the exponential changes we require (Gillwald & Mothobi, 2019).

- **DIGITAL DEVICES.** The After Access² surveys findings show that affordability of devices and lack of awareness are the main barriers to Internet use in the countries surveyed. Of those who do use the Internet in Mozambique, 76% indicated they cannot afford Internet enabled devices despite having amongst the lowest data prices on the continent, while in Tanzania this figure is not much less at 64%, in Uganda, half the population and in Rwanda just less than half. Of those who do use the Internet, 33% of South Africans stated that the price of data is unaffordable.

- **INNOVATION.** Creating a competitive regulatory environment to ensure positive consumer welfare outcomes should not be neglected and is also associated with fostering innovation. The African Innovation Policy Manifesto well articulates the environmental considerations for fostering the innovation environment of the digital economy as including education and research and development (R&D)(particularly increasing the participation of women or other vulnerable groups in education and skills development programmes; public multidisciplinary spaces; simplified business registration; innovation focused finance opportunities; local and pan-African markets; secure intellectual property rights; tax incentivisation; and digital infrastructure. Some countries have even sought to facilitate this component of the digital economy through the creation of “Start-up Laws”, such as Tunisia’s Start-up Act, 2018. As was noted:

---

² The After Access Surveys are nationally representative, demand-side surveys that generate comparable data across 16 developing countries in Asia, Latin America and Africa, on mobile phone and Internet access and use in the Global South. The African datasets are housed here: https://www.datafirst.uct.ac.za/dataportal/index.php/catalog/765/related_materials.
To capture the full growth potential of digital trade, there is a need for regulators and public infrastructure to cater for established businesses as much as for start-ups. Both require a solid legal framework (Lopes, 2019).

- **DIGITAL SKILLS AND EMPLOYMENT.** Beyond the skills necessary to ensure the benefit of digital dividends from the user side addressed early, there is also the need to develop sufficient digital skills from the labour supply side (Barnes et al., 2019; Mothobi et al., 2018). Digital skills development should directly incorporate the digital technologies and products that will eventually be produced by domestic workforces (ITWeb, 2020). This will mean making necessary adjustments to both educational programmes, as well as skills development programmes, domestically.

- **E-GOVERNMENT AND E-SERVICES.** This raises an additional enabler: and that is the ability of e-government services to both serve business, but also support citizens and the broader ambitions of the 2030 Agenda for Sustainable Development. This would include e-government services that are interoperable and accessible in a digital economy context (AU-EU Digital Economy Task Force, 2019). While by no means exhaustive, enablers such as those addressed should be considered when generating legislative options.

### Inhibitors of a digital economy

- **DIGITAL INEQUALITY.** Digital inequality in ICT access is a key inhibitor in preventing a ‘good’ digital economy. Digital inequality is evident in a number of contexts. Those related to inequitable access and use (consumptive and productive) have been highlighted above and are discussed further in relation to the SADC below.

- **EXPLOITATION OF LABOUR.** The growth in the gig economy comes with the risk of exploitation of workers through lack of labour regulation and regularity of employment. This precarity also needs to be understood within the context of an ensuing “youth bulge”: Africa’s youth population is expected to double to over 830 million by 2050, but the potential benefits of Africa’s youth population are challenged by the reality that two thirds of non-student youth are “unemployed, discouraged, or marginally employed” (African Development Bank, 2016). Any ability to absorb more youth within the economy is threatened by the regional reality that while only three million formal jobs are created annually, 10-12 million youth attempts to enter the workforce (African Development Bank, 2016). While digital commerce and other dividends of the digital economy may present opportunities for youth employment in Africa, it is unclear what role labour regulation may have in facilitating these opportunities (UNECA, 2019). Solutions may also be generated by cost savings borne of digitisation itself, if these savings are reinvested into “… job-creating activities, building the absorptive capacity of the workforce and promoting better domestic linkages between firms and sectors” (UNECA, 2019).

- **EXTRACTIVE NATURE OF THE DATA-CENTRED DIGITAL ECONOMY.** It has been claimed that data from the global South is being “computationally appropriated and siphoned” to power technologies from outside of the continent, with little safeguarding or economic exchange (Gwagwa & Koene, 2018). The realities that underscore data flows and extraction have often raised questions about the potential for data localisation, though the reality of such options in globalised contexts is highly problematic (Hicks, 2019). This tendency towards ‘extraction’ is facilitated by the nature of the economic value of data, which create tendencies toward concentration. The ‘non-rivalrous’ and ‘non-exclusive’ nature of data predisposes it toward scaled collection and protectionism (United Nations, 2018). This extraction is not only of data itself, but also – given the nature of value chains – of profits.

- **DOMESTIC TAXATION.** The centrality of this issue is evident in a document released by the Organisation for Economic Co-operation and Development (OECD) which seeks to generate a ‘Unified Approach’ to taxation that reallocates taxing rights in favour of the user/market jurisdiction by targeting digital businesses (OECD, 2019).

---

3 The gig economy refers to a labour market characterised by freelance, flexible, on-demand work facilitated by digital technologies.
• **PUBLIC MONOPOLISATION.** State monopoly of infrastructure may have a real impact on communication infrastructure. This was recognised in the Zimbabwean case of Retrofit (Private Limited) (1998). In this case, the state refused a license to a company to operate a mobile cellular telephone service. The Supreme Court ruled that such a refusal violated the applicant’s freedom of expression, but was also an indication of how state monopolies on infrastructure can affect citizens’ rights to communicate. Questions of monopolisation should bring to mind competition laws and authorities within domestic contexts particularly as, within SADC countries, several countries do not have competition legislation (Baker McKenzie, 2019).

• **PRIVATE OLIGOPOLIES.** Many of the broader inhibitors of the digital economy for domestic benefit are associated with private sector oligopolies. The digital economy is dominated across digital services by a handful of American firms (Google, Amazon, Facebook, Apple, Microsoft – GAFAM) and Chinese firms (Baidu, retail Alibaba, platform Tencent and Xiaomi – BATX) (Thieulin, 2019). It is this massive dominance of the digital market that is resulting in the digital colonialism cited by many authors (and results in the extraction of data and value already identified as significant inhibitors to digital economic progress). Importantly, it has been noted that this dominance is not just an inhibitor to outcomes to the digital economy, but notably to the capacity of domestic environments to intervene legislatively and regulatorily (Thieulin, 2019).

**Implications for domestic policy**

When we consider both the digital environment, but also the peculiarities of the digital economy and its needs, it implies that within a framework of global governance a national strategy is required for developing countries to create an enabling and equitable digital economy for social inclusion and economic prosperity, and to create the safe, secure and trusted environment required for the digital economy to flourish. This will require a transversal national strategy to create an enabling and equitable digital economy for social inclusion and economic prosperity; to prevent harms associated with the permanent surveillance of data subjects by global monopoly platforms and by the state and to safeguard the rights of citizens, to create the safe, secure and trusted environment required for the digital economy to flourish. To achieve this, policies will need to derive from participatory multistakeholder processes in which civil society and the private sector engage with Government. Such national policies will require coordination between the public and private sector to meet national demand and to be able to compete effectively in the global economy. This will require:

- the crowding in of productive private investment for improvements in physical infrastructure (including power and broadband);
- effective economic regulation of infrastructure providers to ensure fair competition policy and regulatory experimentation to enable the delivery of lower cost broadband services;
- integrated institutional arrangements to deal with the complex, adaptive global information system, including infrastructure, content, data and new competition issues the governance of which require national and global responses;
- policies to open both public and commercial data as a critical asset for new entrants and data flows to enable cross border trade and to combat first-move advantage accumulations of data, while protecting the private information of individuals and the security and integrity of national systems;
- changes to basic education curricula that move from rote learning and thinking that can easily be replicated by machines to critical and creative knowledge-building better suited to the dynamic digital environment, together with large scale crosscutting digital skills programmes to align and scale with new labour force requirements;
- financing mechanisms to extend access to these new means of production for supply chain integration, regional trade and global competitiveness and harmonise regional frameworks to enhance trade and enable cross border data flows; and
- removal of excessive corporate taxation inhibiting network investment and regressive social network taxation dampening usage by the poor as well as engaging with global digital taxation regime reform seeking the taxation of digital products and services in the jurisdiction in which revenues are generated, even if the producer does not have a physical presence in it.

It is not possible within this Discussion Paper to deal with all the policy issues related to this enabling environment at length. Below, the paper focuses on the policy and governance considerations for developing countries to harness the benefits of greater efficiency, improved productivity and value creation associated with the digital and data-driven economy. While highlighting the need to redress digital inequality as a precondition for inclusion in the digital economy, it explores the governance frameworks necessary to enable the digital evolution of the economy.
While there are general environmental factors worth noting in discussions on legislating for a ‘good’ digital economy, the SADC region presents very specific contextual features worth considering.

**User and demand side factors**

As flagged above, low levels of Internet penetration persist amongst SADC countries with a sub-regional average of only 26% (with a range of between 4.7% and 56.5%), and both demand and supply side challenges (Mothobi, Chair & Rademan, 2017). The first point of access to the Internet by most Internet users is through mobile phones (more than 80% of individual users) (Mothobi, Chair & Rademan, 2017), and this reliance on mobile access means that costs of Internet-enabled devices have an important impact on accessibility more broadly. Affordability is cited as a key barrier to Internet uptake in the region, with other user issues such as a lack of digital literacy and a lack of relevant content, impacting uptake and experience (Chair, 2017).

A number of SADC countries are below the 20% critical mass believed to be necessary to enjoy the network effects associated with improved efficiencies and enhanced information flows for economic growth and innovation (Gillwald & Mothobi, 2018).

The experience of Internet access for users in the SADC is marked by inequality. The SADC Declaration on Information and Communication Technologies (2001) invokes member states to prioritise rural and remote areas, underprivileged urban areas, institutions of learning and other communities of special benefit, as a way of bridging the digital divide—yet there remains a notable urban-rural divide. User survey data for Tanzania, Lesotho and South Africa, demonstrated that there are significant differences in access between rural and urban communities (Gillwald & Mothobi, 2019). Infrastructure presents a particular challenge for rural users, as rural areas ordinarily only have a single operator available, with poor service and uncompetitive pricing, consequently being experienced (Chair, 2017). Further, gender and inequality of access was also revealed within the SADC data results:

![Percentage of individuals using the Internet in SADC countries](source: RIA 2018 After Access Survey and ZICTA Household Survey 2018 for Zambia.)
Figure 3: Internet use in 5 African countries Lesotho, Mozambique, Tanzania, South Africa and Zambia (2017)

<table>
<thead>
<tr>
<th>Country</th>
<th>Male</th>
<th>Female</th>
<th>Urban</th>
<th>Rural</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lesotho</td>
<td>32%</td>
<td>36%</td>
<td>31%</td>
<td>54%</td>
</tr>
<tr>
<td>Mozambique</td>
<td>10%</td>
<td>13%</td>
<td>7%</td>
<td>23%</td>
</tr>
<tr>
<td>Tanzania</td>
<td>14%</td>
<td>16%</td>
<td>11%</td>
<td>32%</td>
</tr>
<tr>
<td>South Africa</td>
<td>53%</td>
<td>57%</td>
<td>50%</td>
<td>61%</td>
</tr>
<tr>
<td>Zambia</td>
<td>14%</td>
<td>17%</td>
<td>12%</td>
<td>5%</td>
</tr>
</tbody>
</table>

Source: RIA, After Access surveys, (ZICTA, 2018)

Supply-side factors

Competition and regulatory authorities are often concerned about the lack of competition and high prices in the mobile market. This is mainly due to the market being assumed to be oligopolist in nature, with few players able to enter the market. Due to high off-net charges, consumer loyalty and high costs of switching networks, the SADC telecommunication market has largely been dominated by two players, which in most cases are the first entrants. For instance, in South Africa, more than 75% of market share is controlled by two dominant operators, MTN and Vodacom. Cell C and Telkom Mobile have not been able to sustain much more than 15% and 10% of the market, respectively, as late entrants. The duopoly market in Lesotho consists of Econet (23%) and Vodacom (77%), while in Swaziland there is a monopoly operator, MTN.

The entry of OTT services was seen as a strategy through which smaller operators would be able to overcome competition challenges related to high off-net charges and high switching costs and pose a

Figure 4: 1GB Data prices in SADC countries

Source: RAMP, Q3 2019

---

4 Off-net charges are, generally, higher charges levied for calls between one network provider to another network provider. On-net charges are, generally, lower charges for consumers if they contain their calls to the same network.
competition threat to first entrants. However, in some cases, like South Africa, the smaller operators were the first to embrace OTT services to garner high market shares. Once the dominant operators all began offering these free services, smaller operators lost their competitive edge. Mobile broadband tends to follow the same pattern as voice and text messages. Dominant operators that control a larger share of industry revenue leverage their revenue strength to outcompete smaller players. For instance, despite Cell C being the first to embrace OTT services and Telkom providing the cheapest data services, the two smaller operators have been unable to compete on coverage and quality to build market share to generate the revenue required to invest in the deployment and upgrading of their network infrastructure. This has affected the quality of services provided by smaller operators and in the process also losing the competition battle.

**Figure 5:** Evolution of 1GB data prices (in USD) in SADC countries (Botswana, Lesotho, Namibia, South Africa, Swaziland, Zambia, Zimbabwe).

*Source: RAMP, Q3 2019*

**Figure 6:** Evolution of 1GB data prices (in USD) in SADC countries (DRC, Madagascar, Malawi, Mauritius, Mozambique, Tanzania, Angola).

*Source: RAMP, Q3 2019*
The lack of competition in the mobile broadband has led to calls for regulators to examine pricing of broadband services in a number of SADC countries. For instance, following persistent concerns expressed by the public and stakeholders, the Competition Commission of South Africa initiated a Data Service Market Inquiry in 2017 and the preliminary findings released in 2019 concludes that mobile prepaid broadband services are generally high in South Africa, with some competitive issues found in the wholesale market.

The high cost of data has also been an issue in Zambia, with the Zambian Parliament adopting a motion to ban Internet service providers from providing data services that have an expiry date. In 2017, the Botswana Communication Regulatory Authority directed all mobile operators to reduce data prices and cut off-net charges by 41%. Compared to other African countries, SADC countries especially, Botswana, Namibia, Swaziland, Zimbabwe have the most expensive data packages in Africa (see Figure 3). The high data cost in the SADC region is attributed to inefficient regulatory policies, lack of competition in both retail and wholesale markets, market entry problems and delays in the release of high frequency spectrum.

Mozambique with a 1GB data priced at USD 1.97 and Zambia at USD 2.70 are the only SADC countries that offer data packages that are comparable to some of the cheapest countries in Africa, such as Egypt (USD 1.21) in Q3 2019. Low data prices in Zambia are attributed to fierce competition among players in anticipation of the entry of the new player (Uzi), which was expected to launch in 2019. This has resulted in more than a 70% decline in data prices between Q2 2017 and Q1 2019. Despite increased concern over expensive data packages, most SADC countries have remained stagnant. Swaziland and Zimbabwe offer the most expensive 1GB data in these countries is 20 times more expensive than Egypt and almost 10 times more expensive than Mozambique, Tanzania and Zambia - making it even cheaper for residents of these countries to roam on networks of neighbouring countries' operators.

Driving prices down can have implications for investment both on coverage and quality. With some of the countries with the lowest prices all suffering from limited broadband coverage and poor quality of services.

Outside of mobile data, broadband, spectrum and digital migration also potentially have an impact on digital economy initiatives. Secondary spectrum use, such as TV white space, through to dynamic allocation of unused spectrum in rural areas, could provide access at a fraction of the cost of current GSM data services. Unused GSM spectrum assigned to operators at the national level, which is unused in many rural areas, could be reassigned for community self-provision (Chair, 2017).

**Economic factors**

The SADC regional economy has a strong bias towards services and agriculture as the largest contributing sectors to GDP, sectors in which innovative digital applications and platforms can be adopted with relative ease in the right policy conditions (Abrahams, 2017). The beneficial aspects of digitalisation for manufacturing, in particular, are worthwhile highlighting when considering the role of the ‘digital’ for the region from a production perspective (Banga & te Velde, 2018). In considering this opportunity within manufacturing, the threats of the high cost of capital (inclusive of labour) compared to other regions, as well as challenges in financing for capital, are noteworthy (Banga & te Velde, 2018). Yet again, however, it is questions of ensuring the necessary skills are in place that would allow countries to receive the dividends of digitalisation (Banga & te Velde, 2018) that support this research’s early priority calls for domestic policy.

The SADC region registered an estimated average growth rate of only 1.8% in 2018 compared to 2.1% in 2017. Overall growth has been increasing at a lower rate since the global financial crisis in 2009 (SADC, 2018). The Manufacturing sector, identified for growth in the SADC, grew by 4.3% in 2018 compared to 4.6% in 2017 (SADC, 2018).

In the economic context, the Gini coefficient also plays an important role. Some of the countries with the world’s highest inequality measures are based within the SADC region – with South Africa, in particular, being noteworthy for regional economic stability given the size of its economy. This income inequality creates the conditions for the lived inequality of citizens within a country across a number of different markers.

According to the World Bank Findex survey conducted in 2017, financial inclusion was found to have increased from 23% to 43% in Sub-Saharan African countries from 2014 (Demirgüç-Kunt, Klapper, Singer, Ansar & Hess, 2018). The After-Access survey findings seem to confirm that mobile money services have contributed to a growth in financial inclusion. The study finds that five out of ten (46%) people in the
surveyed countries have access to financial services either through a mobile money platform or a banking account, though this includes results from outside the SADC (Mothobi et al., 2020).

Nevertheless, digital beneficiation is still low in Africa. Despite a number of initiatives to enhance digital opportunities such as the creation of online jobs, e-commerce and digital financial instruments, few Africans participate actively in the digital economy. The After Access survey shows that only a small proportion of economically active individuals in Kenya, Ghana and Tanzania are online; but Mozambique and South Africa have the largest percentage of micro workers among economically active populations, at 8% and 7%. The low levels of micro workers (as a demonstration of participants within a component of the digital economy) in Africa are attributed to low Internet penetration. Only three countries (Lesotho, Senegal and South Africa) have reached Internet penetration rates of 30%.

Emerging technologies (and economies) naturally present new opportunities for taxation. But these taxation opportunities must bear in mind the income and digital exclusion considerations addressed so far. So, for instance, the imposition of digital taxes on popular DT services like Voice Over Internet Protocol (VoIP), social media sites and instant messaging, or additional levies on mobile money transactions, will have a disproportionate impact on low-income users in a region that still has the lowest rate of Internet penetration in the world (Munya, 2019). Affordability remains one of the most significant obstacles to universal access and sector-specific taxes like these pose a huge threat to Internet access, affordability and financial inclusion.

Figure 7: Map of Gini coefficient results as of December 2016 (United Nations Development Programme, 2017)
Regulatory factors

Naturally, given the significant role of the private sector within the Internet and digital economy space, regulation plays a significant role within the environment. The ITU measures the forms of regulation of telecommunications in different countries along a four-scale measure:

- Generation 1: Regulated public monopolies, command & control approach;
- Generation 2: Opening markets, partial liberalization and privatization across the layers;
- Generation 3: Enabling investment, innovation and access; dual focus on stimulating competition in service and content delivery, and consumer protection; and
- Generation 4: Integrated regulation, led by economic and social policy goals.

**Figure 8:** ITU Regulation Measures for the SADC region

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>GENERATION</th>
<th>SCORE</th>
<th>COUNTRY</th>
<th>GENERATION</th>
<th>SCORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Angola</td>
<td>2nd</td>
<td>64.67</td>
<td>Mozambique</td>
<td>2nd</td>
<td>57.67</td>
</tr>
<tr>
<td>Botswana</td>
<td>4th</td>
<td>85.0</td>
<td>Namibia</td>
<td>3rd</td>
<td>70.67</td>
</tr>
<tr>
<td>Comoros</td>
<td>3rd</td>
<td>82.33</td>
<td>Seychelles</td>
<td>2nd</td>
<td>62.00</td>
</tr>
<tr>
<td>Democratic Republic of Congo</td>
<td>3rd</td>
<td>79.33</td>
<td>South Africa</td>
<td>3rd</td>
<td>71.33</td>
</tr>
<tr>
<td>Lesotho</td>
<td>2nd</td>
<td>67.83</td>
<td>Swaziland (Eswatini)</td>
<td>2nd</td>
<td>59.33</td>
</tr>
<tr>
<td>Madagascar</td>
<td>2nd</td>
<td>69.50</td>
<td>Tanzania (United Republic of)</td>
<td>4th</td>
<td>85.00</td>
</tr>
<tr>
<td>Malawi</td>
<td>4th</td>
<td>87.00</td>
<td>Zambia</td>
<td>3rd</td>
<td>71.87</td>
</tr>
<tr>
<td>Mauritius</td>
<td>3rd</td>
<td>80.83</td>
<td>Zimbabwe</td>
<td>3rd</td>
<td>74.00</td>
</tr>
</tbody>
</table>

Source: ITU (2018) ICT Regulation Measures for the SADC Region

Analysis of the SADC environment has indicated how effective the establishment of regulatory bodies is, as a central way to coordinate the public and private sectors towards a common vision on ICT infrastructure and access provision (Markowitz, 2019). Sound regulating is a key step for ensuring universality of access and service in the SADC region (Abrahams, 2017).

Regulation has regional functions atop domestic functions. In an acknowledgement of the need to coordinate regulation and regulators across the region, the Communications Regulators’ Association of Southern Africa has been established with the goal of preparing and finalising country-level regulations based on model laws or guidelines for regulatory harmonisation (Abraham, 2017). CRASA has played an important role in SADC technical capacitation on ICT policy for policymakers in recent years, which is a vital function for regional coordination entities (Markowitz, 2019). Hence, at regional level it is hoped that this kind of intervention can help ensure broader inter-agency collaboration. Particularly within the context of digital complexity, intra-regional coordination improves harmonisation in regulatory measure, but also improves the ability for cross-collaborative jurisdiction on digital challenges (Abrahams, 2017).
Within the context of the digital ecosystem this section now looks more closely at the digital economy, and the processes of digitalisation and ‘datafication’ that underpin it. Narrower definitions of the digital economy describe it as:

That part of economic output derived solely or primarily from digital technologies with a business model based on digital goods or services (Economic and Social Research Council of the United Kingdom quoted in Bukht & Heeks, 2017).

However, it is more useful to think of the emerging digital economy more broadly as the contemporary global economy, with the analogue aspects of the ‘old’ economy and physical labour being facilitated by online sourcing, use or delivery, together with purely digital products and services, online work and production. Yet this emerging global digital economy is arising within an unequal context, in which undeveloped economies are still struggling to implement, and benefit from aspects of both the third and fourth industrial revolutions.

The digital economy presents some clear opportunities. In Africa the contribution of the Internet to GDP growth currently remains low, but as problematic as various forecasts are, suggestions are that emerging economies in particular may see amplified benefit moving forward with the Internet eventually adding significant value to Africa’s GDP (Manyika, J et al., 2013). Digital benefits are seen as being derived through three main mechanisms that are attributable to the digital economy: inclusion, efficiency and innovation (World Bank, 2016). These mechanisms can then result in digital dividends for African economies:

For businesses, the Internet promotes inclusion of firms in the world economy by expanding trade, raising the productivity of capital, and intensifying competition in the marketplace, which in turn induces innovation. It brings opportunities to households by creating jobs, leverages human capital, and produces consumer surplus. It enables citizens to access public services, strengthens government capability, and serves as a platform for citizens to tackle collective action problems. These benefits are neither automatic nor assured, but in numerous instances digital technologies can bring significant gains (World Bank, 2016).

Businesses that generate from within a digital economy, which include start-ups and innovation companies, have the potential to be ‘high-growth firms’ with the capacity to generate output and create jobs (Goswami et al, 2019).

Digitised information is increasingly integrated with automation and used to assist decision-making. Digitalisation refers to a different and more advanced phenomenon than digitisation. Although the concepts of digitisation and digitalisation are used interchangeably in much of the literature, it is conceptually useful to distinguish between the two. Digitisation refers to encoding analogue information digitally so that it can be stored, processed, and transmitted by computers (Bloomberg, 2019). Digitalisation refers to a deeper and more transformative process sometimes also captured by the term “digital transformation”. Gartner defines digitalisation very narrowly within a business frame as “the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business” (Gartner, n.d.). A more encompassing definition is offered by Gray and Rumpe, (2015, p. 1319) who define it as “the integration of multiple technologies into all aspects of daily life that can be digitized”. It has also been defined as, “the way in which many domains of social [and economic] life are restructured around digital communication and media infrastructures” (Bloomberg, 2019).
Yet even digitalisation within the ‘traditional’ economy could reap benefits for countries, for instance in manufacturing (Banga & te Velde, 2018). But many of the pre-existing policy challenges impact beneficence even from this stage of digital transformation – for instance, inadequate access to skills, and comparatively expensive capital costs (within a challenging financing environment).

So, what is the scope of the digital economy? In the table below, the breadth of the digital economy is demonstrated across several economic dimensions (e.g. productivity, value added, employment, income and trade), for different actors (workers, micro, small and medium-sized enterprises MSMEs), platforms and governments, and for different components of the digital economy (core, narrow and broad in scope).

The core or digital sector refers to the established telecommunications and ICT sector that has produced positive outcomes for different actors, and contributed to improved growth, productivity and value add. While creating new jobs in areas such as mobile communications, technology induced efficiency gains have also resulted in job losses in more traditional infrastructure companies.

With the advent of the digital economy and the shift from sectoral development underpinning simple online source and delivery of offline goods that characterise e-commerce, new jobs arise in digital services and products. There is additional potential in micro-work or platform work by a dispersed work force, working flexibly, and paid for pieces of work that contribute to global value chains. Although there is evidence of high growth, productivity and value add, trade outcomes remain mixed and market concentration increases with negative competition consequences.

Once the economy is digitalised there is a need for higher value skills to design and implement new platform-based business models, including automation, visualisation and augmented reality, with consequent job losses in more traditional areas of work. Platform enabled businesses increase productivity, but there is also a race to the bottom with reduced transaction costs and unregulated labour costs. While new opportunities emerge for smaller, informal enterprises, there is an extreme concentration of market power and control of the data value chain by a handful of global platforms in limited geographic locations – the United States and China.

Although productivity improvements and innovation increase exponentially in the fully digitalised economy, there is no contribution by global giants to local tax bases for states to mitigate the effects of these developments. With the crowding out of local firms, these developments are potentially disruptive and structurally impact on the global economy. Safeguarding citizens’ rights by preventing these harms and introducing measures to mitigate associated risks, will require global cooperation, as will a global digital tax regime to ensure that revenues can be taxed in the jurisdiction in which the revenues are generated.
## Figure 9: Potential impacts on value creation and capture from an expanding digital economy, by its component and actors.

<table>
<thead>
<tr>
<th>Digital Economy Component</th>
<th>Individuals (as Users / Consumers and Workers)</th>
<th>MSMES</th>
<th>Multinational Enterprises / Digital Platforms</th>
<th>Governments</th>
<th>Economy-Wide Implications</th>
</tr>
</thead>
</table>
| **Core, Digital Sector**  | • New jobs for building and installing ICT infrastructure.  
   • New jobs in telecom and ICT sector, especially ICT services.  
   • Greater inclusion under suitable circumstances or spillovers/domestic linkages.  
   • Increased competition from cloud-service providers. | • Investment opportunities for companies that meet high capital, technological and skills requirements.  
   • Attracting investment.  
   • Tax revenues from the economic activity created. | • Increased growth, productivity and value added.  
   • Employment creation.  
   • Investment and diffusion of technologies; R&D likely located in high-income countries.  
   • Mixed trade impacts. |
| **Digital Economy**       | • New jobs in digital services, especially for highly skilled people.  
   • New forms of digital work, including for the less skilled.  
   • New opportunities in digital ecosystems.  
   • Increased productivity from data-driven business models.  
   • Greater control of value chains using platform-based business models.  
   • New opportunities in the sharing economy. | • Enhanced productivity from data-driven business models.  
   • More tax revenue resulting from increased economic activity and formalization of enterprises.  
   • Lost customs revenue from digitalization of products.a  
   • Increased growth, productivity and value added.  
   • Employment creation/losses.  
   • Higher investment.  
   • Aggregation of digital firms in some locations.  
   • Mixed trade impacts.  
   • Market concentration. |
| **Digitalized Economy**   | • New jobs in ICT occupations across industries.  
   • Need for new skills as higher-value roles are redesigned using digital tools.  
   • Greater efficiency of services received.  
   • Job losses or transformation due to digitalization.  
   • Risk of worsened working conditions.  
   • More choice, convenience, customization of products for users and consumers.  
   • Lower consumer prices.  
   • Platform-enabled market access.  
   • Reduced transaction costs.  
   • Risk of “race to the bottom” in markets vs. ability to find a niche.  
   • Lost opportunities due to automation (e.g., logistics, business processes).  
   • New roles in service provision.  
   • New business opportunities for digitalized enterprises. | • Emergence of platform firms with data-driven models.  
   • Gains from efficiency, productivity and quality.  
   • Opportunities for the monetization of data.  
   • Increased competitive advantage to digital platforms.  
   • Increased market power and control of data value chain.  
   • Leading digitalization in different sectors.  
   • Increased efficiency of services through e-government.  
   • Increased revenue from customs automation.  
   • Unclear impact on tax revenue: increases from higher economic activity; losses from tax optimization practices by digital platforms and MNEs.  
   • Data-driven opportunities to meet various SDGs.  
   • Growth through improved efficiency in sectors and value chains.  
   • Productivity improvements.  
   • Innovation impacts.  
   • Potential crowding out of local firms in digitally disrupted sectors.  
   • Potential automation in low- and medium-skill jobs.  
   • Wider inequality.  
   • Mixed trade impacts.  
   • Impacts on structural change. |

Source: UNCTAD 2019, Digital Economy Report 2019
LEGAL CONTEXT
Having addressed the socio-political, economic and technological background for the Digital Economy, it becomes clear that the domestication of a Digital Economy Law would need to be constrained by certain essential domestic elements, whilst still pursuing the broader objectives required of the Digital Economy Model Law itself (which will be realised through the thematic policy recommendations outlined later). This approach is significantly informed by the understanding of the digital ecosystem (and its attendant complexity).

As can be seen in Figure 10, domestic laws and regulations as well as bilateral and multilateral agreements (and instruments), will provide foundations and constraints to a Digital Economy Law. For the Law to eventually achieve the objectives it seeks to achieve, the environmental preconditions – which include infrastructure and Internet access - should be in place, and the Law should be developed through public participation processes. In addition, the requisite policy environment will need to support and foster the enabling factors for the digital economy, such as sound innovation investment and skills development (reference here should be made to the digital economy enablers and inhibitors detailed earlier).

The Framework can be implemented in-country as a tool that facilitates an environmental scan prior to the domestication of the Model Law.

---

**Figure 10:** Diagram providing framework for development of a Model Law on Digital Economy

Source: Author’s own
Jurisdiction challenges and governance

A central concern with any attempt to legislate and regulate the digital environment is the manner in which jurisdictions are rendered practically superfluous. How can laws intervene where a border is not a reality? These challenges are borne of the nature of the Internet itself and also the nature of data flows, but also due to the extended remit of multinational and trans-national corporations and the mobility of persons with the growth of globalisation. Legal rules, in contrast, have been very formally applied within jurisdictions of physical reference (Razzano, 2016). International discussions on digital governance have directly raised the challenge of jurisdiction, with the a key report noting how such challenges limit the form of legal responses available (Internet & Jurisdiction Policy Network, 2019).

There are challenges in enforcing legal obligations across borders, which is why regional harmonisation and coordination is such an important priority for helping construct a feasible environment for the digital economy in the SADC. Governance challenges that arise from jurisdiction are a key foundation for the SADC’s collaborative objectives – and one response to the challenge of jurisdiction, in particular, is to try and facilitate a level of harmonisation in regional legal instruments that are adopted. These jurisdictional challenges, in fact, lend support to Model Law development – not only for assisting in harmonisation between jurisdictions, but also for prioritising domestic responses that can incorporate contextual specifics within the globalising environment. And at the same time, it helps provide the idea of ‘balance’ that is required when considering how much domestic legislation may influence these dynamics.

Human rights and justiciability

Where harmonisation is an objective, the question of shared norms and values naturally arises. Human rights give a frame for enforcing normative values, but also for deriving a degree of harmonisation across borders. The SADC Treaty notes how the pursuit of establishing common economic, political and social values and systems (whilst enhancing enterprise and competitiveness, democracy and good governance, respect for the rule of law and the guarantee of human rights, popular participation and the alleviation of poverty) underpin the establishment of the SADC itself (SADC, 1992).

Human rights values form an important frame for contextualising norms within the SADC digital economy, as they can help ensure that new opportunities for growth resulting from trade, including digital trade, do not detract from human development, by allowing for the incorporation of social and political objectives within the economic policy area - consistent with the ambitions of the 2030 Agenda for Sustainable Development.

In the face of economic policy questions, the ability to bring human-centred concerns to be adjudicated on is particularly important for attempting to protect citizens from unfair treatment. Human rights oblige not just protection, but promotion as well – helping to ensure economic regulation in the digital realm places human concerns centrally. The spectrum of this justiciability has expanded over time. In the case of Social and Economic Rights Action Centre & Another v Nigeria (2001) AHRLR 60 (ACHPR 2001) (Ogoni case), the African Commission on Human and People’s Rights held that it would “apply any of the diverse rights contained in the [African] Charter” and welcomed the “opportunity to make clear that there is no right in the Charter that cannot be made effective”. This is a relatively radical approach, as it sees all rights across the civil, political, social and economic spectrum as equally enforceable. This is an important development in the African context, given how strongly our regional human rights discourse has driven understandings of communal human rights ideas. And the African human rights regime has been central in raising the importance of communal rather than individual rights; a significant concept for understanding public goods.
Considering the centrality of this justiciability, it is therefore a pity that the SADC Tribunal no longer offers the ability for individuals and communities before it. The current moratorium in place on the appointment or re-appointment of members to the SADC Tribunal, as well as on the receiving of new cases, presents an obstacle for redress in the SADC region that is challenging given the cross-jurisdictional nature of the digital economy. It also limits the capacity for the development of regionally specific legal responses to regional challenges.

Regardless of the reduction of external forums available for redress, the creation of norms for contextualising social and political objectives within the economic space is additional assisted by the flexibility of these standards. Especially within the context of the digital economy, where emerging technologies present significant challenges for ‘direct’ legislative intervention, these frameworks are of exceptional utility. As Frank La Rue, the former UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, noted:

“[...] the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet” (La Ru, 2011).

Private sector horizontality and regulation

Discussions on the obligations between state and citizen often reveal their inadequacy when confronting economic questions, given the increasing power (social, political and economic) of the private sector. Human rights instruments traditionally see the creation of negative and positive obligations on states in relation to infringements of rights (Universal Declaration of Human Rights, 1948). However, advances in the understanding of human rights soon turned to questions on the horizontal application of rights between natural and juristic persons, as:

“It can thus be argued that it is the commitment of this legal order to ensure that those rights are effectively protected regardless of whether the source of their violation is private or public conduct” (Krzeminska-Vamwaka, 2009).

Human rights discourse allows for consideration of the horizontal application of obligations, the balance of which is pertinent when considering the monopolistic power of large data holders, in particular, within the digital economy (Paulson, 2017). While regulation can of course create direct obligations on the private sector in the domestic context, the human rights discourse is emerging to help provide context for placing socio-political obligations more directly on private actors. Considering the collaborations necessary between the public and private sector, particularly for trying to establish the necessary infrastructure for a digital economy, the reality of trying to imbue these forms of obligation become important. Particularly in establishing direct public–private partnerships, these obligations can be incorporated through contract. Additionally, they can, through regulation, be inserted as socio-economic markers in considering operational licensing that are then incorporated into statute. For instance, the UNECA policy recommendations on digital trade included a recommendation that: “Operational licenses should only be issued to those platforms that respect regulatory frameworks” (UNECA, 2019). The approaches to horizontal applications of human rights are, however, exceedingly varied across jurisdictions when considering the extension of obligations outside of regulation or contract. The European Court of Human Rights views obligations as arising as follows:

That private entity’s infringing act has to be regarded as originating from the state’s failure to sufficiently protect given basic right, i.e. it would not have occurred if appropriate legislation was in force (Nawrot, F. et al., 2010).
The UN, in turn, has tried to more directly engage the role of business in the enforcement and protection of human rights through the creation of UN “Guiding Principles on Business and Human Rights” (the Ruggie Principles), drafted by the United Nations Secretary-General’s Special Representative for Business and Human Rights, Professor John Ruggie. However, the Ruggie Principles still focus on the duty of host states to act against human rights violations by companies, rather than being satisfactorily positive (Commissioner for Human Rights: Council for Europe, 2014). African human rights jurisprudence has strongly adopted dictates on the responsibilities of business, and in many ways may be able to facilitate the Ruggie Principles more directly than has been seen till now (Jacob, 2015). The recent development of the African Union Policy Framework on Business and Human Rights, provides a good opportunity for this (Adeola, 2017).

Multi-stakeholder governance and public participation

One of the methods for trying to engage the complexities of regulation in particular, is to encourage multi-stakeholder participation, and even multi-stakeholder governance models. Within the legislative realm of innovation laws, there has been an increased attempt to collaborate on law-making with private sector actors (particularly start-ups), as opposed to being sourced from regulators alone (Jackson, 2019). And public participation within the law-making process is a necessary component to the development of robust, and legitimate, laws. Human rights imperatives support these as necessary process components within the law-making environment.
Introduction

Human rights\(^5\) are, naturally, mutually reinforcing and inter-connected. It is nevertheless helpful to outline specific rights of relevance within the digital economy landscape before embarking on analysing specific policy areas of relevance for legislating. Given the data and information-centred landscape of the digital economy, references to rights that exist with the civil-political spectrum of rights is most common. Certainly, while these rights have strong connections to the enabling environment for the digital economy in particular (for instance in their association to facilitating enablers such as telecommunications and Internet as digital infrastructures), there are certainly socio-economic rights such as the right to work and right to equality of relevance. However, at least for the exercise of providing a frame (particularly a justiciable frame given limits of some socio-economic rights), the paper will focus on components of the civil political spectrum for considering specific constitutional provisions within the SADC and turn to broader rights categorisations under the policy areas.

Privacy

Privacy is a fundamental right guaranteed in almost all declarations of rights. Personal privacy\(^6\) is the human rights idea that considers an individual's personal life an area of sanctity, worthy of rights protection. In the classical human rights enunciation of the Universal Declaration of Human Rights (1948), Article 12 states that:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Similarly, the International Covenant on Civil and Political Rights (1966), to which all SADC Member States are party, guarantees the right to privacy in article 17, as follows:

No one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Notably, the International Covenant on Civil and Political Rights (ICCPR) includes a protection against unlawful interference, thus emphasising the importance of legal frameworks having an impact on the right to privacy to be established by law.

The strong link between the private space and the person is evident. Yet in the Internet age, privacy has come to be a particularly notable area of concern in relation to the protection of a person's own data and information – with fewer countries articulating the right to privacy within the information frame. Traditional American scholarship on privacy described it as the “right to be let alone”, but that was fundamentally envisioned within the context of space and property (Warren & Brandeis, 1890). The understanding of privacy within the information and communication contexts, is in fact far more modern. A review of regional Constitutions\(^7\) highlights that several regional contexts do not in fact have constitutional enunciations on the right to data privacy, per se. This modern development in our understanding of the scope of privacy is also challenged by the political and cultural context of privacy in African human rights jurisprudence.

---

5  See Annexure 1.
6  See Annexure 2A.
7  See Annexure 2A.
In the region, personal privacy was not prioritised previously as a rights area given its association to individualised, rather than communal, rights (Boshe, 2017). For instance, the African Charter on Human and Peoples’ Rights (1981) provides for a number of rights under the Universal Declaration of Human Rights (UDHR, 1948) but does not mention the right to privacy. This omission is believed to have emanated from the perceived nature of the right by the framers of the African Charter, as promoting individualism contrary to the communalism that typifies African societies. Nevertheless, the right to access, update and correct personal information, which has its origins in the right to privacy, is protected in the Declaration of Principles on Freedom of Expression in Africa. Principle IV (3) of the Declaration states that “everyone has the right to access and update or otherwise correct their personal information, whether it is held by public or by private bodies”. The African Commission also adopted Resolution 362 on ‘Freedom of Expression and Access to Information on the Internet’ (2016), which recognises that online privacy is important for the realisation of human rights, especially the right to freedom of expression and association.

Domestically, all SADC countries have constitutional guarantees on the right to privacy. These articulations of the right to privacy in domestic constitutions tend to be categorized across three key dimensions: the right to privacy in the home; the right to privacy in communications; and/or the right to personal privacy. The fact that all constitutions have some reference to privacy, demonstrates that recognition of individualised and dignity-based rights is a fundamental component of the SADC rights framework. Whether personal data privacy can be seen as a derivative of privacy in these contexts seems strongly founded; with Mozambique even demonstrating a specific data privacy component.

Yet, this must be understood within the recent case of Madheewo v The State of Mauritius & Another 2015 SCJ 177. This Mauritian case, heard eventually in the Supreme Court of Appeal, concerned the national identity card system being introduced in the country. The Appellant challenged the constitutionality of the relevant enabling law. The Court directly considered the application of Article 9 (the privacy provision) in the context of the compulsion to provide the state with biometric data. The court held that: “the coercive taking of fingerprints from the fingers of a person and the extracting of its minutiae would thus clearly fall within the scope of the protection afforded to the integrity and privacy of the person under Section 9 (1) of the Constitution”. However, in the context, it was seen to be a justifiable limitation of the Article. Importantly though, the court held that this right to privacy did not extend to a right to “private life”, but was logically only in relation to the person, property and home. It is important to note therefore that – as we have noted - the drafting of the constitutional provisions matter in considering the nature of privacy in relation to data, in particular. The courts may not be willing to broaden constitutional notions of privacy readily to privacy of information and data, if the constitutional provision is not so phrased. There is however room for courts within the SADC to be progressive by reading the right to data privacy into existing constitutional provisions on privacy. This is so, taking into account the fact that the level of technological advancements that have been witnessed since the adoption of most constitutions, has greatly altered the nature and scope of the right to privacy today.

Nevertheless, it is also worth noting that the Court, turning to the issue of storage of personal biometric data collected under the Act found that it was not ‘reasonably justifiable’ as it was not ‘relevant and sufficient’. This was because the Court was not satisfied with the provisions of the law read with the Data Protection Act related to the security of the retained and stored fingerprints and other biometric information. This was because:

Based on expert evidence, the judges concluded that there was too high a risk of unwarranted access to such highly personal data, especially in this era of cybercrime, cyberattacks and hacking. The Court was of the view that ‘the potential for misuse or abuse of the exercise of the powers granted under the law would be significantly disproportionate to the legitimate aim, which the defendants have claimed in order to justify the retention and storage of personal data under the Data Protection Act’. The Court therefore held that the retention and storage of personal data under the Data Protection Act were not reasonably justifiable in a democratic society. The provisions in the 1985 Act and the Data Protection Act allowing for the retention and storage of fingerprints and other biometric information were held to be unconstitutional (Mahadew, 2016).
In other words, strong norms on data protection standards are starting to emerge in SADC jurisprudence, even where constitutional provisions on privacy may be limited. And these norms are directly engaging with the consequences of globalisation, and the broadening of our understandings of political power from state-centred notions, to those acknowledging the complicated intersections between political and economic power; state and private actors; and notions of what constitutes public or private action.

Access to information
The right of access to information\(^8\) is of profound import within the digital economy – and of profound import for development and empowerment on the African continent. When we look to standard rights instruments, there has sometimes been a traditionalist tendency to articulate access to information as an aspect of the general guarantee of freedom of expression; a legacy of the 1948 United Nations Declaration of Human Rights (Mendel, 2013). However, access to information has come to be recognised as a self-standing right both within individual Constitutions, international human rights court decisions (Gomes-Lund et al., 2010), and international instruments. Of particular relevance are the regional instruments, which do so, such as Article 9(1) of the African Charter on Human and Peoples’ Rights: “Every individual shall have the right to receive information” (Mendel, 2013).

Access to information empowers citizens to act on their rights, ensuring cross-sectional accountability. Further, the SDGs place access to information and the pursuit of transparency as an enabler of many of the goals, while also envisioning the Internet as a vital role-player in the achievement of these goals.\(^9\) It has been noted within this context:

It is self-evident that such access to information is not only a target—an aspiration and an outcome, in other words an “end” of development. It is also a means towards achieving all the other targets of development, and not least those on justice, health, education, environment and gender (Berger, 2015).

For many, the right to access information forms the conceptual basis for many discussions on the right to the Internet as an essential enabler of access in the digital world. And a further dimension of relevance is the extension of access to information to the proactive disclosure of information associated with open government data as a necessary component for development and innovation (World Bank, 2018).

Within SADC members’ domestic constitutions, all countries have at least some recognition of access to information in the context of freedom of expression. Thus, there is a strong notion of information that emerges within the context of the ‘free flow’ of ideas and speech. However, many countries go further to include not just the notion of access to information in terms of the free flow of ideas, but also within the context of being able to petition, apply or actively receive specified information.

Freedom of expression
As seen, there are strong associations between the right of freedom of expression\(^10\) and access to information. Within the context of the digital economy, the strong role of the Internet as an avenue for freedom of expression is particularly relevant. In SADC, the right to freedom of expression is constitutionally entrenched fairly consistently. This right is no longer understood just as the right to free media but includes individualised dimensions.

When one considers the digital economy, there are, of course, additional rights such as the right to freedom of association that may be directly applicable to the notion of an unhindered Internet environment as a site for civil and political expression. Intersections with other rights will be considered more directly under the different policy areas.

---

8 See Annexure 2B.
9 These connections were well foreshadowed by the work of the World Information Society, for instance in their Declaration of Principles (2003).
10 See Annexure 1C.
Socio-economic rights

Much emphasis has been placed on the role of political and civil rights in the online context, partially as a response to where those rights sit within the normative consensus of international human rights governance. But the African region has led in human rights enunciations, which support justiciable socio-economic rights and appreciate their centrality to the realisation of justice and law, as the African Charter on Human and Peoples Rights (1981) confirms:

“…[I]t is henceforth essential to pay particular attention to the right to development and that civil and political rights cannot be dissociated from economic, social and cultural rights in their conception as well as universality and that the satisfaction of economic, social and cultural rights is a guarantee for the enjoyment of civil and political rights”.

Within the context of the digital economy, socio-economic rights – which include the right to education, the right to housing, the right to an adequate standard of living and the right to health – have a strong association to issues of content online. So, for example, the right to education imposes duties on the state. As a socio-economic right, it must be progressively realised. At a minimum this includes immediate non-discrimination, no retrogressive measures, minimum obligations and an obligation to take steps to fulfil the right and report on its realisation (Office of the High Commissioner, 1996). The right includes the right to the means of realising it, in some contexts this includes Internet access and online education. Retrogressive measures include blocking Internet access or raising the costs of Internet access where this prevents people from exercising their right to education (Rens, 2016). Copyright legislation, which has not kept pace with technology, may restrict online education but this can be resolved with suitable exceptions for online education.

The Internet can both hinder and facilitate different socio-economic rights in different ways; but their strong association to development more broadly means that it is a further dimension of the rights framework that must be incorporated into the design of policy and governance solutions (Finlay & Brown, 2016).
POLICY AREAS
The section below deals with policy recommendations which have been organised into three broad areas:

- data ownership, control and access;
- data safety and interference; and
- data-driven value creation.

Within each of these broad policy themes, there are sub-themes to further assist in thinking about policy options. This helps address the complexity of the content, but also follows traditional legislative functional areas, which could help in considering how these areas might apply within a domestic context:

<table>
<thead>
<tr>
<th>MAIN POLICY AREA</th>
<th>SUB THEME</th>
<th>SUB THEME</th>
<th>SUB THEME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data ownership, control and access</td>
<td>Data protection and privacy</td>
<td>Data and information access</td>
<td></td>
</tr>
<tr>
<td>Data safety and interference</td>
<td>Cybersecurity and Surveillance</td>
<td>Cybercrimes</td>
<td>Access restrictions</td>
</tr>
<tr>
<td>Data-driven value creation and data flows</td>
<td>E-commerce and e-transactions</td>
<td>Intellectual property and copyright</td>
<td></td>
</tr>
</tbody>
</table>

Each policy area examines key issues of relevance within the theme, following a specific consideration of SADC-relevant instruments and domestic laws (which should be read alongside the mapping exercises contained in Annexures 3A, 3B and 3C), followed by key recommendations for expansion under a Model Law on the Digital Economy.
Data protection and privacy

Key issues
Personal data privacy has emerged as an increasingly important digital rights area in the face of emerging technologies of relevance to the digital economy. In an increasingly digitalised world, there are numerous emerging concerns of relevance.

PRIVACY SELF-MANAGEMENT AND DATA SUBJECT RIGHTS
The right to personal privacy in a data context consists primarily of rights to notice, access and consent regarding the collection, processing, use and transfer or disclosure of personal data. The goal of this right is to provide a data subject\(^{11}\) with control over their personal data. Through this control, data subjects can decide for themselves how to weigh the costs and benefits of the processing against their own considerations of privacy.

However, due to the increasing number of devices and entities connected to the Internet with data subjects’ personal data, for individuals to exercise control over personal data will become extremely difficult, especially as uniform protections are not yet a reality (Cranor, 2012). And within the regional context, the reality of exerting data subject rights is made more challenging by low levels of digital literacy (the After Access survey indicates for instance that 22% of those surveyed in Nigeria, and 14% in Mozambique and Ghana, are digitally illiterate).

PROTECTION OF PERSONAL (HEALTH) DATA, AND DATA PROCESSORS\(^{12}\) BEYOND HEALTH INSTITUTIONS
There are examples emerging from the application of biotechnology, AI, machine learning, and block chain usage in Health Records Information Systems to personal health data (Dickson, 2017), and questions over the adequacy of existing laws to secure the confidentiality of associated data and information. This is especially relevant given health information as being especially sensitive and often covered by multiple forms of confidentiality arrangements. Often the laws require that the data processor of health data and information is in fact a health institution. However, it is clear that this will not be the case for tech companies providing e-health, whose services are not specifically healthcare related, but whose services are rather related to computing health data and information. The data protections afforded this form of data, also need to be weighed against the public good benefits for health aims from the effective analysis of such data.

E-health and health data are particularly important areas for considering how to balance regulation and self-regulation, given the significant benefit that digitalisation may have for public healthcare (Abrahams, 2016). There are, as well, particular public health benefits from both collection and sharing of health data (in the right conditions) for disease prevention, which has significant cross-border relevance – an issue that the COVID-19 crisis has brought to the fore (Abrahams, 2016).

BIOMETRIC DATA AND PERSONAL PRIVACY
The mass collation of biometric data (such as fingerprints, voice identification and iris identification) by the state and private sector as an identification activity – and its privacy implications – is of emerging significance. Biometric data, data which differentiates between people based on their physical characteristics, is understood as a form of particularly sensitive personal data, because of their unique and distinctive characteristics (Deliversky & Deliverska, 2018).

This ability to accurately and uniquely identify individuals has been touted for its fraud prevention strengths, and its intrinsic association to strong digital identity has it associated to positive development.

---

\(^{11}\) A data subject is any person whose personal data is being collected, held or processed.

\(^{12}\) The data processor processes personal data only on behalf of the controller. The data controller determines the purposes for which and the means by which personal data is processed.
goals like financial inclusion digital engagement (Hersey, 2019). Yet, it is worthwhile noting there can be physical limitations to biometric data reliance as a converse that could lead to exclusion – for example, absence of fingerprints, or false negatives and/or positives as a result of system failures (Privacy International, 2013).

Nevertheless, the normalisation of biometric and digital identification collection by the state has been met with caution from human rights and data justice activists (Taylor, 2017). Concerns include the role digital systems may have in exclusion and, even, growth in lived inequalities for citizens (Taylor, 2017). From a human rights perspective, there are strong emerging concerns in relation to potential privacy violations that bring issues of data protection to the fore – particularly when forms of biometric data collection intersect with surveillance technologies. Last but not least, the risk of breaches into government-hosted centralised databases with biometrics have given rise to growing concerns about the safety and security aspects of such systems.

PRIVACY AND IDENTIFIERS
'Data controller' is the term for someone who collects and controls personal data of others. Data controllers manage and process vast amounts of personal information about data subjects, from geo-localisation data, to voice and other biometrical data. Although only a few companies have comprehensive personal information for a single data subject, the aggregation of personal information from different sources can lead to very deep insights in the data subject’s life and privacy, with potential abuse as a consequence. Databases may be cross tabulated (Park et al., 2018). This means that, although a person may not be identified specifically in one database, if there is unique information in that database that can be correlated with information in another database, there are risks a person may be re-identified.

DATA SECURITY
Digital ecosystems, and the broad use of data, also raises important issues around cyber-security. An increase in touch points from where data is collected and exchanged also means more potential points of entry for an attacker (PricewaterhouseCoopers, 2016). While this is raised in more detail when we look at policy areas of cybercrime and cybersecurity, an important part of the privacy paradigm is creating positive obligations around the assurance of security for personal data.

PRIVACY AND THE INTERNET OF THINGS (IOT)
The IoT refers to everyday devices such as cars, heart monitors and smoke detectors that are connected to the Internet. IoT devices gather data, communicate it to Internet servers and are often, themselves controlled by automated systems. Despite often not being visible, or perhaps because of this, IoT devices are intrusive. Many of these devices have microphones to enable voice commands, which are constantly recording information to detect an instruction. The data is likely to be stored in the cloud. It is important to understand that there are very different kinds of data, not all of which is equally sensitive. But this does present a challenge to traditional understandings of a reasonable expectation of privacy in the home (an idea we have already seen underlying many of the SADC constitutional protections of the right). This will undercut the foundational privacy jurisprudence. IoT and AI applications are likely to operate outside of the requirements of informed consent, given their continual data processing, and create barriers between attempts to distinguish between processing personal information and sensitive personal information (such as health profiles where additional safeguards are necessitated). A recent study argued specifically on this issue that regulation in relation to IoT in Africa is ‘lagging’ the deployment of the technologies; noting that personal data protection mechanisms may not always be sufficient (Abrahams, 2017).

CROSS-BORDER TRANSFERS
An increasingly important issue regarding international and regional trade is the cross-border transfer of personal (including sensitive and not sensitive) and other data (Deloitte, 2016). In the African context, international and regional frameworks that facilitate cross-border transactions and personal data flow across countries are essential for the creation of common markets and particularly for the realisation of the African Free Trade Agreement. The cross-border data transfer of personal data is shaped by the data sovereignty approach that a country wants to pursue, which refers to the legal principle that information

---

13 See for instance the body of work developed by Privacy International on its own Identity Program, available here: https://privacyinternational.org/topics/identity
14 For an example of this, see: 2012 Stanford Law Review Symposium, The Privacy Paradox: Health and Medical Privacy, YouTube [Feb. 27, 2012]. Available at http://www.youtube.com/watch?v=nLkW45fK6x0&feature=player_embedded#
15 The African Continental Free Trade Area (AfCFTA) legal texts and policy documents are available at the following link: https://www.tralac.org/resources/our-resources/6730-continental-free-trade-area-cfta.html
(generally in electronic form) is regulated or governed by the legal regime of the country in which that data resides. As noted, this concept is challenged by the modern reality of data movements.

It is also worth mentioning the common position that the transfer of data is dependent on whether the receiving country has an ‘adequate level of protection’. However, what amounts to this adequate level of protection is usually determined by the Data Protection Authority (DPA), with some guidance from the law. Thus, in the absence of a data protection law in the receiving country, the transfer of personal data cannot be subject to proper regulation unless the law of a country forbids transfer of data except to a country with an adequate level of protection, or through the establishment of bilateral obligations through contracts between the transferring parties.

SADC review

SADC Model Law on Data Protection

The SADC Model Law on Data Protection (2013) includes two main formulations. Article 43 regulates cross-border flow of data between SADC countries that have domesticated the model law. Articles 44 and 45 regulate cross-border data transfer from a SADC country that has domesticated the model law to a non-SADC country or a SADC member state that has not transposed the model law. According to Articles 44 and 45, data flow restrictions are related to the fact that data can be transferred only if “an adequate level of protection is ensured” in the destination jurisdiction (Ncube, 2016). The SADC Model Law under Article 48 (1) restricts cross-border data flow to non-members if the non-member does not provide adequate levels of protection.

However, these restrictions are not meant to place barriers to regional and global business operations. They rather outline the conditions, which must be met for the transfer of personal data across borders. The requirement is that the transfers should be within the limits of the relevant personal data protection legislation. In cases where these laws are not complied with national legislations, public and private entities would not be able to lawfully transfer personal data across borders as part of their operations.

In addition to creating a frame for the transfer of personal data, the Model Law in the main also provides guidance on:

• The establishment of a domestic DPA;
• Integrity and quality of data;
• The provision of data subject rights;
• General rules for the processing of data;
• Obligations on those who control and process data;
• Recourse and sections; and
• Codes of Conducts.

Domestic Legal Frameworks on Data Privacy in SADC

Angola, Botswana, Lesotho, Madagascar, Mauritius, Seychelles and South Africa have enacted laws on data protection. However, only the law of Mauritius is fully in force, especially in relation to the establishment of an independent DPA, which is widely acknowledged as an essential element of an effective enforcement of data privacy laws demonstrating the lack of preparedness of several countries for the data-driven digital economy. In South Africa, the Information Regulator has been established, but the Act is only partly in force (sections 1, 112; 113 and Ch. 5 Part A have commenced under proclamation No. R. 25, 2014) (Protection of Personal Information Act, 2013). Failure to appoint a DPA in due time is repeatedly criticised for being a major impediment to effectively enforce data protection legislations, and this occurs more often in Africa than elsewhere (Greenleaf, 2011). On a positive note, all existing DPAs enjoy the status of independent agencies (Greenleaf, 2011).

In countries such as Angola, Madagascar and Seychelles data protection measures seem weak as there is no general or specific obligation to notify the data authority of a data security breach, which is a European Union (EU) General Data Protection Regulation (GDPR) requirement under article 33. All these laws include both public and private sectors. Therefore, certain data protection and privacy laws in SADC have still to establish adequate notification mechanisms in the event of data breaches. This might be due to difficulties in establishing the DPAs who will be the entity to whom to report such breaches.
South Africa’s Protection of Personal Information Act, 2013 is modelled on the EU’s personal data protection framework, especially the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. For instance, in South Africa, cross-border transfers are forbidden unless they satisfy certain requirements – most notably that the recipient is subject to a law, code or contract that ensures a level of privacy protection equivalent to that of South Africa.\textsuperscript{16}

Mauritius is considered the most advanced SADC country in terms of data protection legislation. The amended law of 2017 is now much closer in standard to the EU’s GDPR. Similarly, the recently enacted Data Protection Act in Botswana has been drafted considering the requirements of the GDPR\textsuperscript{(Ntombela, 2018)}. However, the Courts have raised concerns about the adequacy of the security provisions for biometric data collection in the Madhewoo v S (2015) judgement.

Other countries have official data privacy Bills, and it is expected that a number will be enacted soon. Those are Comoros, the Kingdom of Eswatini, Tanzania, Zambia, and Zimbabwe. Zambia has signed the AU Cybercrime and Data Protection Convention before enacting a data privacy law, which Cabinet had approved in July 2018\textsuperscript{(Greenleaf, 2011)}. In Zimbabwe, the only law dealing with data protection, or protection of personal privacy, is the Access to Information and Protection of Privacy Act (2002). However, the Act only deals with the prevention of unauthorised collection, use or disclosure of information by public bodies while private institutions are not regulated. The Act does not adequately serve to protect privacy, but it is rather an instrument of information control as it allows the government to control the media through measures such as the accreditation of journalists\textsuperscript{(Privacy International, 2016)}. In reality, Zimbabwe lacks data protection legislation and does not have a DPA to investigate breaches of data protection principles and order redress. In 2015, the government put forward a Data Protection Bill to govern both private and state bodies, which, if enacted, would "provide for the regulation of data protection" and establish a Data Protection Authority\textsuperscript{(Privacy International, 2016)}. Most recently, a Cyber Crime, Cyber Security and Data Protection Bill was approved by cabinet in October 2019 and is expected to be tabled in cabinet in due course (Muriwa, 2017).

In 2013, Tanzania embarked on the legal reform process with the aim of transposing the SADC Model Law into a domestic law. Through the HIPSSA project and with financial, technical and expert support from the ITU, European Commission and the EU, Tanzania produced her first comprehensive data protection draft bill titled ‘Draft Privacy and Data Protection Bill’, which was in 2014 renamed to ‘Draft Personal Data Protection Bill’.

The remaining SADC countries do not have separate data protection laws or official Bills. These are Democratic Republic of Congo, Mozambique and Namibia.

Namibia, which is one of only five African States to have ratified the African Union Convention on Cybersecurity and Personal Data Protection (also known as the Malabo Convention), is another country that was supported by the ITU to domesticate the SADC Model Law on data protection. It seems Namibia will not establish an entirely new DPA, but the Authority will be incorporated into the existing communications regulator, CRAN.\textsuperscript{17}

In 2017, Mozambique approved the Electronic Transactions Law, which establishes principles, general norms and a legal regime of Electronic transactions. The law is applied to public or private individuals using information and communication technologies in their activities, namely electronic or commercial transactions and electronic government. The same law appointed the National Institute of Information and Communication Technologies (NTIC), as the ICT Regulator within the scope of the Electronic transactions. Chapter IX of this Electronic Transactions Law refers to the Protection of Personal Electronic Data in Articles 83 to 85. In addition, in 2019 Mozambique, ratified the African Union Convention on Cybersecurity and Data Protection.

The main personal data protection principles that differ between SADC jurisdictions therefore include: i) registration with a DPA; ii) authorisation by the DPA for the processing of certain categories of data; iii)

\textsuperscript{16} Specifically, Section 72 of the Protection of Personal Information Act, 2013 provides the following with regards to the issue of “data sovereignty”:

- (a) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that reflect 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.

\textsuperscript{17} Interview with Deputy Director – IPRM, Ministry of ICT, Directorate: ICT Development, Government of Namibia.
Definition of “de-identification” and “anonymisation” are nuanced and context dependent. Anonymisation can be defined as “The act of permanently and completely removing personal identifiers from data, such as converting personally identifiable information into aggregated data. Anonymized data is data that can no longer be associated with an individual in any manner.” De-identification involves the removal of personally identifying information in order to protect personal privacy. In some cases, de-identified data may not necessarily be anonymised data. This means that the personally identifying information may be able to be re-associated with the data at a later time. See Educase (2015).

Principled recommendations

LAWFUL PROCESSING GUIDES
UNCTAD (2019) highlights seven challenges in the development and implementation of data protection where action is particularly needed: addressing gaps in coverage; addressing new technologies; managing cross-border data transfers; balancing surveillance and data protection; strengthening enforcement; determining jurisdiction; and managing the compliance burden. But even before addressing these higher level international alignment issues, there are more fundamental data protection issues to be addressed in law.

Typically, the laws put in place to protect the informational privacy of individuals is to place guides and limitations on how that information can or cannot be processed. Data protection processing principles can include:

- limitations on collection;
- purpose specification;
- use limitation;
- data quality;
- security safeguards;
- openness (which includes incident reporting, an important correlation to cybersecurity and cybercrime imperatives), and
- accountability.

And during all this processing, the rights of the data subjects need to be complied with and respected, with these obligations corresponding to a variety of data subject rights. Some of these policy areas are specified in more detail later.

DATA MINIMISATION
The Draft SADC Model Law on Data Protection deals with the ‘general rules of processing personal data’ and places emphasis on the right of the data controller to collect only personal information for a specific and legitimate purpose. The protection of privacy cannot simply be achieved by restricting data collection or restricting the use of computers and networking technology. In order to balance the negative consequences of over-regulating privacy by restricting ICT use, a balance needs to be identified between minimizing the collection of personal data and allowing free flow of personal data to meet the needs for analysis of large volumes of information and knowledge production, to harness the opportunities of data-driven economies and societies (Brankovic & Estivill-Castro, 1998). An important consideration within this framework is considering direct public benefits that can be facilitated by data transfer, particularly within the research realm, but also for facilitating trade (and the assessment of risk), and for law enforcement. Issues such as the improvement of cyber- and other security, as well as public health imperatives in controlling the spread of disease, serve as additional and distinct public benefits to states promoting health flows of data, regionally.

DATA INTEGRITY
Linked to the understanding that data may have economic and public benefits, data subject rights are important not only for ensuring privacy – but also helping to contribute to and sustain data integrity. Data integrity refers to the accuracy and consistency of data, which clearly impacts their broader economic benefits (Waterman & Bruening, 2014), and potentially the treatment or results of data particular to individual data subjects. This can be facilitated both through positive obligations in relation to the processing of data, but also by ensuring that data subject rights include proactive rights to access and have their personal data amended.

DE-IDENTIFIED AND ANONYMISED PERSONAL DATA

Most data protection regulations suggest that de-identified data is not personal data because it does not belong to an identifiable individual. But de-identified data is increasingly likely to be re-identified.
especially since the 4IR expands personal data uses beyond traditional processing, such as with IoT. This, therefore, requires additional scrutiny of the methods of aggregating data and third-party handling of aggregated data to minimise threats of de-identified data being misused (Tene, 2013). De-identified data may need to be incorporated within lawful processing requirements.

Comparatively, anonymised data remains anonymised and does not pose major concerns for personal data regulation, although exclusive control of anonymised data may raise competition concerns. Practical indicators for businesses to understand how to facilitate the options given the centrality of trust building in the privacy sphere should be developed.

CONSENT
Consent underscores much of lawful processing as the key mechanism for establishing permission from individuals for the use of their personal data. As the central permissive ‘act’, what constitutes consent is exceptionally important; and the nature of that consent is that it should be voluntary and informed. The digital environment presents significant challenges as to what the reality of informed consent can mean (Pearce, 2016). However, a properly capacitated DPA that can provide both best practice for collectors and processes, while also providing guidance on technological tools available for the public to enhance the reality of granting consent, can be instrumental (Pearce, 2016).

PERSONAL DATA AND SECURITY BREACHES
Article 25 of the SADC Model Law on Data Protection, 2013 refers to security breaches and requires reporting without undue delay. But the Model Law does not specify what would constitute a security breach, or undue delay, or what would be considered a reasonable cause for delay. Also, it does not place an obligation on the data controller to explain to the Authority why it delayed.

The Article also does not place an obligation on the data controller to notify the data subject of a breach, and there is no requirement on the part of the data controller and data processor to disclose what information has been compromised.

Importantly, placing these obligations on a data controller need not be onerous if a regulator is in place to provide guidance. Data controllers can establish notification procedures when initially complying with personal data obligations so that for most this will be a once off exercise.

Personal data can be manipulated to the detriment of the data subject in ways that leave the data subject unaware and vulnerable. Obligations to notify the data subject and the DPA within a reasonable time, taking into account any circumstances of the breach, should be included in legislation. Furthermore, the data controller should notify both the DPA and the data subject of the information that has been compromised and suggest ways to safeguard themselves from attack. This is because the business itself is best placed to understand the nature and extent of the breach. Without creating these forms of positive obligations, laws failed to provide for adequate transparency.

Meaningful accountability and consistent enforcement mechanisms are essential for any effective data protection framework and strategy. A baseline of cybersecurity capacity is necessary to enforce data protection, but must be realistic as to the resources, capacity and imperatives in the SADC. Security should not be an afterthought when rapid development and deployment of digitalisation initiatives are taking place.

PRIVACY BY DESIGN
Privacy by design is the approach taken when developing digital technologies and systems by which privacy is incorporated into technology and systems by default during the design and development process (Cassakian, 2011). It means a product is designed with privacy as a priority, along with whatever other purposes the system serves. This design should incorporate a particular understanding of how data subjects engage with products, and their capabilities for asserting their privacy (Park et al., 2018).

The Draft SADC Model Law on Data Protection does not place emphasis on the principle of ‘privacy by design’. However, instead of placing ‘check-box obligations’ on the data controller, emphasis should be on requesting the data controller not only to simply comply with the data protection regulations placed on them, but also to implement appropriate technical and organisational measures and procedures in such a way that all data processing activities including the collection, storage and use of data meet the data

---

19 See Section 22 of the South African Protection of Personal Information Act, 2013. The provision on Breach Notices places an obligation on the data controller and data processor to be transparent and accountable when it comes to security breaches.
protection requirements, while ensuring the protection of the rights of the data subject (Bert-Jaap Koops & Leenes, 2014). These forms of positive obligations on businesses are able to practically coerce changes to the practice of data protection but need not be highly punitive. Such provisions would have to be considered against the counter imperative of innovation.

**CROSS-BORDER CO-OPERATION, HARMONISATION AND MINIMUM STANDARDS**

Limitations on cross-border data transfer could result in business opportunities lost and reduce the ability of an organisation to trade internationally, leading to a reduced geographical footprint and loss of market competitiveness. But data regulation that is synchronous with that in other jurisdictions contributes to mutual trust and lays a foundation for a trusted exchange of data, including (but not limited to) personal data. In this sense, personal data protection regulation enables and improves trust and trade in the cross-border movement of persons, goods and services (Information Society, 2018).

A misconception on data protection harmonisation comes from the view that harmonisation requires all national laws to be identical. This approach does not consider national differences in existing frameworks, or advancements in technological innovation. Rather, harmonisation should be pursued through compatibility between national legislations, based on a set of core, agreed data protection principles.

**DATA PROTECTION AUTHORITIES**

Independent, accessible and well-resourced (both in terms of financial and human resources) DPAs are an important mechanism for achieving the balance between flexible rule making, and accountable oversight. The effectiveness of DPAs also hinges on the extent to which they have been empowered by the enabling Act to investigate and issue binding orders in relation to their mandate. This in turn acts as a deterrent and ensures that victims of personal data breaches can access effective remedies. There is also a role to be played by regional entities: A significant criticism of the AU Convention on Cyber Security and Personal Data Protection is the lack of a regional body to help oversee and monitor laws, though this is of course not a concern for domestic law making (Shyllon, 2019).

Not only do proper functioning DPAs offer flexibility and expertise, they can also issue regulations that are responsive to sectoral peculiarities – and thus help to ease potential compliance burdens, which may not be commensurate to digital (and other) innovation imperatives.

**ADMINISTRATIVE JUSTICE AND RECOURSE**

Outside of notification procedures, data subjects need to be assured of adequate access to remedies. In order to facilitate the adaptable generation of regulations, DPAs need to be adequately empowered. For example, empowering a DPA to allow for considered exclusions, helps prevent the positive obligations generated from being inappropriately onerous on different business forms. However, in order to facilitate this kind of flexibility, an adequate administrative justice paradigm is necessary to ensure accountability for such decisions.

In considering administrative justice and data protection, some laws do include provisions that preclude automated decision-making on the basis of a data subject’s personal data. In the context of AI, but also complex data processing, the utility of such prohibitions as a form of accountability assurance should be considered.

**DATA SOVEREIGNTY**

Data sovereignty draws on the concept of the sovereign nation state, which has been the organisational unit of international relations for the past 200 years. In the context of digitisation of global markets and the expansion of services and digital products across borders, data sovereignty refers to the view that data that is generated in, or passing through, national internet infrastructure should be protected and controlled by that State. In the digital context, it can be understood as a subset of cyber sovereignty defined as the subjugation of the cyber domain (which is global by definition) to local jurisdictions (Wright & Polatin-Reuben, 2014). Two approaches of weak and strong data sovereignty exist: on the one hand, weak data sovereignty refers to private sector-led data protection initiatives with an emphasis on the digital-rights aspects of data sovereignty. Comparatively, strong data sovereignty favours a state-led approach with an emphasis on safeguarding national security (Wright & Polatin-Reuben, 2014). In general, the transfer of personal data to a third country is allowed only under certain conditions, for instance when a third country has a law that requires sufficient safeguards (including privacy and security) for the processing of personal data. It is recommended, however, that instead of taking a ‘weak’ approach, which expands private sector influence, or ‘strong’ approach that expands state influence, sovereignty demands the expansion of both
state and individual sovereignty in the context of data. This necessitates ensuring strong data subject rights, but also focusing on a governance model that enhances multistakeholderism (and does not just exist on continuum between state and private sector).

Data localisation is a concept that moves beyond data sovereignty. Despite a number of benefits associated with the possibility of organisations (and states) being able to easily share data across borders, a number of countries—across every stage of development—have erected barriers to cross-border data flows, such as data-residency requirements that confine data within a country’s borders, a concept known as “data localisation” (Cory, 2017). Data localisation can be explicitly required by law or can result from other restrictive policies that make it onerous to transfer data legally, such as requiring companies to store a copy of the data locally, to process data locally, and mandating individual or government consent for data transfers. It can also be sectoral, i.e., only relate to data within a particular sector or function. This extremity in policy may present practical challenges given the actualities of the environment, and also may introduce the opportunity for potential abuse by security apparatus (Hicks, 2019). Beyond the practical challenges, strict data localisation rules requiring the storage of all data locally and not merely a copy, renders such data susceptible to security threats including cyber-attacks and foreign surveillance. Such policy may also have an impact on the decision of foreign businesses to invest in an economy. Data localisation does not replace the need for sound data processing practices; and ensuring data processing practices must be the regulatory priority.

**Data and information access**

**Key issues**

**OPEN DATA**

There is a need for information access to extend beyond reactive disclosure, directly recognised by the AU Model Law on Access to Information. The proactive release of open government data offers broader social, political and economic gains (McKinsey estimate that open data could unlock USD 3-5 trillion in economic value annually across specific sectors) (McKinsey, et al., 2013). Internally for business, innovation can be fostered by increased access to data (World Bank, 2014). It can also be used to improve evidence-based decision-making within organisations.

Some forms of foreign direct investment are encouraged by strong in-country good governance measures, to which open government data significantly contributes. In addition, more accurate and frequent disclosure of macroeconomic open government data has been found to allow countries a statistically significant reduction in borrowing costs (on average there is an 11% reduction in credit spreads) (Trenovski, 2016).

These kinds of economic benefits can have more discrete benefits to digital businesses – open government data can be used to reduce the “red tape” that can inhibit businesses and agencies from thriving. It can also enhance market entry and allow for greater access to procurement systems by a wider range of actors.

There is also a plethora of utilitarian benefits that open government data can forward. Open accurate data can be used to facilitate reporting (and automate significant portions of it), but also to forward coordination efforts between departments and agencies. These improvements in efficiency and time have very direct economic value: the European Commission has estimated that open government data is forecasted in 2020 to result in cost-saving benefits to European countries to the tune of EUR 1.7 billion (Carrara, 2015).

**ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND DEEP LEARNING**

The significant appetite for data required for machine learning processes has of course spurred the growth in data collection. The ability to analyse mass amounts of data is facilitated by algorithms and formulas – but the opacity of these algorithms present challenges, both in terms of the outputs of the algorithms (for instance content limitations on information such as in newsfeeds) and decisions made through them (and their ability to perpetuate bias) (Comninos, & Konzett, 2018). Bias can be introduced through the data used, assumptions used, or even within the formula design choices. And the opacity in relation to algorithms can be both technical, but also are proprietal (i.e. restrained due to commercial interests) (Comninos, & Konzett, 2018). All these problems then are underscored by a lack of transparency, and thus associated with the requirements for a broader transparency framework that facilitates the digital economy.

Despite a number of benefits associated with the possibility of organisations (and states) being able to easily share data across borders, a number of countries—across every stage of development—have erected barriers to cross-border data flows.
NATIONAL SECURITY
Access to information needs are often juxtaposed directly against security concerns and the balance between the two can be challenging for policymakers. This balance will be discussed in more detail later, but the Global Principles on National Security and Access to Information could be instructive in this area.

EMERGING RIGHTS
While the right to Internet access has begun to emerge in the rights lexicon, recent jurisprudential developments in India have raised an issue of incredible relevance to the SADC: and that is the extension of the right to Internet access to include access to Internet-enabled devices (ZLHR and MISA Zimbabwe v Minister of State for National Security, 2019). As indicated by the After Access Survey results, seven in ten of African Internet users access the Internet through a mobile phone. Device accessibility is of incredible relevance to notions of information access and the development of a good digital economy.

In Europe, an extremity to the right to access (and correct) one’s own data as a form of data subject right has been the development of the ‘right to be forgotten’. This concept, the result of a European Court of Human Rights decision, allows data subjects in Europe the power to request to have a URL that links to their personal data delisted (so it won’t show up in general searches) (Bertram et al., 2019). The practice of this ‘right’ has demonstrated a form of hybrid governance that was not necessarily the intention of the decision and empowers platforms with a new form of editorialising power through their ‘review and moderation’ function (Chenou & Radu, 2019). The abuse of the procedures by individuals and politicians to challenge legitimate legal and/or public information is a practice that has been highlighted in data analysis, and then problematises how decisions can be made on the rights balancing required in future (Bertram et al., 2019).

SADC review
DOMESTIC LEGAL FRAMEWORKS ON ACCESS TO INFORMATION IN SADC
The Model Law on Access to Information for Africa is an important reference instrument in the region. Notably, the Model Law places a strong emphasis on focused and detailed proactive disclosure provisions.

Within SADC, Angola, Malawi, Mozambique, Seychelles, South Africa, Tanzania and Zimbabwe have standalone access to information laws (though again, criticism has been raised from some quarters about Zimbabwe’s law as being one which does more to restrict, rather than facilitate, access).

There have been long-fought campaigns across the region for access to information laws, and countries such as Botswana, Mauritius, Namibia and Zambia, which have notably failed to pass Bills on access to information for many years (Lesotho, Madagascar and Swaziland also have Bills in progress). The Comoros has no foreseeable legislation currently.

Most of these laws lack comprehensive proactive disclosure provisions, in spite of the Model Law. There is also not a strong consistency in the provision of Regulators, which present challenges both to the adaptability of the laws, but also limit the access to recourse for businesses and citizens.

Principled recommendations
ACCESS RIGHTS
While data subject rights are provided for in many data protection regimes, there are other components of the right to access information of relevance to the digital economy. The right of persons to access information includes, but is not limited to, the right to access their own personal data.

Rights to access government and, in certain circumstances, private sector data, fosters transparency and directly combats the information asymmetries that challenge regional business development. In order to benefit from global value chains (facilitated of course by ICTs), the private sector in developing countries need to be actively assisted in overcoming information asymmetries (Organisation of Economic Co-operation and Development, 2013). This should mean the development of data access rights where they do not exist, which include rights of access for both public and private sector actors, as promoted by the AU.
Model Law on Access to Information. Consideration should be given to open data policy, in which the default for government is for (protected, anonymised) data to be open rather than closed.

DATA PORTABILITY

As another area of data subject rights, and of particular relevance in the context of competition and the digital economy, is the issue of data portability. Data, generally, is non-rivalrous (at the technical level, it is infinitely usable without detracting from another person's ability to use it) (Jones & Tonetti, 2020). Yet, importantly too for understanding the movement of data within the digital economy, it is not simply portable in a way that can facilitate scale effects easily between firms (Rinehart, 2020). Portability remains a key cited strategy for facilitating competition, and consumer benefit, though the realities are not yet definitively beneficial (Mitretodis & Euper, 2019; Rinehart, 2020). Importantly from a privacy perspective, outside of just interoperability changes, the nature of big data collection means that data portability implicates other users privacy (Nicholas & Weinberg, 2019).

Yet, it is not just the data of citizens or consumers that is relevant considering in relation to data portability, but also the labour rights of platform workers – such portability might allow them to shift their portfolios across competing platforms – with potentially positive labour and consumer welfare outcomes.

It is the collective nature of data collection that actually drives economic value for firms – big data is the source of the anti-competitive dominance of the GAFAM and BATX companies (Thieulin, 2019), alongside the capacity to interpret that data, but also (to a degree) to sell it on (Noble, n.d.). Yet the reality is that the data brokerage is increasingly only secondary to the economic value that the dominating firms can extract from interpreting that data and feeding it into their own product and service design, which relates to economies of scale (Martinez, 2019; Mitretodis & Euper, 2019). This is why, while it is non-rivalrous technically, it is still treated proprietorially by firms and businesses.

With regard to potential abuse of dominant position in relation to the process of datafication, an example of such conduct would be dominant platforms preventing data portability of ‘contractors’ and users. While the EU's General Data Protection Regulations provide a broad right to data portability, domestic data protection laws like South Africa's do not (De Hert et al., 2018). Yet, there have been some criticisms of the EU's right from a competition perspective stating it is too uniform, and not first considered by establishing whether or not a dominant market power exists (Swire & Lagos, 2013).

There are practical challenges to facilitating data portability (and prescribing it in law) (Rinehart, 2020; Swire & Lagos, 2013). For instance, without the necessary skills, other businesses cannot leverage this data anyway; nor may they find value in it given the specificity of how data might be collated for the originating firm's priorities. However, interoperability of data and data portability is a necessary area of exploration for a digital economy. Moving forward, this will become especially important as a consideration for facilitating domestic competition in relation to AI, which relies on big data sets. This is because the inability to access big data has been identified as a partial inhibitor (in collaboration with ineffective innovation policy) to the growth of local capacity in relation to AI development. Data portability is not to be considered as a direct response to that challenge, but it is worth considering as additional policy support for a ‘good’ digital economy from a competition and ‘supply side’ perspective.

OPEN DATA

Access to information laws should have clear guidance on open data. Although open data policies are a necessary step for ensuring open government data domestically, legislative guidance could assist in creating a more enabling environment for the passage of such public policies. Within these frameworks, governments "...should prioritize the collection of qualitative and quantitative gender disaggregated data on women's participation in the digital economy to inform meaningful dialogue and policymaking" and to enhance the positive benefits of government data (UNECA, 2019). In other words, obligations should extend beyond mere disclosure, to including the positive obligation to generate data of certain types, and standards. These data generation obligations can go some way to creating harmonisation on issues of biometric and other data collection by the state.

EXPLAINABILITY, TRANSPARENCY AND ALGORITHMS

There are challenges to transparency, both practical and normative, that are generated through the growth in automated decision-making and algorithmic-based services. One solution in relation to algorithms is

---

22 South Africa's Protection of Personal Information Act, 2013 does not include a right to data portability, as the European General Data Protection Regulations do.
deemed “as the right to explainability” potentially generated from a composite of data subject rights in the EU’s GDPR, which requires data collectors of personal data to explain to data subjects how the data is being processed and used (which could explain algorithmic biases) (Comninos, 2014). However, some legal scholars have argued that this is an unfounded expansion of the actual rights in current European law though it is desirable (Wachter, 2017). But the limits of current EU law need not inhibit the SADC from developing next generation law.

Another form of ensuring transparency within algorithms is by preventing automated decision-making (such as the prohibition against automated decision making seen in section 17 of the Protection of Personal Information Act, 2013). While these prohibitions of course come with exceptions, they seek to address a very specific avenue of algorithmic transparency: decisions taken on the basis of algorithms that are based on personal data.

These concepts have been driven by the privacy imperatives of emerging personal data regimes. However, important questions remain about possible ends served by other expressions of algorithmic transparency, particularly in relation to accountability for content provision in ‘feeds’ of social media platforms (commonly understood within the context of disinformation) (European Union, 2018). It may also be instructive to consider how existing access to information paradigms may be amended or utilised to serve some of the ends described, together with open data frameworks as discussed above.
Cybersecurity and surveillance

Key issues

CYBERSECURITY
Cybersecurity refers to defensive mechanisms put in place by government, private sector, CSO, or individuals to protect themselves from malicious online behaviour. These concerns are relevant at all levels from international to regional to national - and in the context of the digital economy - attention to security imperatives should be placed at the business level, as well. Nevertheless, cybersecurity measures are currently seemingly not prioritised by African businesses: Cybersecurity budgets in many organisations are reported to be less than 1%, with many organisations having a zero-budget allocated to cybersecurity (Kshetri, 2019). Company security is extremely important because of both ripple effects internally and network effects externally. So internally, failure to use up-to-date software, for instance, can increase an organisation’s exposure of threat to malware and hacking. Externally, strong cybersecurity practises in an economy are akin to the concept of ‘herd immunisation’: a base level of security infrastructure needs to be in place across organisations (whether networked together or not) to increase security levels, as a whole, sufficiently, to prevent cascading failures (Dawson, 2019).

Cyber-attacks can be launched either by States or by non-state actors. If state actors launch them, they may fall under the category of cyber warfare, which considers state interference in national affairs. If non-state actors launch these attacks, they amount to cybercrime. National security threats are no longer earth bound: cyber warfare refers to computer or network-based conflict involving politically motivated attacks by a state-actor on another state-actor. Given both globalisation and security developments, these politically motivated attacks may even be perpetrated by non-state cross-border organisations or actors (Mbanaso, 2016). A classic example of cyberwarfare was demonstrated in Estonia in 2007, where cyber attackers (allegedly Russian) disrupted public web resources, including the Estonian Parliament, banks, ministries, newspapers and broadcasters, through a coordinated online assault (Mbanaso, 2016). Such an attack presents not only technological challenges, but the repercussions also affect real lives, processes, organisations, etc. with substantial economic effects.

MASS SURVEILLANCE AND COMMUNICATIONS INTERCEPTION
Mass (or bulk) surveillance involves the mass pre-emptive collation and analysis of citizen data, going beyond communication interception. It is normally conducted by State Security Agencies and is cited as necessary to fight terrorism, prevent crime and social unrest, protect national security and control the population. Although famously perpetrated by the United States, African governments have also participated in mass surveillance - with several states cited as having procured mass surveillance technologies from popular German producer Trovicor (Electronic Frontier Foundation, 2012). The Egyptian government has frequently been outed for the mass surveillance of social media communications through its “Social Networks Security Hazard Monitoring Operation”.

Associated to mass surveillance is mass or bulk data collection (resulting in ‘big data’). Such activities might be state-driven as, for instance, in the mass collection of epidemiological data for combatting diseases, such as COVID-19. Mass personal data collection (either directly or through telecoms networks) in such a context, might also happen to facilitate contact tracing and quarantine enforcement (Gillwald et al., 2020). The public interest in these scenarios often leads to reduced oversight – yet, while these crises are time-bound, the data collection and retention may not be (McDonald, 2016).

Mass surveillance presents a number of problems: First, considering that mass surveillance capability is increasingly automated, such a practise raises questions about oversight and scrutiny of the technology utilised to carry out such surveillance (Livioia, 2019). From a human rights perspective, in democratic states, mass surveillance can be unlawful and invalid because it clashes with constitutional rights to privacy. Surveillance is unlawful or unconstitutional when it fails to adequately prescribe the procedure
for notifying a person whose information has been intercepted or when it fails to adequately prescribe the proper procedures to be followed when state officials are examining, copying, sharing and sorting through data obtained via interception of communications. This was demonstrated in the South African case of Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others [2019] ZAGPPHC 384. The Court, on learning of acknowledged practice of mass surveillance by state security agencies, ordered that: "...It is declared that the bulk surveillance activities and foreign signals interception undertaken by the National Communications Centre are unlawful and invalid." This was because of the lack of express empowering legislation to do so. Any attempt at legislating for permissions of mass surveillance would have to consider the necessity and proportionality of such a law - given the nature of proportionality requirements in international law, it is in fact difficult to consider what a justifiable, lawful permission for this form of activity could look like.

Surveillance and communications interceptions are practices that can undercut trust in the state when abused, and human rights imperatives become instructive to avoid loss of confidence in state institutions that have a duty to protect citizens’ security. Considering that states have the duty to put in place the correct mechanisms to protect citizens’ rights to safety and security, lawful interception of communications (i.e. not on a mass basis) is a resource for States seeking to monitor security threats. Therefore, the constitutional right to privacy might be justifiably limited when safety and security of citizens are a risk. In such a case, the State has the duty to authorise the police, defence force and intelligence agencies to assist a lawful interception of communications to meet the State's security obligations. Parliaments, therefore, are called to balance these two conflicting rights – right to privacy on the one hand, and right to safety and security on the other, by providing for judicial oversight and limiting interception only to those cases where a serious crime is involved.

Mass surveillance by African states tends to rely on technology supplied by commercial providers that are based in the global North. As a result, mass surveillance brings with it the risk that the data will also be accessible to other actors that might include the security services of other countries. The accumulation of personal data by African states creates a target for state and non-state actors, many with superior technological capabilities.

**FACIAL RECOGNITION**

The growth of popularity in the use of facial recognition software is changing the surveillance landscape. The utilisation of facial recognition by law enforcement is facing increasing scrutiny from lawmakers (Ulle, 2019). Beside more generic concerns related to data privacy, high levels of inaccuracy bring into stark clarity questions of how such instituted measures can be proportional as a means to achieve purported aims (as discussed in relation to broader biometric data earlier). And, even if accuracy of such measures is to grow, oversight of the incorporation of the technologies remains a concern.

Facial recognition projects are of growing interest to many governments, with Zimbabwe recently implementing a large project in collaboration with Chinese firm, Cloudwalk (Jilli, 2019). But as seen in discussions on data collection more broadly, within the facial recognition realm there is, again, a growing reality of facial data monopolisation and thus monopolisation within the software segment as well, with one study suggesting that by 2023 China will dominate the market with a 44.59% market share (Burt, 2018).

**CRITICAL INFRASTRUCTURE**

A key vulnerability that must be considered within Cybersecurity interventions are the specific vulnerabilities of critical infrastructure (assets essential for the functioning of the economy). The networked nature of computer infrastructure within such entities, as well as Internet-enabled operations, means such infrastructure may be susceptible to external attack (Cohen, 2019). Within the context of cyber warfare, an understanding of the reality of risks for critical infrastructure is important for policy development (Lewis, 2006). The networked nature of such attacks also implicates cross-border coordination in cybersecurity responses for critical infrastructure, as well (Brechbühl et al., 2010)pervasive relationship, and trust. It presents a network model of the interactions needed for effective cybersecurity, consisting of nodes that collaborate in the performance of various key elements of a cybersecurity framework. It mentions that an effective cybersecurity policy requires developing international collaboration wherein information on risks, vulnerabilities, and best practices are shared. It says that the Global Regulatory Exchange of the International Telecommunication Union (ITU).
NETWORK SECURITY
When considering vulnerabilities within a cybersecurity framework, telecommunications actors should have specific security obligations such as:

- denying unauthorised persons access to information of value;
- ensuring the authenticity of information handled by telecommunications systems;
- preventing the disruption of telecommunications services; and
- ensuring the resilience of telecommunications networks (Calandro, 2019).

These obligations are normally met through technical standards on safety and security. Also, telecommunications operators have a strong interest in keeping networks safe and secure, because cyber-attacks might compromise their reputation or their capacity to protect the confidentiality, integrity and authenticity of data and information of their clients, with serious repercussion on client subscription rates.

Nevertheless, legislators in other regions have put in place mechanisms to achieve high standards of network and information security by setting a number of reporting requirements (Brechbühl et al., 2010), which apply to operators of essential services and digital service providers (DSPs), specifically related to security risk management and incident reporting obligations (EU Directive on Security of Network and Information Systems, 2016).

INTERNET CONNECTED DEVICES
Internet connected devices include the IoT. Examples include smart pacemakers, cars and connected security cameras. Security for these devices is often poor, even though an attack using these devices could have serious physical consequences. Many have hardcoded default passwords that cannot be changed by users, while others by default do not have unique passwords.

SADC review
MALABO CONVENTION
The African Union Convention on Cyber Security and Personal Data Protection (2014) is a regional instrument on cybersecurity. The Convention has been signed by Comoros, Mozambique and Zambia, but only ratified by Namibia and Mauritius and is thus not in force. However, the content has not been without criticism, from free speech activists in particular. For instance, the normally broad blanket ban on the processing of personal information without consent, is in this Convention attenuated with the phrase: “Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed”. There are also content restrictions for materials that “insult” - a term that is left unsettlingly vague. If countries were to ratify, however, reservations on particular clauses could be noted.

DOMESTIC LEGAL FRAMEWORKS ON CYBERSECURITY
Beyond legislation focused specifically on cybercrime, Malawi, Zambia and Zimbabwe have broader cybersecurity laws. Angola has also enacted a cybersecurity law on the protection of information networks in 2017. South Africa’s Cybercrime Bill (split from the controversial Cybercrimes and Cybersecurity Bill, 2017) is awaiting Presidential signature. Comoros and The Democratic Republic of the Congo meanwhile lack either enacted, or proposed, cybersecurity legislation. In relation to surveillance and communication interception in particular, South Africa and Zimbabwe have express communication interception legislation. It is worthwhile in this context to consider the recent judgment on South Africa’s interception legislation, Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others [2019] ZAGPPHC 384. The court deemed certain aspects of the law as unconstitutional, because the procedural aspects described for gaining permissions in terms of the Act were generally insufficiently detailed and failed to provide for adequate oversight of requests.

CAPABILITY AND COUNTRY MATURITY ASSESSMENTS
An important consideration often raised in the context of cyber security is not just the risks it poses, but the capabilities of the state and its agencies to combat cybercrime. Capability and maturity assessments therefore become a precondition for exploring legal and policy interventions. Member states require the capacity to develop and deliver cybersecurity strategy and enhance their cybersecurity resilience. Capability is required in early warning, deterrence, resistance and recovery systems, effective security...
policy, in delivering national defence and resilience capability, maintenance of benefits of a cyberspace vital for government, international business and society in general.

The Global Cybersecurity Index (ITU, 2018) indicates that only Mauritius demonstrates a high commitment across all five pillars of their index. Neither Angola, the Democratic Republic of Congo or Lesotho, in fact, participated in the 2018 study and all are ranked ‘low’, as countries that have only started to initiate commitments in cybersecurity (other SADC countries ranked as ‘low’ include Comoros, Madagascar, Malawi, Mozambique, Namibia, Seychelles, Swaziland, and Zimbabwe. Botswana, South Africa, Tanzania and Zambia are ranked as ‘medium’ countries, ‘that have developed complex commitments and engage in cybersecurity programmes and initiative’.

INSTITUTIONAL ARRANGEMENTS
The arrangement or framework of institutions responsible for creating, governing and managing cybersecurity capacities vary from state to state in the SADC. All members have a department or ministry related to communications or ICT, but only a few have an institution dedicated to cybersecurity: Mauritius has the IT Security Unit and National Computer Board; Zimbabwe the Department of ICT Systems Security, and South Africa has a National Cybersecurity Advisory Council and Cybersecurity HUB. Mauritius and Zambia both have an ‘ICT authority’ responsible for overseeing cybersecurity initiatives like the National Computer Board and zm-CIRT, and in the case of Botswana, Tanzania and Malawi, cybersecurity capacity, including the planned and operational cybersecurity response teams, falls under their communications regulatory authorities. In Seychelles, an IT division under the president is responsible, while some ICT ministries have a designated chair, like the minister of cyber security in the Ministry of Information Communication Technology, Postal and Courier Services in Zimbabwe.

MULTI-STAKEHOLDER COLLABORATION
Intersections between such a variety of stakeholders from both the public and private sector as well as the public good of cybersecurity across the spectrum, requires multi stakeholder collaboration for governance. Mauritius has instituted a model for stakeholder engagement in this area that – rather than being hierarchical – includes users as targets of public awareness campaigns from law enforcement agencies and the national Computer Emergency Response Team (CERT)(Van der Spuy & Oolun, 2018). Adapting traditional governance models in this manner is to be commended, though this version of the model does not formally include space for civil society engagement in decision making. While lessons for (or from) the model are instructive, so are the calls for the adaption of that model, which included involving local banks as well as financial regulators; smaller businesses; and young IT professionals (Van der Spuy & Oolun, 2018). Cybersecurity collaborations should be both vertical (e.g., between overseeing organisations and other stakeholders) and horizontal (e.g., between peer stakeholders) interaction between and among stakeholders (Van der Spuy & Oolun, 2018).

INCIDENT RESPONSE
Technical cybersecurity capacity is effectively developed through the creation of cybersecurity response teams (generally referred to as a CSIRT, CIRT or CERT). These teams are tasked with preventing, analysing and responding to cyber incidents, among other services and functions aimed at creating a more secure cyberspace.24 National CIRTs have been set up by the ITU in Zambia and Tanzania, and are also in place and operational in South Africa and Mauritius. Phase 1 of operations are reportedly underway in Botswana following a CTO policy collaboration and have been announced in Angola and Malawi, though signs of implementation are limited. Beyond national CIRTs, incident response is reportedly provided ad hoc by telecommunications providers in Madagascar, while South Africa and Mozambique have internationally recognised sectoral CIRTs, in finance (Standard Bank CIRT in South Africa and academia (SANREN CSIRT and UCT-CIRT in South Africa, and MoRENet in Mozambique). Comoros, DRC, Eswatini, Lesotho, Seychelles and Zimbabwe have neither implemented nor announced CIRTs of national or sectoral capacity, although a CIRT readiness assessment was conducted by the ITU in 2014 for DRC, Lesotho, Eswatini and Zimbabwe.
Principled recommendations

CYBERSECURITY STRATEGIES

The first stepping-stone for an effective cybersecurity policy and regulatory framework is a cybersecurity strategy. As a contributor to other regulatory efforts, member states should publish a national cybersecurity strategy that provides for inclusive economic opportunities and risks associated with ICT uptake. National strategy must align with the country's economic vision and its national security imperatives. The strategy should:

- Demonstrate commitment to cybersecurity, which is public and transparent;
- Designate a competent authority and the clear delineation of its authority; identify the key government entities affected by, and/or responsible for the implementation of the national cyber security strategy;
- Identify commercial-sector entities affected by, and/or responsible for the implementation of the national cyber security strategy (recognizing commercial sector dependencies);
- Identify the financial and human resources requested and allocated for the implementation of the strategy;
- Define a roadmap for governance that identifies key stakeholders and clear responsibility for cybersecurity at all levels of government (local, regional and federal or national) with clearly defined roles and responsibilities;
- Involve private sector and civil society involvement and partnership in multi-stakeholder initiatives to promote cybersecurity;
- Identify the percentage of GDP expected to be gained or lost (grossly) by implementing the strategy;
- Identify critical services (in addition to critical infrastructures) that the strategy intends to make more secure and resilient; and
- Identify national standards for continuity of service agreements (24 hours/7 days a week) and outage reporting requirements for each critical service, industry and infrastructure.

Statute should support the powers outlined in the strategy and empower as necessary for the implementation of such a strategy.

INCIDENT RESPONSE, REPORTING AND DATA SHARING

In the event of natural or manmade cyber-related disasters that affect critical services and information infrastructures, each member state needs an effective national incident response capability. Member states must establish and maintain National Computer Security Incident Response Teams (National CSIRTs) or Computer Emergency Response Teams (CERTs). The CSIRTs should serve a broad national constituency (beyond government and critical infrastructure providers), such as proactive obligations for incident reporting (a key factor to combat cyber threats). To this aim, CSIRTs should collect good data on types of incidents and risks. CSIRTs should also facilitate information sharing horizontally across government agencies, as an act of national security. The access to information regime can also facilitate the sharing of information.

Some specific provisions with regards to CSIRTs are:

- The publication of an incident response plan for emergencies and crises;
- The identification and mapping of cross-sector dependencies that address continuity of operations and disaster recovery mechanisms;
- Evidence that the plan is exercised and updated regularly;
- The publication and dissemination of a national cyber threat assessment(s) on government, critical infrastructures and essential services networks;
- The identification of a network of authoritative national contact points for governmental and regulatory bodies;
- The development of an information warning and alert system that can be used by national crisis/response centres to effectively receive, address and transmit urgent information in a timely manner;

---

25 A detailed description of a CSIRT Service Framework is available on FIRST.org, at the following URL https://www.first.org/education/csirt_services_framework_v2.0
• The identification of the financial and human resources requested and allocated for the National CSIRT to carry out its mandate;
• The identification of additional funding to activate and regularly test the information warning and alert system and to measure the country's resilience to cyber incidents and crisis through national cyber security exercises;
• A demonstrated capability in the incident containment, management, resilience and recovery processes for critical services and infrastructures;
• A demonstrated ability by national crisis/response centres to address and transmit alerts in a timely manner;
• Evidence of ongoing research methods analysing trends or groups of computer security incidents of national concern—sharing similar actors or tactics, techniques and procedures—in order to identify patterns; and
• The development and implementation of a system/program to regularly test and measure the nation's resilience to cyber incidents and crises through national cyber security exercises.

CROSS-BORDER COORDINATION AND JOINT RESPONSE

Fighting cyber-attacks require cross-border coordination. The EU has recently established a joint sanction regime for cyber-attacks, which is a model that SADC could replicate. While this is more a question of regional organisation, domestic legislatures will need to ensure a base level of cyber security readiness in order to proactively engage. These should also have a cybercrime focus.

CAPACITY-BUILDING

Bearing in mind a country's cybersecurity capability assessment, there is a strong need to ensure the capacity both within both the policymaking and implementation arms of the public sector. And, given the digital and networked ecosystem, the public sector must also oversee and encourage the capacitation of the private sector on cybersecurity capabilities (particularly those involved in critical infrastructure functions).

Cybercrimes

Key issues

TYPES OF CYBERCRIME

There is a vast range of cybercrimes that are relevant to both the digital economy and broader security. Such crimes might involve the use of electronic devices to commit copyright infringement, fraud, hacking, account thefts, identify theft and computer viruses. An example of how traditional crimes have been transformed by digitalisation includes fraudulent ‘pay-per-clicks’ in e-commerce. There have been such a large number of reported fraudulent ‘clicks’ from Africa on Internet pay-per-click advertising, that paid-search companies such as Overture have implemented “continental cut-off” services, which reportedly disregard clicks on advertising originated from the continent (Kshetri, 2010).

HORIZONTAL PRIVACY

An interesting area of concern are the invasions of privacy and surveillance that may occur between citizens, as a result of digital technologies (Kurbalija, 2016). This is an important specific consideration for criminalisation, particularly in the context of digitalised violence against women. Protections against voyeurism and digital harassment should be incorporated within criminal sanction (Kurbalija, 2016).

CRITICAL INFRASTRUCTURE AND NATIONAL KEY POINTS

As seen, there is a significant focus in the national cybersecurity policy environment on critical infrastructure (Lewis, 2006). The response by some domestic jurisdictions is to criminalise different forms of interference with critical infrastructure, which includes digital intervention. However, both regionally and domestically, these forms of laws are criticised as being overly broad and used as a method for repressing lawful dissent or could unduly interfere with legitimate business activities (Baser et al., 2017; Ferreira, 2019). Attempts to legislate in this context must be done in synergy with human rights norms, and the broader digital economy ecosystem.

USER SIDE CONCERNS

According to the After Access Survey results, privacy and security have directly impacted on the extent of use of the Internet for a number of African users (Chair, 2017). Physical security, financial fraud, hacking, harassment, slander, stalking and surveillance were privacy and security concerns mentioned by focus group respondents. However, these issues were more predominant for urban and peri-urban users than rural users. For some of the respondents, privacy-related crime was an issue, and they expressed concern about protecting passwords for websites and banking details and about the hacking of private e-mails and social media accounts (Chair, 2017). In particular, there are concerns about malware that could be used to steal information. In Nigeria, users were greatly concerned with fraudulent access to banking information (Chair, 2017).

Thus, it can be seen that there is a legitimate concern for the security of persons in relation to online forms of crime, which threaten trust and participation in digital marketplaces. The actual cost from cybercrime to the global economy has been stated as ‘more than [US$]445 billion’ (Tamarkin, 2015). And Africa is a region at risk:

Africa [is] becoming a cybercrime safe harbour because of increased Internet availability at lower costs, a rapidly growing Internet user base and a dearth of cybercrime laws on the continent. Cybercriminals in Africa are not only using techniques such as the ‘419’ scam or ‘advance fee’ fraud that originated in Nigeria, but are also deploying more advanced and ‘lucrative forms of cybercrime that involve the use of botnets, remote access Trojans, and banking/finance-related malware’ (Tamarkin, 2015). [Footnotes excluded].

It has been posited that cybercrimes cost African economies $3.5 billion in 2017 (with Nigeria losing $649 million and Kenya losing $210 million) (Kshetri, 2019).

Levels of both digital and English literacy, as well as broader awareness of cybercrime, present particular challenges for African users (Kshetri, 2019). This digital literacy is impacted with how many African citizens engage with the online space: low Internet penetration rates and high data costs mean many African Internet users only use the space rarely, which means they are largely ‘passive’ consumers of online content (Gillwald & Mothobi, 2019). And many are at the same time are unaware of the potential risks, which calls for broader awareness-raising efforts.

SADC review

SADC MODEL LAW ON COMPUTER CRIME AND CYBERCRIME

The SADC Model Law on Computer Crime and Cybercrime, 2013, creates a discrete list of offences. It seeks to guide jurisdiction. A further focus is efforts to support cyber law enforcement through outlining the admissibility of digital evidence for combating cybercrime and other procedural law adaptions. It also seeks to provide guidance on issues of liability for various forms of digital intermediary.

DOMESTIC LEGAL FRAMEWORKS ON CYBERCRIME

Dedicated cybercrime bills have been enacted in Madagascar in 2014, Mauritius in 2003, Seychelles in 1998, Namibia in 1988, Zimbabwe in 2004 and 2019, and South Africa and Zambia in 2004 and 2018, though the Computer Misuse Act in Seychelles and Namibia have been identified as inadequate for the current technological landscape (Calandro, & Berglund, 2019). Draft bills on cybercrime, though not yet ratified, have also been introduced in Botswana in 2018, Eswatini in 2014, and Namibia, Lesotho and Seychelles in 2013.

Principled recommendations

CYBER LAW ENFORCEMENT AND CROSS-BORDER COLLABORATION

Cybercrime transcends national borders and requires transnational solutions and international, multination and regional approaches. By developing law enforcement capabilities to fight cybercrime through the ratification of treaty documents, international cooperation, capacity development, the implementation of anti-botnet programs and other initiatives, countries can mitigate their cyber risks and boost future economic growth. Member states should show international commitment to secure society against cybercrime and proactively build domestic cyber law enforcement capacity by developing legislation and regulatory frameworks. This takes the form of involvement with international fora dedicated to addressing international cyber–crime issues as well as the establishment of domestic legal and regulatory mechanisms...
to combat and prosecute cyber-crime. The legal and regulatory authorities designated with carrying out activities to curb cybercrime must define what constitutes a cyber-crime and empower governmental entities with the mechanisms, expertise and resources to investigate and effectively prosecute cybercrime activities.

CRIMINALISATION
An overemphasis on criminalisation can detract from the preventative components of law-making within this area. This is particularly important within the regional context, as over-criminalisation can then either purposefully or accidently impede on other rights. In particular, in the SADC region, caution must be exercised to avoid the criminalisation of speech (Seger, 2015). However, this must be weighed against the existence of socially destructive behaviour that can only be the subject of state power if a criminalising statute is put in place (Seger, 2015). Legislation should provide some clarity in the form of a list of offences, which should include offences focussed on ensuring computer system integrity.

Specifically, legislation should, in addition, cover the criminalisation of the possession and transmission of child pornography and gaining access to child pornography websites. An exemption that enables law enforcement agencies to carry out investigations should be included. These should include provision for criminalising the intentional and illegal production, sale and associated acts related to child pornography.

CRIME INVESTIGATION AND AUTOMATION
Investigation of crimes must consider digital realities. For one, legislation must ensure that the admissibility and sanctity of digital evidence can be protected to effectively combat crime (Kshetri, 2010). Procedural law should accommodate considerations of data preservation, production order, search and seizure, real-time collection, extradition, mutual assistance and the limitation of use of evidence.

And within this area, the law must ensure that automated decision-making and data collection from law enforcement cannot unfairly prejudice the public. Scope for legislating on automated decision making can, as seen, be included within data protection provisions.

ORGANISATIONAL SECURITY
Considering the issues of cybersecurity, herd immunisation and commerce vulnerabilities discussed, it is important to create positive obligations on businesses to implement security. However, in order to balance such obligations from being overly oppressive, they should be linked to a regulatory regime with a regulatory authority able to ensure that obligations are flexible and appropriate.

EDUCATION AND AWARENESS
The establishment of a mature institutional ability to fight cyber-crime can only be assured by including training for court judges, prosecutors, lawyers, law enforcement officials, forensic specialists as well as other investigators on cybercrime and cyber-security challenges and regulation.

And, particularly when considering the role of cybercrime and cybersecurity in creating the necessary trust environment vital for stimulating the digital economy, these awareness activities must extend to the broader public - both as a demonstration of activities taking place, but also for capacitating individuals to enhance their own cybersecurity.

Access restrictions
Key issues
INTERNET AND SERVICE SHUTDOWNS
An Internet shutdown is the intentional disruption to Internet access within a particular jurisdiction. It can be defined as:

(An) intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information (AccessNow, 2019).

A shutdown can cause wholesale disruption, but might also be a 'partial' disruption to specific services (and could also include ‘filtering’ or ‘blocking’). There are both social and economic impacts to such disruptions. A seminal report by the Brookings Institution indicated that shutdowns crippled the global digital economy by...
USD 2.4 Billion between 2015 and 2016 (West, 2016). Expanding on the methodology used, the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) also commissioned a report in 2017, in which it estimated that sub-Saharan Africa lost up to USD 237 million to Internet shutdowns since 2015 (CIPESA, 2016). The ICT Policy Centre for Eastern and Southern Africa provides a framework for estimating the cost of such shutdowns in sub-Saharan Africa. The risks are not just threats to civil and political rights, but to direct social rights as well. There are inherent health and security risks that can directly affect citizens when services are interfered with through Internet service disruption.

INDIRECT RESTRICTION
It is worth reflecting on indirect forms of Internet and service restriction outside technical obstructions, which could include social media taxes placed on users. This form of restriction greatly inhibits users and the opportunity to exploit digital dividends. So, for instance, the introduction of a social media tax in Uganda has been directly attributable to a decline in Internet penetration in the country from 47.4% to 35% (Nanfuka, 2019). Outside of the direct negative consequences for the broader digital economy, it also becomes counter-productive in that it shrinks its own tax base, as users decline and in addition, find ways (such as through the use of Virtual Private Networks) to circumvent the tax (Nanfuka, 2019). The direct impact on socio-economic rights through these interventions constitute retrogressive steps that may violate existing human rights commitments. An Internet tax that raises the cost of Internet access, thus reducing Internet access, infringes on the human rights to expression, education and work for every person whose use of the Internet for expression, education or work is eliminated or reduced. Since these are existing entitlements, retrogressive steps such as an Internet tax are prohibited by human rights law.

CONTENT RESTRICTION
Content restrictions can be viewed as separate to Internet and service disruptions – as they are interference in the distribution of online content directly related to the nature of the content itself. Unlike traditional electronic and print media for which there are strong normative frameworks, and which can be regulated effectively on the basis of penalties (and incentives) at the national level by broadcast authorities and print ombudsmen, the Internet content generated flow across jurisdictions, presenting various enforcement challenges. Increasingly, these have taken the form of ‘take-down’ of specific types of content and are frequently legislated for across jurisdictions as a responsibility for service providers. A broad array of content may be illegal in different jurisdictions, for instance, on the basis of child rights, privacy and personal data, pornographic content, etc. The challenge, of course, becomes developing a normative basis for the processes that is consistent enough to allow for cross-border clarity.

Domestically, key concerns are the applicability of territorially bounded national laws on cross-border online spaces, the proper procedures for content restriction orders by public authorities, and the role of providers.

INTERMEDIARY LIABILITY ISSUES
Issues around intermediary liability present themselves in the context of all the types of interference so far described. In many senses, collusion, persecution or private agreements between state governments and Internet Service Providers (ISPs) have been examples of a sort of indirect control over the Internet that contradicts openness principles (Lucchi, 2011). In fact, one of the first incidences of Internet ‘censorship’ was experienced in 1996 in Zambia when the government wielded the threat of criminal prosecution against an ISP, Zamnet, to force the removal of a banned edition of the Post Newspaper (Burnheim, n.d.). However, when a United States based reader posted a version on a United States hosted site, the ban was rendered useless since the copy was hosted beyond the limit of Zambian prosecutorial jurisdiction. Typically, though, intermediaries such ISPs are granted limited liability for the content they host, though subject to take-down and/or other notification procedures and rules. These kinds of “incident specific” procedures provide a simpler statutory mechanism for instilling balanced normative considerations. However, such intermediaries now hold incredible powers over access to information, but also mediate risks in terms of certain content distribution. How they regulate and police their content through policy and bilateral agreements is becoming increasingly significant to understanding the digital environment (Internet & Jurisdiction Policy Network, 2019).

27 An online tool, which implements this methodology is available at: https://netblocks.org/cost/. The tool helps demonstrate, for instance, that even for a partial shutdown of just social media in Zimbabwe, the daily cost is still upwards of USD 1 million.

28 An outline of the forms of content that might be restricted in different jurisdictions is given a useful typology in Internet & Jurisdiction Policy Network (2019).
Imposing obligations on service providers to police content may appear to offer a solution. However, in a bid to reduce costs intermediaries are likely to deploy automated systems and low-cost labour, which is unable to achieve an appropriate balance between competing interests and the values at stake. Moreover, even a well-functioning system of private adjudication would be significant abdication of state power and responsibility.

The South African experience with intermediary liability is instructive. The Electronic Communications Act 2002 limited liability for ISPs. One class of providers that cache or host content must comply with takedown notices. However, the provisions inadvertently fail to give all the types of communications providers immunity. The take down procedure does not give the person who uploaded content a right to respond to the claims made by a complainant, nor impose adequate penalties for false claims (Comninos, 2012). The takedown procedure in practice, therefore, seems an unjustifiable infringement of the right of freedom of expression. A proposed change, intended to remedy the lack of appeal process, was no better: giving the complainant the power to decide whether the response to the complaint was valid. A notice and notice procedure could resolve many of the problems that arise on notice and takedown (Rens, 2015). Such a procedure obliges the intermediary to forward on the received notice to the subscriber, to help achieve a balance between the competing interests.

The roles of intermediaries in content restriction, and freedom of expression, has only become more heated in the context of global content platforms like Facebook and Twitter. Contributing to this is the particular political role First Amendment rights on free speech play in the American context, where such global platforms derive from. The issue with these global content platforms is that they have become the main way in which many consumers engage with content and create and circulate their own content online. In the context of traditional media, there is increasing pressure to consider content platform intermediaries less as ‘neutral’ intermediaries, but more likened to publishers with attendant editorial responsibilities. This places a disproportionate amount of power in the hands of only a few companies. In this context, legal scholars are starting to posit alternative legal mechanisms for achieving the required balances, such as creating fiduciary duty on platforms to the consumer or creating positive obligations in law on content platforms to include adequate technical mechanisms for regulating content (Li, 2018).

SADC review

SADC MODEL LAW ON ELECTRONIC TRANSACTIONS AND ELECTRONIC COMMERCE

The SADC Model Law on e-Transactions provides significant guidance on the different types of intermediary liability that may be relevant across policy areas when it considers ‘service providers’. In addition, issues of relevance to criminal liability are outlined in the SADC Model Law on Computer Crime and Cybercrime.

DOMESTIC LEGAL FRAMEWORKS ON ACCESS RESTRICTIONS

Zimbabwe, Malawi, Lesotho and the Democratic Republic of Congo have all experienced forms of Internet shutdowns in recent years. Many of these have been facilitated through ‘acts of collusion’ with the private sector, rather than through empowering legislation. This has been replicated elsewhere in the region: in 2011 former President Hosni Mubarak shut down the Internet and cell phone access in Egypt during the ‘Arab Spring’ through collusion with three major telecoms companies — Vodafone, Mobinil and Etisalat (MacKinnon et al., 2015). This Act was later declared “unconstitutional” on the basis that the interventions were done without the appropriate court orders, resulting in fines.

There may also be instances where legislation permits forms of shutdowns in the SADC. In Angola, partial restrictions on access are permitted by the Social Communication Legislative Package (Pacote legislativo da comunicação social). Additionally, in Zimbabwe, though a recent court decision (ZLHR and MISA Zimbabwe v Minister of State for National Security, 2019) successfully interdicted the suspension of Internet access instituted by government, it did so not on the basis that there is no such authority to do so, but rather that the Minister was the incorrect authority in light of the interception legislation available.

Principled recommendations

TAKE-DOWNS AND HUMAN RIGHT NORMS

While notice and take-down procedures are commonly incorporated within electronic legislation - and provide a case-specific form of intervention - it is possible to include human rights and rule of law
considerations into such processes by including ‘fair balance’ considerations (Angelopoulos & Smet, 2016). Extending notice and notice provisions may also be positive.

**CONTENT RESTRICTION**

Content restrictions are noticeably different to Internet shutdown. Certainly, there is a need for coordination between platforms and government to achieve the balance between protection against harm and the scope of interventions (Li, 2018). Importantly though, this broader debate on content regulation must be considered when forms of liability, and limitations on liability, are being established under law – and the balance should be informed by human rights considerations, as well as digital economic considerations.

**DUE PROCESS OF LAW, PROPORTIONALITY AND NECESSITY**

Normative standards for considering interference with Internet access can be sourced from international human rights. Considerations such as proportionality and necessity could be used to guide the actions of possible law or policy interventions, all under pre-conditions of lawfulness being established.

Necessity means that any restriction of Internet access must be limited to measures, which are strictly and demonstrably necessary to achieve a legitimate aim (Internet Society, 2019). It should be demonstrated that no other measure would achieve similar effects with more efficiency and less collateral damage. Any restriction of Internet access must also be proportional. A proportionality assessment should ensure that the restriction is the least intrusive instrument amongst those which might achieve the desired result. The limitation must target a specific objective and not unduly intrude upon other rights of targeted persons.

However, any attempt to interfere with access will need to be understood within the context of the Joint Declaration on Freedom of Expression and the Internet, which co-declared with the then ACHPR Special Rapporteur on Freedom of Expression and Access to Information, Adv. Pansy Tlakula, that:

Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet (UN Special Rapporteur on Freedom of Expression & Others, 2011).
E-commerce and E-transactions

Key issues

E-COMMERCE READINESS
A fundamental contextual concern is assessing the e-commerce readiness of each jurisdiction. UNCTAD provide indexing in this area and their results have demonstrated a strong relationship between the Index Values and actual incidences of online shopping (UNCTAD, 2018). A noteworthy analogue measure in e-commerce readiness is the reliability of postal services – a factor that strongly negatively impacted regional results, but is not necessarily readily thought of within the digital economy environment (Stuart, 2018). The strengthening of the digital economy obliges us to look across the commerce value chain. E-commerce presents possibilities for greater visibility for African products; and market expansion and reach (with significantly lower financial investment than traditional commerce) that could facilitate access to global markets (Kituyi, 2019). However, notably the results of the Index for the developing world demonstrate the reality of the digital divide in the e-commerce context:

The elite, together with an emerging middle class, which have the technical ability and are financially qualified to undertake e-commerce, are the groups most likely to be able to participate. The rural underclass and the poorest of the urbanised underclasses are currently excluded (Stuart, 2018).

CONSUMER DATA
A significant part of business-to-consumer (B2C) e-commerce is the use of consumer data for profiling needs and targeting user experience and product offerings – which benefits relate significantly to economies of scale (Martinez, 2019; Mitretodis & Euper, 2019). Data analytics (and potentially for the well-developed firm, AI) and the use of other intelligent data extraction and analysis tools can enable regional businesses to compete in higher value-added industries, “...and are examples of transformative digital technologies that will impact skills development for the twenty-first century” (Bayat, 2019). Harnessing the data has proven difficult also for e-commerce companies in Africa as the uptake of e-commerce remains small, and there are many analogue components that are not well functioning in the ecosystem.

But, as it develops and with the multinational platforms operating on the continent the mass collection and processing of personal data (which could include aspects of use behaviour) will require e-commerce enterprises to be cognisant and compliant with data privacy obligations. There are, of course, also implications for advancing digital skills to include user experience methods and data analytics for individuals to fully realise the dividends of e-commerce opportunities. And, as seen under “data portability” issues addressed earlier, consumer data issues also have implications for worker data in the context of digital work.

CONSUMER PROTECTION
The digital economy, and its ability to facilitate cross-border exchange, presents concomitant challenges in terms of consumer protections, which are typically domestically defined. This of course also links to the issues of cybercrime addressed earlier with risks ranging from credit card fraud to user and password identity theft. As will be shown with smart contracting, technological solutions begin to present themselves – such as the growing incorporation of two-phase authentication for preventing fraud (Chandran, 2011). From a legal perspective, imposing legal obligations on businesses can go some way to helping ensure a more trustworthy digital commercial space (similar to how data protection processing requirements extend
security obligations) (Chandran, 2011). Obviously, data protection requirements contribute to consumer protection, but include other considerations like payment security, returns, false advertising and after sales service. Providing consumers with effective redress for these issues is both an offline and online challenge in the consumer space, expounded upon cross-jurisdictional issues (Trade and Development Board, 2017).

**DIGITAL IDENTITY**

Ambitions for comprehensive state-led digital identity systems have been influenced by the foundational work of multilateral organisations. In 2017 the World Bank, under its “Identification for Development” (ID4D) program, developed “Principles on Identification for Sustainable Development” (World Bank, 2017); including guidance such as ensuring universal coverage and robust security, these principles were then used as the foundation for the #Good ID movement. This movement brings together a variety of stakeholders to co-develop solutions for “good” digital identity system implementation, globally. The GSMA has a specific Digital Identity Programme focused on mobile technologies (GSMA, 2019). Other organisations, such as the International Monetary Fund (Gupta et al., 2017) are influencing the discourse insofar as digital identities relate to their broader mandates. A strong focus of the literature is therefore digital identities as a “fundamental gateway to development” (Dahan & Sudan, 2015).

Good digital identity becomes a central enabler for engaging in public and private digital services, as well as necessity for reaping forms of digital dividends. Digital identities can be viewed through the prism of a developmental economy, with cited benefits being efficiency gains for government service delivery (Dahan & Sudan, 2015), the ability to assert rights to access service (a vital component then in turn of South Africa’s developmental programme) (World Economic Forum, 2018), and/or boosts to financial inclusion (World Bank, 2017).

Those development benefits cited consider broader digital identity systems. However, when digital identity is considered in the context of functional needs, it also becomes the mechanism through which consumers can engage with commercial services (whether B2C or B2B), and through which users engage in platform and other Internet services. From a broader digital economy, digital identities are the mechanism through which, from the supply side, workers might engage (and benefit) from new forms of work.

Caution must however be noted on centralising digital identity to avoid excessive centralisation on ‘entrance’ requirements to services and digital economy opportunities within the regional context. Some of those cautions link back to those discussed on digital inequalities, passivity and security. In addition, in many developing countries where electricity supply may be unstable, essential BDI systems may go offline: the Kenya elections were in fact threatened by the introduction of new electoral systems that struggled with both electricity supply and Internet coverage, meaning a manual back up is relied on (Privacy International, 2013). With Internet penetration still a challenge across the continent, particularly in rural areas, new forms of digital exclusion emerge when the provision of state services or digital opportunities begin to be intrinsically associated to new BDI systems.

**CONTRACTING**

Underscoring digital commercial transactions, both business-to-business (B2B) and B2C, is the issue of validly establishing both transactions and contracts. Due to the nature of the digital economy, this requires establishing mechanisms for validly concluding a contract in the digital space, as well as consistency in how this is achieved across borders. The United Nations Commission for International Trade Law’s (UNCITRAL) Model Law on Electronic Commerce suggests establishing rules for:

- Ensuring the legal recognition for a data message;
- Admissibility and evidential weight of electronic messages;
- Formation and validity of contracts and the recognition of electronic documents by parties;
- Attribution of electronic documents;
- Time and place of dispatch of electronic communications; and
- Signature (South African Department of Communications, 2000).

These areas are traditionally the realm of e-transaction laws. But with the growth of globalised negotiations, and as we move from the role of individual transactions to establishing formalised contracts, the need to move beyond recognition of digital signatures to formalising the requirements for advanced electronic signatures becomes more relevant. This is because there has been a slow uptake of advanced

---

29 The foundations of the Good ID movement can be explored here: https://www.good-id.org/en/about/
electronic signatures in jurisdictions such as South Africa, which has been identified as inhibiting e-commerce (Snail, 2018). In jurisdictions that recognise advanced signatures, uptake may nevertheless be low because of the registration requirements normally associated with their implementation. Ensuring formal recognition for different forms of digital signatures is essential for building trust in the digital commerce environment and becomes increasingly significant as a mechanism for preventing fraud and other forms of cybercrime (Schoeman, 2019). Some recommended characteristics of advanced electronic signatures include:

- That it is unique to the user;
- That it can identify the user;
- That it can only be created by the user;
- That it can be linked to the data message in such a way that any subsequent change of the data message is detectable; and
- It is based on the face-to-face identification of the user (Schoeman, 2019).

Smart contracts are also an emerging reality worth noting. Smart contracts are blockchain-based operations that control the entire commercial transaction: the protocol only releases the funds once all contract conditions are met by both parties or, at least, the distributed software governing the contract has received signals the conditions have been met. The truth is that many of the transactions that occur online do not require complex agreements; instead, they rely on trust more than formality. And trust can be designed (Ryan, 2017):

“The types of contracts that demand close attention to and legal expression of the terms and conditions are those that give rise to enduring relationships that require significant investment or those that expose one or both parties to high levels of risk. The need to reduce terms to a written contract rarely arises in relation to small, low-risk, ongoing transactions”.

It should be clear then that the full formalities of contracting and their recognition in the digital space, will remain important - particularly as we move from the B2C to B2B space. What the concept of smart contracts helps bring to the fore, is how trust-building might in fact be enhanced by technological and digital innovations, rather than being considered a challenge.

There are further contracting trends too in the digital space that relate to the recognition of transferable documents, which historically relied on physical possession (such as bills of lading, etc.). Especially within a trade context, specificities on legal recognition of such documents has been recognised in European instruments, such as the UNCITRAL Model Law on Electronic Transferable Records (2018).

Websites, including many commercial websites, claim to bind users to their terms of service. Similarly, many websites, especially transactional websites, require users to agree to extensive contractual terms by clicking on a box. There is no option for negotiating the terms. These are referred to as contracts of adhesion. The online environment imposes so many such agreements that the time required to read and understand these agreements makes them impractical; with research confirming this directly within regional contexts such as South Africa (Baloyi & Kotze, 2017). These issues associate back to some of the challenges in relation to consent that were discussed when considering data protection.

**MOBILE MONEY AND E-PAYMENT**

Mobile money not only facilitates electronic payment for e-commerce services, but may also bring the unbanked into the commercial environment (FinMark Trust, 2017). So central is mobile money to the digital economy, that it is included alongside banking account ownership as an indicator for assessing a state’s B2C e-commerce readiness (UNCTAD, 2018). And the promotion and fostering of mobile money markets and systems by regulators is likely to have a direct benefit for fostering intra-regional trade (Abrahams, 2017). Quite simply, it facilitates exchange beyond physical boundaries.

Within this environment, the challenges are similar to those experienced throughout the digital economy environment: how best to balance regulation with innovation:
For e-money institutions, proportionate prudential requirements must be tested in terms of a balance between ensuring the stability of the institution and avoiding the creation of barriers to market entry and enhancing new innovations in this market. In this case, setting the initial capital amount is less important than achieving the envisaged objectives of a legal framework (Tuba, 2014).

There are real user benefits to the facilitation of mobile money and e-payments, as evinced from the After Access User Survey. In Nigeria, participants across all income groups said they use the Internet for financial transactions and professed their satisfaction with the ease of this activity. One user in Nigeria said: “I use mobile banking. If I want to pay now, I can do it now even to recharge my phone. I don’t normally buy airtime [in any other way], I buy from my account.” And online financial transactions were seen directly to foster participation in e-commerce (Chair, 2017).

CRYPTOCURRENCIES

While mobile money is regarded as being ‘on par’ with conventional currency, an entirely different world of digital exchange exists whereby digital tokens of various types can be used in exchange for goods (Tuba, 2014). Cryptocurrency in turn provides a specific regulatory reality. Many cryptocurrencies are blockchain-enabled digital currency. Blockchain is a form of distributed ledger, which means that the ‘ledger’, which monitors the production and distribution of the currency is held on an entire network of computers, meaning that (as no single place controls that record) it is impossible to counterfeit. They are, fundamentally, not controlled by a central reserve bank. Exchanges of the currency are also anonymous, facilitated by their design.

Cryptocurrency adoption on the continent is growing significantly, with 13% of South African users for instance claiming to own some form of cryptocurrency (International Finance, 2020; Olivier, 2020). For regulators and governments, the fundamental challenge is the exclusion from oversight of both mining of the currency and exchange of the currency. This creates challenges for tax collection, with many jurisdictions having to rely on the voluntary declarations of such assets (Olivier, 2020). The value of cryptocurrencies has been notoriously unstable, which financial regulators have raised as their chief concern (Masie, 2020). Many African countries have been unwilling to take a clear stance on the regulation of crypto, while many have simply banned its use (International Finance, 2020).

For users, however, the security of the exchange and the ability for remittances and digital transactions to occur in countries where local currencies may be problematic or expensive to exchange from originating currencies, is incredibly appealing.

ENCRYPTION

Encryption becomes important as a method of empowering users to protect themselves from cybercrime. This can be encryption on communications, but also within the framework of transactions. Yet encryption presents an interesting conflict: while it of course improves an individual’s security online, law enforcement officials complain that it hinders their ability to investigate (CCDCOE, 2019). Two key approaches emerge: some countries support legislation to compel technology and communications companies to decrypt customers’ data, while others (the Netherlands, Estonia) have voiced support for strong encryption (CCDCOE, 2019). Some claim that requiring “encryption backdoors” at the regional bloc level, if a strongly capacitated regional oversight entity could be assured, would enable law enforcement while preserving the integrity of communications. However, no viable methods to ensure that a designed weakness in an encryption system will not be exploited by bad actors, has yet emerged. Since many of the global actors, both state and non-state, that threaten the security of digital communications and transactions in Southern Africa have superior technological capabilities to almost all commercial actors (and most of the state actors) in the region, requiring ‘designed flaws’ will render the region vulnerable to bad actors – while simultaneously discouraging technologically innovative companies from operating in the region.

SERVICES-BASED E-TRADE

This concept links back to how the digital economy is impacting the labour market. The facilitation of e-commerce from the consumer side can drive the market for services-based e-trade (Stuart, 2019). Of course, as mentioned, this does not necessarily guarantee the creation of ‘decent’ work. Platform work is often able to circumvent the requirements of traditional domestically sourced labour protections (ILO, 2018).
CUSTOMS COMPLEXITY AND IMPACT

The reduction of customs complexity through policy is a key method for facilitating regional e-commerce by improving both logistics for customer and business as well as costing and internal efficiencies for business. Importantly too within the context of the African Continental Free Trade Area (AfCFTA), trade tariff incongruency more broadly can presents risks of ‘trade deflection’ (Stuart, 2019). In addition, is the reduction in customs friction through digitisation – with policy becoming relevant to help facilitate the acceptance of electronic documentation for freight and logistics (World Bank, 2016). Thus, the digital economy is not just impacting how customs should function but facilitating customs efficiencies through digitalisation and e-customs processes (World Bank, 2017). To enable this conducive customs environment further will also require the required ICT infrastructure, capacitation of officials, and ensuring cross-border traders are made aware of digital custom procedures.

Demand-side research has demonstrated that affordability of devices is a main barrier to Internet use in Africa (Gillwald & Mothobi, 2018). In spite of this, digital products are taxed as luxury goods in many countries, driving up costs (World Bank, 2017) and the costs are often amplified with additional customs taxes. The digital dividend gains of improving access to devices and thus, connectivity, have the potential to largely offset the direct economic losses experienced by minimising taxation (ITU, 2015).

E-TAXATION AND DIGITAL TAXATION

Taxation is an innately domestic strategy and thus the digital ecosystem – by its very nature – presents challenges for taxation. However, there are issues specific to digital and e-taxation worth noting for the growth of the digital economy in Africa.

A central issue is how to reallocate taxing rights in favour of the user/market jurisdiction by targeting digital businesses (OECD 2019). A particular project of the OECD relates to trying to manage tax base erosion and profit sharing, called the BEP Action Plan (Oguttu, 2016). However, the Plan insufficiently considers the African context (for instance, the plan ignores strengthening more traditional anti-avoidance provisions that have remained a challenge for developing countries even prior to the e-taxation challenges) – which has reiterated calls for African governments to have a more active voice in these forms of global policy debate (Oguttu, 2016).

In 1998, the World Trade Organisation issued a Declaration on Global Electronic Commerce, which created a moratorium on taxing ‘electronic transmissions’. A broad interpretation of the moratorium has meant that transmitted intangibles need not be taxed. However, the rapid expansion of the digital economy, since the Declaration was released, has revealed its inefficiencies. Developing countries have lost the ability to use tariffs as a way of encouraging local digital industry and tariff revenue losses (Indian Government & South African Government, 2020). This is particularly challenging in the context of the market dominance of global digital platforms like Facebook and Twitter, which increases tax base erosion. Countries such as India, Australia and the United Kingdom are exploring different methods for taxing digital platforms to try and manage tariff revenue losses to these mega-companies (Barnes et al., 2019).

A further concern is the manner in which digital technologies can facilitate tax evasion and illicit financial flows (Tropina, 2016). These then intersect with issues that were raised in relation to cybersecurity and cybercrime, where calls for ensuring definitions can extend to the crimes concerned, but also the facilitation and capacitation of cyber law enforcement must all be supported by cross-border collaboration.

SADC review

SADC MODEL LAW ON ELECTRONIC TRANSACTIONS AND ELECTRONIC COMMERCE

As seen, the Model Law does outline issues which relate to the role (and liabilities) of service providers. It pays significant attention to definitions relating to electronic communications in order to try and facilitate e-transactions. It outlines the legalities of electronic transactions (including a provision on electronic signatures). It also outlines consumer protection provisions.
E-COMMERCE READINESS
According to the UNCTAD E-commerce Index 2018, the regional average for Africa was 30, which was well below the world average of 55 (UNCTAD, 2018). However, since 2014, "sub-Saharan Africa has surpassed global growth on three of the indicators used in the Index" (UNCTAD, 2018).

MOBILE MONEY AND E-PAYMENT
The Payments Systems Project is a very active one in the SADC, in direct recognition of the digital economy benefits that can be facilitated by digital payment. This was developed under the Payments Subcommittee of the Office of the Committee of Central Bank Governors (CCBG) in the SADC (Abrahams, 2017). In addition, the Mobile Money Guidelines (which followed a review commissioned by the CCBG) provide useful legal and regulation guidelines, adopting a model where mobile money licenses can only be granted by a central bank (Abrahams, 2017).

In 2016, mobile money adoption ranged from 21% in Swaziland and 22% in Botswana to highs of 45% and 51% in Zimbabwe and Tanzania respectively, but this does not assist a strong SADC regional average (Abrahams, 2017). Contextually, there is evidence to support an approach that focuses on improving mobile penetration and device access (Abrahams, 2017). Later data from the GSMA demonstrates how Sub-Saharan Africa is "the enduring epicentre of mobile money" (Naghavi, 2019).

Principled recommendations

ROLE OF REGULATORS
There are strong guidelines available in the SADC Mobile Money Guidelines on regulators for that specific subset of digital economy concerns. As is fairly consistent within the digital economy framework, regulation requires balancing innovation and constraint:

In the mobile financial services context, this applies to, among other things, the presence of agents and super-agents; clarifying the relevant market definitions; and consumer protection, e.g. transparency in billing (Abrahams, 2017).

To allow for innovation, particularly in the realm of both mobile money and cryptocurrencies, businesses can be given space through "Regulatory Sandboxes" to test out their products without the risk of potential legal liability (Centre for International Private Enterprise and New Markets Lab, 2018). The South African Reserve Bank has already publicly stated its intention to such (Masie, 2020).

ELECTRONIC TRANSACTIONS
The Draft SADC Model Law on Electronic Transaction and Electronic Commerce (2013) notes more specifically how regulation in relation to components of the electronic transaction should assist in providing legal clarity. To expand on this, it is instructive to consider that UNCITRAL texts, in trying to seek balance, have been drafted along three key ideas:

- Non-discrimination - “a document would not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form”;
- Functional equivalence - which sets down the criteria “under which electronic communications may be considered equivalent to paper-based documents”; and
- Technology neutrality - which intends to “provide for the coverage of all factual situations (...) irrespective of the technology or the medium used” (Ng, 2018).

The simplicity of these guides could be instructive within the broad digital economy framework.
CONSUMER PROTECTION
It is vital to foster trust between consumers and e-commerce businesses, particularly because the buyer and seller are ‘displaced’. The key becomes dispute resolution mechanisms – both the businesses and payment gateways should provide avenues for this. Additional principles for prioritising consumer protection include:

- Fair business and advertising practices (think, for instance, about clarity in paid-for product placement in social media contexts);
- Appropriate and full disclosures (such as labelling);
- Effective processes for transaction confirmation and payment that focus on consumer clarity;
- Proactive measures to address privacy and security risks;
- Product safety across ecommerce supply chains;
- Consumer cooling-off periods; and
- Meaningful access to effective mechanisms to resolve disputes, which can include online dispute resolution (Centre for International Private Enterprise and New Markets Lab, 2018).

DIGITAL IDENTITY
Strong digital identity depends on an existing data protection framework that is both in place and implemented. Additionally drawing from the data protection reflections, “privacy by design” solutions can be obliged for fintech (and other) system designers incorporating digital identity solutions, guided by the World Bank’s “Principles on Identification for Sustainable Development”.

Bad identity systems may play a role in exclusion and even growth in lived inequalities for citizens. This reinforces the need for the institutional mechanisms that support data justice imperatives to be in place and sufficiently resourced, as a necessary support to digital identity enablers – which necessarily include DPAs. And institutional strength should result in lawful data processes and practices from every actor in the digital identity value chain, given its underpinning on personal identifying data, whether public or private sector.

E-TAXATION, DIGITAL TAXATION AND CUSTOMS POLICY
As has been addressed previously, taxation issues form a key component in creating and sustaining a healthy digital economy. A Model Law on the Digital Economy must be supported by broader financial and tax policies that can focus on enhancing domestic benefits, which can be included in digital industrial policies (Barnes et al., 2019).

In particular, these taxation challenges reinforce the need for African policymakers to actively engage in global governance debates on digital economy issues. Policymakers will be strengthened by improving and leveraging, the regional coordination activities being developed as part of AfCFTA, but also in the regional activities driven by the SADC across the spectrum of digital economy issues.

**Intellectual property and copyright**

**Key issues**

**THE INTERNET AND INTELLECTUAL PROPERTY**
Although most countries in the SADC had intellectual property laws imposed during colonisation, notably the 1911 Imperial Copyright Act in British colonies, intellectual property was not considered an important policy issue. In the aftermath of the Trade Related Aspects of Intellectual Property (TRIPS) agreement under the World Trade Organization, pressure was placed on developing countries to pass more extensive intellectual property laws. Policy space for SADC countries became increasingly constrained. Even the least developed countries (LDCs), which do not strictly speaking need to comply with TRIPS, experience trade pressure to pass new intellectual property laws. Laws on intellectual property, copyright and patent are intended to give incentives for innovation (Global Innovation Index, 2019). A methodology developed by the World Intellectual Property Organization (WIPO) was used to calculate the value of copyright industries to the South African economy as contributing 4% to overall national employment and 4.1% to the country’s GDP (Garnet, 2012). Much of the revenue generated by copyright and patents flows from developing countries to developed countries.

---

By design, the Internet is an information sharing system while intellectual property laws seek to control use of information. During the first decades of the growth of the Internet, until the mid 2000’s, this generated tension between early adopters of Internet technologies and content intermediaries whose business models relied on controlling access to content. The WIPO Copyright Treaty (the WCT) sought to change copyright law in response to the challenges of the Internet. New business models have emerged to remunerate content creation, including selling advertising alongside content that is available at no cost, for example, You Tube. Some of these business models analyse the data of individual users to target advertisements. Global policy debates are framed around the competing interests of the advertising platforms and the content intermediaries.

The policy challenge of copyright, and other intellectual property rights is to harmonise three policy imperatives: that copyright and other rights give creators incentives to create new works, the necessity of using existing work to create new works, and public interests that must not be unduly limited by exclusivity. The challenges in achieving this balance were in fact directly experienced in the United Kingdom’s Digital Economy Act making wide-ranging alterations to the copyright regime, which was later shelved in favour of a voluntary framework on infringement created in partnership with the private sector (Out-Law News, 2014).

As has been noted in much of the digital policy discussion, intellectual property components of the digital economy have heightened importance in the context of promoting cross-regional digital trade:

“The role of IP in cross-border trade cannot be overstated. Companies seeking to trade their goods internationally require assurances that their IP will be protected in foreign territories” (Nkomo, 2014).

But a major challenge within the digital economy has been trying to ensure that the value of copyright is realised by creators, rather than the online intermediaries who tend to be able to extract all the monetary value (UNCTAD, 2019). Creators and authors are often forced to cede all copyright to intermediaries to see any economic value from their creation (Baloyi, 2014). At the same time, a multiplicity of development and innovation ends can be met by implementing or building on existing knowledge products.

FLEXIBLE COPYRIGHT: FAIR USE, FAIR DEALING AND EDUCATION

Innovation relies on the freedom to find new uses of existing content. For example, a collection of thousands of photographs is needed to ‘train’ a machine learning algorithm to recognise a car. Flexibility in copyright law favours innovation. This flexibility is achieved through exceptions to and limitations on the exclusive rights given to copyright holders. AI and machine learning technologies rely on the mass interpretation and reading of digital materials. Innovators and entrepreneurs as well as established technology actors, are interested in these innovative uses being covered by exceptions to copyright (New, 2019). Creators rely on exceptions as they use existing work to create new work. For example, a filmmaker needs exceptions so that she is permitted to capture copyright works in the background when she is filming, ambient music, architecture, artwork on a wall, etc.

Some jurisdictions have developed a list of specific exceptions. Others take a more flexible approach with a general-purpose exception. Fair use is an open-ended exception in which the fairness of any use must be assessed with reference to four factors, which include the impact of the use on the market for the original work. Fair dealing provisions usually also include balancing tests, but are constrained to a closed list of possible uses. Some jurisdictions have very narrow, detailed exceptions. These have proven unable to adapt to rapidly changing technologies. Even fair dealing does not always keep pace with technology.

Exceptions such as fair use promote education and access to knowledge (de Beer, 2010). Fair use also facilitates access to knowledge for disabled communities by allowing content conversion to accessible formats without requiring permissions. The benefits of a more general exclusion provision such as a ‘fair use’ provision is that it allows for the courts to adapt notions of fairness flexibly to consider emerging technological questions. Fair dealing is a narrower concept from common law jurisdictions that tends to have a finite list of specific purposes that allow for an exception to stand (Schonwetter, 2006).
What was called distance education has already been transformed by the Internet. Because online education is asynchronous and place independent, it has considerable latent potential to meet the urgent need for greater education and training in the SADC. However, online education uses of copyright works often require new exceptions. In Africa, exceptions for online education must facilitate cross border online education.

NEW RIGHTS FOR THE INTERNET
The WIPO Copyright Treaty introduced new rights for creators for the digital environment. The author or successor in title is the only person who can authorise distribution of a literary or artistic work to the public. Authors also have the exclusive right of communicating the work to the public. This includes communication through digital means such as the Internet. This right includes making content available to a member of the public at a time and place chosen by her. In other words, a copyright holder can control who can access a work by streaming or download.

DIGITAL RIGHTS MANAGEMENT AND TECHNICAL PROTECTION MEASURES
Digital technologies have made copying and communicating information much easier. But this is a threat to business models that rely on exclusive control through copyright. The response developed in the 1990's was digital rights management and technical protection measures. Digital rights management systems are an attempt to provide automated ways to control access to copyright work while permitting some access to a customer or other user. “Technological Protection Measures” (TPMs) are often a component of a digital rights management system but are narrower in that they are ‘systems or applications which block access to and/or use of digital content on an absolute or conditional basis‘ (Schonwetter & Ncube, 2011). TPMs can be highly problematic since they are routinely used to block users from uses that are legally permitted. As a consequence, they upset the balance between exclusivity and use established by the legislature when exceptions are crafted, instead imposing a blanket prohibition on exceptional uses (Giblin, 2018).

However, TPMs have proven unable to stop technically adept infringers who infringe on a large scale. TPMs encrypt copyright content but to allow use of it, for example, to allow someone to play a streaming video, the content must be decrypted. Decryption requires providing the user with the decryption code. Thus, motivated technologically savvy actors can almost always circumvent decryption while lawful users of products mostly cannot. As a consequence of this inherent weakness of TPMs, those who deploy them demanded that laws criminalise circumvention. The WIPO Copyright Treaty requires that countries that accede to the treaty agree to prohibit circumvention. However anti-circumvention rules do not need to criminalise circumvention nor does the WCT require that TPMs thwart exceptions. If they are carefully crafted, anti-circumvention measures can counter circumvention of TPMs to prevent infringement without preventing uses authorised by exceptions.

Together TPMs and anti-circumvention laws have been implicated in preventing the owners of digitally enabled devices from repairing and securing their devices (Perzanowski & Schultz, 2015).

CONTRACTING OUT OF EXCEPTIONS
As discussed above, many websites impose contracts of adhesion on users. Some of these contracts claim to bind users from exercising the exceptions and limitations established as part of the balance of copyright law. Like TPMs these contract provisions seek to impose an absolute ban on exceptional uses. However, copyright laws have begun to include provisions that these kinds of contract provisions are unenforceable.31 Given the power disparities that characterise contracts of adhesion, these should not be permitted to prevent uses authorised by law through exceptions and limitations.

AI AND COPYRIGHT
Machine learning, a type of AI technology, uses vast training sets. Training sets may be made up of computer-generated data, but some machine learning software is trained on photographs, software and video, all of which are subject to copyright. During the process, humans do not see the photos or videos nor examine the code of the software. The majority of the outputs of these uses do not resemble the data that they use. Does the use of copyright works to train AI require permission from the copyright holder under current copyright law? Should copyright do so? Machine learning technologies require such large sets that obtaining this permission would be practically impossible for all but a handful of global corporations.

31 For example, the United Kingdom Copyright, Designs and Patents Act 1988 states in Section 29A(5) “To the extent that a term of a contract purports to prevent or restrict the making of a copy which, by virtue of this section, would not infringe copyright, that term is unenforceable.”
Requiring permission would inhibit the development of AI capacity in the SADC. Some jurisdictions, which do not clearly permit use of works for machine learning, propose special exceptions for advanced information analysis.32

But AI algorithms, trained on a vast training set of existing works can generate similar outputs. For example, deep learning systems trained on a corpus of music can generate sound files that humans experience as music (Ramasubbareddy et al., 2019). Is there copyright in the output of AI systems? If so, then who owns it? Should the use of copyright works to train algorithms that generate output that effectively competes with the authors of the original work require copyright permission? These questions are already being debated by the WIPO (WIPO, 2019). However, the debate largely ignores how the answers to these questions might affect developing countries (Research ICT Africa, 2020). Authors, artists and musicians in developing countries are threatened with having to compete with music and art generated by AI systems. The African Regional Intellectual Property Organization (ARIPO) Model Law on Copyright and Related Right (2019) defines an author as a natural person, i.e., a human. Building on this approach, copyright law could stipulate that only creative original works made by natural persons enjoy copyright.

SOFTWARE AND BUSINESS METHOD PATENTS
Software is automatically subject to copyright protection but many producers of software permit use under an open source licence. The world of software has been strongly influenced by the prevalence of open source that underpins much of the developer culture and is demonstrated in GitHub (which provides access to significant amounts of open code) (Valimakki, n.d.). With the exception of a few countries, most do not allow software to be patented. Similarly, most countries do not allow methods, including business methods to be patented. The vast majority of patents obtained in SADC countries are not owned by SADC companies, individuals or governments. One study of patenting in South Africa found that in the period of 2005 to 2015, only 10% of patents were obtained by South Africans, most being owned by corporations from outside the SADC (Berger & Rens, 2018). Where patents cover software or business methods, even though patents over these should not be granted, they inhibit Southern African entrepreneurs who may lack the resources needed for a legal challenge. Inevitably, too, questions on patents raise the spectre of abuse of patent processes by agents that are not necessarily creators but are able to manipulate the legal system by scouring for unprotected works to lay claim to (ITU, 2011).

AI technologies can be used to generate inventions and to mass generate patent claims. Some are already arguing that AIs should be listed as inventors. This development seems likely to negatively affect the percentage of patents obtained by Southern Africans within the SADC and globally. However, AI can also be deployed to examine patents and by comparing an application to existing patents, journal articles and other sources more quickly and easily than a human examiner determine whether a patent application is in fact novel. The technologies involved are changing rapidly, but one policy intervention is for patent law to require applicants for patents to disclose whether and how AI was deployed in developing the invention. This will provide policy makers with information to formulate a response to these developments.

ENFORCEMENT CHALLENGES AND CONTENT PROVIDERS
Fundamentally, the Internet is designed to enable access to content through linking content easily and en masse in what is largely an act of copying. And the nature of modern piracy draws telecommunications and Internet stakeholders increasingly into conversations about IP and copyright (ITU, 2011). Necessarily then, telecommunications regulators are drawn into many discussions to help enact enforcement, as are Internet intermediaries.

CYBERSECURITY AND CYBERCRIME
Contract has traditionally played a strong role in efforts to protect commercially sensitive knowledge with physical security used to prevent external threats. However, the digital realm – and the very nature of the types of intangible property IP seeks to protect – mean that cyber espionage and warfare become emerging threats to trying to preserve economic value for businesses (Dowdy, undated). These threats highlight the need for multi stakeholder engagement and intervention, as such acts have both a socio-political and systematic economic impact that extends beyond individual businesses (Dowdy, undated).

SADC review

DOMESTIC LEGAL FRAMEWORKS ON IP AND COPYRIGHT
All SADC jurisdictions have a form of copyright and patent legislation with a strong tendency to have the laws framed within an industrial and commercial context. Contextual examinations seem to imply that the challenges do not necessarily lie with a lacuna in legal instruments, but rather in the accessibility of those instruments to allow for creators and innovators to derive value (as well as insufficient enabling environments for innovation more broadly) (Phiri, 2008). Research across the continent suggests that most African countries have sufficient rights for creators, but lack appropriate exceptions and limitations (Armstrong et al., 2010).

REGIONAL INTEGRATIONS
SADC as a trading bloc is well-suited to intellectual property and Copyright coordination (Nkomo, 2014) and may be able to overcome some shortcomings experienced by the African Regional Intellectual Property Organization (ARIPO) (such as an inability to enforce remedies for rights issued under ARIPO) (Nkomo, 2014). A number of SADC countries including South Africa, Angola, Mozambique and Madagascar are not members.

Principled recommendations

AI AND INTELLECTUAL PROPERTY
Although this is a relatively new challenge for policy, the stakes for innovators and entrepreneurs are high. Proactive steps include:

- Establishing that copyright vests only in the creative products of human authors.
- Permitting the use of copyright works to enable advanced information analysis such as training AI algorithms.
- Requiring patent applicants to disclose the use of AI in developing inventions.

EXCEPTIONS TO COPYRIGHT
Because copyright exists automatically, the establishment of when exceptions to the blanket rules apply becomes the most significant point of intersection for law. International instruments (Berne Convention, 1886) have essentially established a three-factor test, sometimes referred to as a three-step test, outlining that exceptions and limitations to exclusive rights are permissible:

1) in certain special cases; 
2) that do not conflict with the normal exploitation of the work; and
3) do not unreasonably prejudice the legitimate interests of the author/rights holder. While the precise meaning of each of the steps remains disputed, the test can perhaps best be summarised and clarified as follows: Copyright exceptions and limitations are permissible if they (1) are not unduly vague, (2) do not deprive the rights holders of tangible income in areas in which rights holders normally obtain such income from copyright, and (3) do not harm the interests of the rights holders in a disproportional way.

These exceptions should seek to incorporate public policy considerations and, within both the digital and development context, should strongly focus the role of the expansion of education and inclusion of citizens to help combat the inequality challenges that can arise in the digital economy context. As noted by Nwauche (Pistorius & Mwim, 2019):

The appropriate response of developing countries, including African countries to the WIPO digital treaties has attracted the attention of individuals and groups alike. The fact that there is no agreed consensus on the expression of exceptions and limitations at the international level under the Berne framework and under the WIPO digital treaties underscores the point that they ought to be created in response to the circumstances of each nation. A national response expresses the needs and aspirations of each country. An analysis of the human rights obligations of African countries must have a significant impact on these exceptions and limitations.
Fair use provisions and fair dealings provisions can then exist as more general and flexible exclusions, which apply when no other copyright limitation is available (Schonwetter & Ncube, 2011). This allows for flexibility within a rapidly evolving technological world.

In addition to all-purpose exceptions, certain specific exceptions are important for the digital economy:

- Exceptions to enable online learning.
- Exceptions for cross border use of content that includes content used under an exception in the country of origin.
- Exceptions to enable interoperability of ICT systems.
- Exceptions to enable the repair and securing of things that incorporate software.

ENFORCEMENT MECHANISMS

Regardless of how exceptions may be phrased, a key consideration is creating avenues for creators to exercise their rights to profit from their work. Harmonisation remains important, as does rights education and access to justice mechanisms (issues that can be dealt with through guided regulation).

INTERNET CONNECTED DEVICES

There should be particular security considerations in place for IoTs. For instance, requirements can be created that oblige Internet connected devices to have a password unique to the device, which can be changed by the user. There should also be positive obligations on the supplier of an Internet connected device to supply a contact point for notification of security issues.

SERVICE PROVIDER LIABILITY

Service Providers should be granted limitations on liability. For Service Providers involved in hosting content, limited liability should be conditional on compliance with a notice and notice requirement in which complaints are addressed to the Service Provider, and which in turn gives notice to the person who uploaded the content. If the person who uploaded the content admits the complaint, or fails to respond, the Service Provider can then remove the content. If the person who uploaded the content contests the complaint, the Service Provider gives notice to the complainant of the uploader's contact details and defence. The complainant can then approach a court or other dispute resolution body for resolution of the complaint.
Complexity and legislation make for uncomfortable bedfellows. However, both the immense opportunities for African citizens and governments in good digital economy progress (weighed against the specific risks present for Africa, if the enabling legislative and policy frameworks are not in place) necessitate embracing active participation in global contexts, with considered application to our domestic conditions.

Digital inequalities in SADC highlight the need for consideration of the broader enabling and inhibiting necessities for a global digital economy. Many of these, like universal ICT access, were called for prior to the 4IR - even electrical power, the basis of the second Industrial Revolution, is often lacking or unreliable in some SADC member countries. And the COVID-19 crisis has reinvigorated the urgent need to deal with these fundamentals. The emergence of the 4IR has, however, created a more urgent requirement for data governance frameworks, given the massive expansions (and centralities) of data in the emerging digital industrial production.

A further important aspect of the experienced inequalities in the African context is the hijacking of value from digital advancement. The economic value of data and digital services and developments are extracted to the benefit of countries and businesses largely outside of the region, and significantly monopolised.

Many of the enabling and inhibiting factors will necessitate coordinated policy interventions, which this Discussion Paper has highlighted in order to help in the coordination between policymakers and lawmakers. However, as our Digital Economy Model Law Framework (Figure 11) demonstrates, the law has a central role to play in pursuing a good digital economy. Not least of all, human rights principles present a key mechanism for aligning socio-political objectives within economic policy.

When we consider the variety of potential policy areas of relevance to the digital economy, certain patterns emerge consistently across areas:

- **Complexity** - the environment involves not only a variety of stakeholders, but also a variety of issues that overlap and diverge. This systems complexity increases the risks of unintended consequences through overly prescriptive law-making, especially when not sufficiently context specific.
- **Co-ordination** - as the digital economy covers many policy areas, there is a need for effective inter-ministerial and public private coordination.
- **Co-operation** - many of the potential dividends of a good digital economy are sourced from the globalised and inter-connected nature of the Internet, underpinned by the cross-border intermission of data. Co-operation between domestic jurisdictions is required not as a component of data regulation and broader digital economy imperatives, but also to facilitate intra-regional trade. And, in order to manage complexity domestically, facilitating effective co-ordination between departments, and relevant stakeholders, is also required.
- **Balancing of interests** - the variety of stakeholders involved often have divergent interests in the pursuit of a beneficial digital economy. Human rights norms become essential for providing frames in which these competing interests can be balanced in a legislative paradigm.
- **Regulation** - regulation is necessary, but capacitated Regulators provide an opportunity for sectoral responsiveness that can assist in compliance burdens for the private sector, whilst encouraging multi-stakeholder participation in broader governance.
- **Harmonisation** - associated with co-ordination, harmonisation should not be misconstrued as replication. Creating harmony between legislative and policy realms highlight the role principle-based law and regulation can assist in this harmonisation.
- **Trust** - an important underlying imperative across digital economy areas is ensuring trust in the digital environment that can facilitate beneficial digital economic activity. This trust can be fostered by both the creation of sound rights-based digital governance frameworks that citizens, businesses and consumers witness being implemented.
- **Monopolisation** - while there are a variety of risks involved in considering policy in this area, monopolisation becomes a specific risk due to the datafication reality of the digital economy.
- **Inequality** - inequalities in the experience of digital dividends have marred experiences of the digital economy in the region. Any interventions must be designed with this central risk (and impact) at the fore. In order for the digital economy to equitably provide digital dividends, law making must consider the full extent to which inequalities are experienced, so that development criteria can be meaningfully incorporated into policy that does not just express economic imperatives.
While some patterns emerge from a more globalised consideration of the digital economy, there are specific realities of the digitalisation and datafication that must be considered within law making that helps to fulfil development aims. Internet penetration is still insufficient to provide a properly supportive basis for an emerging digital economy.

The full consideration in the introduction and contexts bring to the fore that objectives should not just seek to encourage the digital economy, as encouraging the digital economy ‘as is’ will only increase digital risks. Instead, the objective should be to create law and policy that promotes a ‘good’ digital economy, which is a digital economy defined by:

- Inclusiveness,
- Human rights objectives,
- Competitiveness,
- Openness,
- Regulation and planning,
- Flexibility, and
- Enabled domestic markets.

This will be essential if SADC is to create and capture value in the evolving digital economy and not be a passive recipient or even be excluded. To achieve this, it is necessary to establish principles that can form the basis of law-making within domestic contexts, cognisant of regional collaboration objectives and the foundations of a good digital economy that can benefit all.
Reference List


Gomes-Lund et al. (Guerrilha do Arcaúia) v. Brazil. Inter-American Court of Human Rights (IACRH), 24 November 2010.


Industrial Development Think Tank. (2019). Towards a Digital Industrial Policy for South Africa: A Review of the Issues. CCRED. Available at: https://static1.squarespace.com/static/52246331e4b0a6e5f1b8ce5f5/5d355997ae8b0f4001ee2906/1563777435535/DPIP_Final.pdf.

The Digital Economy and Society


Retrofit (Pvt) Ltd v Posts and Telecommunications Corporation (Attorney-General of Zimbabwe Intervening) 1996 (1) SA 847 (ZS).


UN Human Rights Committee. (2011). General comment no. 34, Article 19, Freedoms of opinion and expression, 12 September 2011, CCPR/C/65/34. Available at: https://www.refworld.org/docid/4ed34b562.html


ZLHR and MISA Zimbabwe v Minister of State for National Security and Others Case No. 265/19.

STATUTE AND OTHER INSTRUMENTS
Access to Information and Protection of Privacy Act (Zimbabwe), 2002.


Data Protection Act (Lesotho), 2013.


Draft Model Law on Cybercrime and Cybersecurity (SADC), 2013.


Model Law on Copyright and Related Rights (ARIPO).

Protection of Personal Information Act (South Africa), 2010.

ANNEXURES
Annexure 1: Relevant African Regional Instruments

Annexure 1A: Key international, regional and sub-regional instruments for digital rights in SADC

<table>
<thead>
<tr>
<th>INSTRUMENT</th>
<th>YEAR</th>
<th>APPLICABLE SADC COUNTRIES</th>
<th>BINDING?</th>
</tr>
</thead>
<tbody>
<tr>
<td>African Charter on Human and Peoples’ Rights</td>
<td>1986</td>
<td>All</td>
<td>Yes</td>
</tr>
<tr>
<td>African Union Convention on Cyber-security and Personal Data Protection</td>
<td>2014</td>
<td>Comoros (signatory), Mauritius (ratified), Mozambique (signatory)</td>
<td>No, currently insufficient ratifications</td>
</tr>
<tr>
<td>(Malabo Convention)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Council of Europe Convention for the Protection of Individuals with regard</td>
<td>1981</td>
<td>Mauritius</td>
<td>Yes</td>
</tr>
<tr>
<td>to Automatic Processing of Personal Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional Protocol to the Convention for the Protection of Individuals</td>
<td>2001</td>
<td>Mauritius</td>
<td>Yes</td>
</tr>
<tr>
<td>with regard to Automatic Processing of Personal Data, regarding supervisory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorities and transborder data flows.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Council of Europe Convention on Cybercrime (Budapest Convention)</td>
<td>2001</td>
<td>Mauritius (ratified), South Africa (signatory)</td>
<td>Yes</td>
</tr>
<tr>
<td>International Covenant on Civil and Political Rights</td>
<td>1966</td>
<td>All except: Comoros (signatory)</td>
<td>Yes</td>
</tr>
<tr>
<td>International Covenant on Economic, Social and Cultural Rights</td>
<td>1966</td>
<td>All, except: Comoros (signatory), Botswana (not signed), Mozambique (not signed)</td>
<td>Yes</td>
</tr>
<tr>
<td>Southern African Development Community Protocol on Transport, Communications and Meteorology</td>
<td>1996</td>
<td>All</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Annexure 1B: Key international, regional and sub-regional principles and guidelines for digital rights in SADC

<table>
<thead>
<tr>
<th>INSTITUTIONAL HOME</th>
<th>TITLE</th>
<th>YEAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>African Union</td>
<td>Declaration on Internet Governance</td>
<td>2018</td>
</tr>
<tr>
<td>African Union</td>
<td>Declaration of Principles on Freedom of Expression in Africa</td>
<td>2002</td>
</tr>
<tr>
<td>African Union</td>
<td>Declaration on Internet Governance</td>
<td>2018</td>
</tr>
<tr>
<td>African Union</td>
<td>Model Law on Access to Information</td>
<td>2013</td>
</tr>
<tr>
<td>African Union Commission and Internet Society</td>
<td>Personal Data Protection Guidelines for Africa</td>
<td>2018</td>
</tr>
<tr>
<td>Civil Society</td>
<td>African Declaration on Internet Rights and Freedoms</td>
<td>2016</td>
</tr>
<tr>
<td>Civil Society</td>
<td>Manila Principles on Intermediary Liability</td>
<td>2015</td>
</tr>
<tr>
<td>Southern African Development Community</td>
<td>Draft Model Law on Data Protection</td>
<td>2013</td>
</tr>
<tr>
<td>Southern African Development Community</td>
<td>Draft Model Law on Electronic Transactions and Electronic Communications</td>
<td>2013</td>
</tr>
<tr>
<td>Southern African Development Community</td>
<td>Declaration on Information and Communications Technology</td>
<td>2001</td>
</tr>
<tr>
<td>Southern African Development Community</td>
<td>Mobile Money Guidelines</td>
<td>2016</td>
</tr>
<tr>
<td>United Nations</td>
<td>Guiding Principles on Business and Human Rights (Ruggie Principles)</td>
<td>2011</td>
</tr>
<tr>
<td>United Nations, General Assembly</td>
<td>The right to privacy in the digital age</td>
<td>2013</td>
</tr>
</tbody>
</table>
## Annexure 2: SADC Constitutional Mapping

### Annexure 2A: Right to Privacy

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>SECTION</th>
<th>PRIVACY</th>
<th>TEXT</th>
<th>NOTE</th>
</tr>
</thead>
</table>
| **ANGOLA**               | Article 32 | Right to identity and privacy | 1. The right to personal identity, civil capacity, nationality, a good name and reputation, likeness, free speech, and privacy in personal and family life shall be recognised for all.  
2. The law shall establish effective guarantees against the procurement and use of information relating to individuals and families in a manner, which is abusive or offends against human dignity. | Some reference to information privacy in the context of dignity. |
| **BOTSWANA**             | Article 9 | Protection of privacy of home and other property | 1. Except with his or her own consent, no person shall be subjected to the search of his or her person or his or her property or the entry by others on his or her premises.  
2. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision...[limitations provided]. | Reference to privacy of the home and property, not in relation to information. |
| **COMOROS**              | Preamble |                                             | The Comorian people solemnly affirm their will...  
They proclaim: ...the inviolability of the domicile in the conditions defined by law;  
This Preamble shall be considered an integral part of the Constitution. | Reference to privacy of the home and property, not in relation to information. |
| **DEMOCRATIC REPUBLIC OF CONGO** | Article 31 | All persons have the right to the respect of their private life and to the secrecy of their correspondence, of telecommunications and of any other form of communication. This right may only be infringed in the cases specified by the law. | Reference to personal and communication privacy. |
| **LESOTHO**              | Article 4, 11, 14 | Fundamental human rights and freedoms | 1. Whereas every person in Lesotho is entitled, whatever his race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status to fundamental human rights and freedoms, that is to say, to each and all of the following— ...  
b. the right to personal liberty; ...  
g. the right to respect for private and family life; ...  
j. freedom of expression ...  
Article 11. Right to respect for private and family life | 1. Every person shall be entitled to respect for his private and family life and his home.  
2. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision—  
a. in the interests of defence, public safety, public order, public morality or public health; or  
b. for the purpose of protecting the rights and freedoms of other persons. ....  
Article 14. Freedom of expression | 1. Every person shall be entitled to, and (except with his own consent) shall not be hindered in his enjoyment of freedom of expression, including freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons) and freedom from interference with his correspondence.  
2. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision—  
a. in the interests of defence, public safety, public order, public morality or public health; or  
b. for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the courts, or regulating the technical administration or the technical operation of telephony, telegraphy, posts, wireless broadcasting or television; or  
c. for the purpose of imposing restrictions upon public officers. .... | Reference to personal and information privacy (in a freedom of expression context). |
<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>SECTION</th>
<th>PRIVACY</th>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>MADAGASCAR</td>
<td>Article 13</td>
<td>Any individual is assured of the inviolability of their person, their domicile and of the secrecy of their correspondence. ...</td>
<td>Reference to personal and communications privacy.</td>
</tr>
<tr>
<td>MALAWI</td>
<td>Article 21</td>
<td>Every person shall have the right to personal privacy, which shall include the right not to be subject to—</td>
<td>Reference to personal and communications privacy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. searches of his or her person, home or property;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. the seizure of private possessions; or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>c. interference with private communications, including mail and all forms of telecommunications.</td>
<td></td>
</tr>
<tr>
<td>MAURITIUS</td>
<td>Article 3, 9</td>
<td>It is hereby recognised and declared that in Mauritius there have existed and shall continue to exist without discrimination by reason of race, place of origin, political opinions, colour, creed or sex, but subject to respect for the rights and freedoms of others and for the public interest, each and all of the following human rights and fundamental freedoms ...</td>
<td>Reference to privacy of the home and property, not in relation to information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>c. the right of the individual to protection for the privacy of his home and other property and from deprivation of property without compensation, and the provisions of this Chapter shall have effect for the purpose of affording protection to those rights and freedoms subject to such limitations of that protection as are contained in those provisions, being limitations designed to ensure that the enjoyment of those rights and freedoms by any individual does not prejudice the rights and freedoms of others or the public interest.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Article 9</td>
<td>Protection for privacy of home and other property</td>
<td>Reference to privacy of the home and property, not in relation to information.</td>
</tr>
<tr>
<td></td>
<td>1. Except with his own consent, no person shall be subjected to the search of his person or his property or the entry by others on his premises.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. in the interests of defence, public safety, public order, public morality, public health, town and country planning, the development or utilisation of mineral resources or the development or utilisation of any other property in such a manner as to promote the public benefit;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. for the purpose of protecting the rights or freedoms of other persons;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. to enable an officer or agent of the Government or a local authority, or a body corporate established by law for a public purpose, to enter on the premises of any person in order to value those premises for the purpose of any tax, rate or due, or in order to carry out work connected with any property that is lawfully on those premises and that belongs to the Government, the local authority or that body corporate, as the case may be; or</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. to authorise, for the purpose of enforcing the judgment or order of a court in any civil proceedings, the search of any person or property by order of a court or the entry upon any premises by such order, except so far as that provision or, as the case may be, the thing done under its authority is shown not to be reasonably justifiable in a democratic society.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MOZAMBIQUE</td>
<td>Right 40, 71</td>
<td>All citizens shall have the right to their honour, good name and their reputation, as well as the right to defend their public image and to protect their privacy.</td>
<td>Reference to information privacy and, noteworthy, data privacy.</td>
</tr>
<tr>
<td></td>
<td>Article 71</td>
<td>Use of computerised data</td>
<td>Reference to information privacy and, noteworthy, data privacy.</td>
</tr>
<tr>
<td></td>
<td>1. The use of computerised means for recording and processing individually identifiable data in respect of political, philosophical or ideological beliefs, of religious faith, party or trade union affiliation or private lives, shall be prohibited.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. The law shall regulate the protection of personal data kept on computerised records, the conditions of access to data banks, and the creation and use of such data banks and information stored on computerised media by public authorities and private entities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Access to data bases or to computerised archives, files and records for obtaining information on the personal data of third parties, as well as the transfer of personal data from one computerised file to another that belongs to a distinct service or institution, shall be prohibited except in cases provided for by law or by judicial decision.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. All persons shall be entitled to have access to collected data that relates to them and to have such data rectified.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>COUNTRY</td>
<td>SECTION</td>
<td>PRIVACY</td>
<td>NOTE</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td><strong>NAMIBIA</strong></td>
<td>Article 13</td>
<td>Privacy</td>
<td>Reference to personal and communications privacy.</td>
</tr>
<tr>
<td></td>
<td>1. No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Searches of the person or the homes of individuals shall only be justified:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. where these are authorised by a competent judicial officer;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. in cases where delay in obtaining such judicial authority carries with it the danger of prejudicing the objects of the search or the public interest, and such procedures as are prescribed by Act of Parliament to preclude abuse are properly satisfied.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SEYCHELLES</strong></td>
<td>Article 20</td>
<td></td>
<td>Reference to personal and communications privacy.</td>
</tr>
<tr>
<td></td>
<td>1. Every person has a right not to be subjected--</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. without the consent of that person, to the search of the person or property or premises of that person or to the lawful entry by others on the premises of that person;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. without the consent of the person or an order of the Supreme Court, to the interception of the correspondence or other means of communication of that person either written, oral or through any medium.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SOUTH AFRICA</strong></td>
<td>Section 14</td>
<td></td>
<td>Reference to personal and communications privacy.</td>
</tr>
<tr>
<td></td>
<td>Everyone has the right to privacy, which includes the right not to have</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. their person or home searched;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. their property searched;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. their possessions seized; or</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. the privacy of their communications infringed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SWAZILAND</strong></td>
<td>Article 14, 22</td>
<td></td>
<td>Reference to privacy of the home and some communications privacy.</td>
</tr>
<tr>
<td></td>
<td>Article 14. Fundamental rights and freedoms of the individual</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. The fundamental human rights and freedoms of the individual enshrined in this Chapter are hereby declared and guaranteed, namely --</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. protection of the privacy of the home and other property rights of the individual;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. protection of the privacy of the home and other property rights of the individual;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Article 22. Protection against arbitrary search or entry</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. A person shall not be subjected –</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. to the search of the person or the property of that person;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. to the entry by others on the premises of that person;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. to the search of the private communications of that person, except with the free consent of that person first obtained.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TANZANIA</strong></td>
<td>Article 16</td>
<td></td>
<td>Reference to personal privacy and communications privacy.</td>
</tr>
<tr>
<td></td>
<td>Article 16. Right to privacy and personal security</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. For the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of his person, his property and residence may be encroached upon without prejudice to the provisions of this Article.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ZAMBIA</strong></td>
<td>Article 11, 17</td>
<td>Fundamental rights and freedoms</td>
<td>Reference to privacy of the home and property, not in relation to information.</td>
</tr>
<tr>
<td></td>
<td>It is recognised and declared that every person in Zambia has been and shall continue to be entitled to the fundamental rights and freedoms of the individual, that is to say, the right, whatever his race, place of origin, political opinions, colour, creed, sex or marital status, but subject to the limitations contained in this Part, to each and all of the following, namely:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. protection for the privacy of his home and other property and from deprivation of property without compensation;</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ZIMBABWE</strong></td>
<td>Article 57</td>
<td>Right to privacy</td>
<td>Reference to personal privacy and communications privacy.</td>
</tr>
<tr>
<td></td>
<td>Every person has the right to privacy, which includes the right not to have--</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. their home, premises or property entered without their permission;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. their person, home, premises or property searched;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. their possessions seized;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. the privacy of their communications infringed; or</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. their health condition disclosed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Annexure 2B: Right to Access Information

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>ACCESS TO INFORMATION</th>
<th>TEXT</th>
</tr>
</thead>
</table>
| ANGOLA Article 40     | Article 40. Freedom of expression and information  
1. Everyone shall have the right to freely express, publicise and share their ideas and opinions through words, images or any other medium, as well as the right and the freedom to inform others, to inform themselves and to be informed, without hindrance or discrimination.  
2. The exercise of the rights and freedoms described in the previous point may not be obstructed or limited by any type or form of censorship.  
3. Freedom of expression and information shall be restricted by the rights enjoyed by all to their good name, honour, reputation and likeness, the privacy of personal and family life, the protection afforded to children and young people, state secrecy, legal secrecy, professional secrecy and any other guarantees of these rights, under the terms regulated by law.  
4. Anyone committing an infraction during the course of exercising freedom of expression and information shall be held liable for their actions, in disciplinary, civil and criminal terms, under the terms of the law.  
5. Under the terms of the law, every individual and corporate body shall be assured the equal and effective right of reply, the right to make corrections, and the right to compensation for damages suffered. |
| BOTSWANA Article 12   | Article 12. Protection of freedom of expression  
1. Except with his or her own consent, no person shall be hindered in the enjoyment of his or her freedom of expression, that is to say, freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference (whether the Copyright Government of Botswana communication be to the public generally or to any person or class of persons) and freedom from interference with his or her correspondence.  
2. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision-  
   a. that is reasonably required in the interests of defence, public safety, public order, public morality or public health; or  
   b. that is reasonably required for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the courts, regulating educational institutions in the interests of persons receiving instruction therein, or regulating the technical administration or the technical operation of telephony, telegraphy, posts, wireless, broadcasting or television; or  
   c. that imposes restrictions upon public officers, employees of local government bodies, or teachers, and except so far as that provision or, as the case may be, the thing done under the authority thereof is shown not to be reasonably justifiable in a democratic society. |
| COMORES Preamble      | Preamble  
The Comorian people solemnly affirm their will  
... the right to obtain information from a variety of sources and to freedom of the press;  
...This Preamble shall be considered an integral part of the Constitution. |
| DEMOCRATIC REPUBLIC OF CONGO Article 24, 27 | Article 24.  
All persons have the right to information.  
The freedom of the press, the freedom of information and of broadcasting by radio and television, the written press or any other means of communication are guaranteed, under reserve of respect for the law, for public order, for morals and for the rights of others.  
The law determines the modalities of exercise of these freedoms.  
Article 27.  
All Congolese have the right to address, individually or collectively, a petition to the public authority, which responds to it within three months.  
No one may be made the subject of discrimination, in any form that may be, for having taken such an initiative.  
The audio-visual and written media of the State are public services the access to which is guaranteed in an equitable manner to all the political and social movements. The status of the media of the State is established by the law, which guarantees the objectivity, the impartiality and the pluralism of opinion in the treatment and diffusion of information. |
| LESOTHO Article 14    | Article 4. Fundamental human rights and freedoms  
1. Whereas every person in Lesotho is entitled, whatever his race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status to fundamental human rights and freedoms, that is to say, to each and all of the following—  
   j. freedom of expression;  
Article 14. Freedom of expression  
1. Every person shall be entitled to, and (except with his own consent) shall not be hindered in his enjoyment of, freedom of expression, including freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons) and freedom from interference with his correspondence. |
<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>SECTION</th>
<th>TEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>MADAGASCAR</td>
<td>Article 10, 11</td>
<td>Article 10. The freedoms of opinion and of expression, of communication, of the press, of association, of assembly, of circulation, of conscience and of religion are guaranteed to all and may only be limited by the respect for the freedoms and rights of others, and by the imperative of safeguarding the public order, the national dignity and the security of the State. Article 11. Any individual has the right to information. Information under all its forms is not submitted to any prior constraint, except that which infringes the public order and the morality. The freedom of information, whatever the medium, is a right. The exercise of this right includes duties and responsibilities, and is submitted to certain formalities, conditions, or sanctions specified by the law, which are the measures necessary in a democratic society. All forms of censorship are prohibited. The law organizes the exercise of the profession of journalist.</td>
</tr>
<tr>
<td>MALAWI</td>
<td>Article 34, 35, 36, 37</td>
<td>Article 34. Freedom of opinion Every person shall have the right to freedom of opinion, including the right to hold, receive and impart opinions without interference. Article 35. Freedom of expression Every person shall have the right to freedom of expression. Article 36. Freedom of the press The press shall have the right to report and publish freely, within Malawi and abroad, and to be accorded the fullest possible facilities for access to public information. Article 37. Access to information Every person shall have the right of access to all information held by the State or any of its organs at any level of Government in so far as such information is required for the exercise of his or her rights.</td>
</tr>
<tr>
<td>MAURITIUS</td>
<td>Article 3, 12</td>
<td>Article 3. Fundamental rights and freedoms of the individual It is hereby recognised and declared that in Mauritius there have existed and shall continue to exist without discrimination by reason of race, place of origin, political opinions, colour, creed or sex, but subject to respect for the rights and freedoms of others and for the public interest, each and all of the following human rights and fundamental freedoms ... b. freedom of conscience, of expression, of assembly and association and freedom to establish schools, and ... Article 12. Protection of freedom of expression 1. Except with his own consent, no person shall be hindered in the enjoyment of his freedom of expression, that is to say, freedom to hold opinions and to receive and impart ideas and information without interference, and freedom from interference with his correspondence. .....</td>
</tr>
<tr>
<td>MOZAMBIQUE</td>
<td>Article 48, 49, 71, 253</td>
<td>Article 48: Freedom of expression and information 1. All citizens shall have the right to freedom of expression and to freedom of the press, as well as the right to information, 2. The exercise of freedom of expression, which consists of the ability to impart one's opinions by all lawful means, and the exercise of the right to information shall not be restricted by censorship. 3. Freedom of the press shall include, in particular, the freedom of journalistic expression and creativity, access to sources of information, protection of independence and professional secrecy, and the right to establish newspapers, publications and other means of dissemination. 4. In the public sector media, the expression and confrontation of ideas from all currents of opinion shall be guaranteed. 5. The State shall guarantee the impartiality of the public sector media, as well as the independence of journalists from the Government, the Administration and other political powers. 6. The exercise of the rights and freedoms provided for in this article shall be governed by law on the basis of the imperative respect for the Constitution and for the dignity of the human person.. Article 49: Broadcasting rights, right of reply and of political response 1. Political parties shall, according to their degree of representation and to criteria prescribed by law, have the right to broadcasting time on public radio and television services. 2. Political parties that have seats in the Assembly of the Republic but are not members of Government shall, in terms of the law and according to their degree of representation, have the right to broadcasting time on public radio and television services in order to exercise their right of reply and the right to respond to the political statements of the Government. 3. Trade unions, professional organisations and organisations representing social and economic activities shall also be guaranteed broadcasting rights, according to criteria prescribed by law. 4. During election periods, contestants shall have the right to regular and equitable broadcasting time on public radio and television stations of national or local range, within the terms of the law. Article 71. Use of computerised data 1. The use of computerised means for recording and processing individually identifiable data in respect of political, philosophical or ideological beliefs, of religious faith, party or trade union affiliation or private lives, shall be prohibited. 2. The law shall regulate the protection of personal data kept on computerized records, the conditions of access to data banks, and the creation and use of such data banks and information stored on computerised media by public authorities and private entities. 3. Access to data bases or to computerised archives, files and records for obtaining information on the personal data of third parties, as well as the transfer of personal data from one computerised file to another that belongs to a distinct service or institution, shall be prohibited except in cases provided for by law or by judicial decision. 4. All persons shall be entitled to have access to collected data that relates to them and to have such data rectified. Article 253. Rights and guarantees of citizens 1. Citizens shall have the right to receive information from the competent Public Administration services, whenever they request it, on the progress of processes in which they have a direct interest, in terms of the law. 2. Interested parties shall be notified of administrative acts within the terms and the time limits established by law, and reasons for these acts shall be given whenever they affect the rights or interests of legally entitled citizens. 3. Interested citizens shall be guaranteed the right to judicial appeal against the illegality of administrative acts that endanger their rights.</td>
</tr>
<tr>
<td>COUNTRY</td>
<td>SECTION</td>
<td>TEXT</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| NAMIBIA      | Article 21 | **Article 21. Fundamental Freedoms**  
1. All persons shall have the right to:  
   a. freedom of speech and expression, which shall include freedom of the press and other media; …  
|             |          | **Article 22.**  
1. Every person has a right to freedom of expression and for the purpose of this article this right includes the freedom to hold opinions and to seek, receive and impart ideas and information without interference.  
2. The right under clause (1) may be subject to such restrictions as may be prescribed by a law and necessary in a democratic society-  
   a. in the interest of defence, public safety, public order, public morality or public health;  
   b. for protecting the reputation, rights and freedoms or private lives of persons;  
   c. for preventing the disclosure of information received in confidence;  
   d. for maintaining the authority and independence of the courts or the National Assembly;  
   e. for regulating the technical administration, technical operation, or general efficiency of telephones, telegraphy, posts, wireless broadcasting, television, or other means of communication or regulating public exhibitions or public entertainment; or  
   f. for the imposition of restrictions upon public officers.  
| SEYCHELLES  | Article 22, 28 | **Article 22.**  
1. Every person has a right to freedom of expression and opinion.  
2. A person shall not except with the free consent of that person be hindered in the enjoyment of the freedom of expression, which includes the freedom of the press and other media, that is to say -  
   a. freedom to hold opinions without interference;  
   b. freedom to communicate and information without interference;  
   c. freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons); and  
   d. freedom from interference with the correspondence of that person.  
|             |          | **Article 28.**  
1. The State recognises the right of access of every person to information relating to that person and held by a public authority, which is performing a governmental function and the right to have the information rectified or otherwise amended, if inaccurate.  
2. The right of access to information contained in clause (1) shall be subject to such limitations and procedures as may be prescribed by law and are necessary in democratic society including-  
   a. for the protection of national security;  
   b. for the prevention and detection of crime and the enforcement of law;  
   c. for the compliance with an order of a court or in accordance with a legal privilege;  
   d. for the protection of the privacy or rights or freedoms of others;  
3. The State undertakes to take appropriate measures to ensure that information collected in respect of any person for a particular purpose is used only for that purpose except where a law necessary in a democratic society or an order of a court authorises otherwise.  
4. The State recognises the right of access by the public to information held by a public authority performing a governmental function subject to limitations contained in clause (2) and any law necessary in a democratic society.  
| SOUTH AFRICA | Section 32 | **Section 32. Access to information**  
1. Everyone has the right of access to  
   a. any information held by the state; and  
   b. any information that is held by another person and that is required for the exercise or protection of any rights.  
2. National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.  
| SWAZILAND (ESWATINI) | Article 24 | **Article 24. Protection of freedom of expression**  
1. A person has a right of freedom of expression and opinion.  
2. A person shall not except with the free consent of that person be hindered in the enjoyment of the freedom of expression, which includes the freedom of the press and other media, that is to say -  
   a. freedom to hold opinions without interference;  
   b. freedom to receive ideas and information without interference;  
   c. freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons); and  
   d. freedom from interference with the correspondence of that person.  
| TANZANIA (UNITED REPUBLIC OF) | Article 18 | **Article 18. Freedom of expression**  
Every person-  
   a. has a freedom of opinion and expression of his ideas;  
   b. has a right to seek, receive and, or disseminate information regardless of national boundaries;  
   c. has the freedom to communicate and a freedom with protection from interference from his communication; and  
   d. has a right to be informed at all times of various important events of life and activities of the people and also of issues of importance to the society.  

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>ACCESS TO INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ZAMBIA</strong></td>
<td><strong>Article 11, 20</strong></td>
</tr>
<tr>
<td><strong>Article 11: Fundamental rights and freedoms</strong></td>
<td></td>
</tr>
<tr>
<td>It is recognised and declared that every person in Zambia has been and shall continue to be entitled to the fundamental rights and freedoms of the individual, that is to say, the right, whatever his race, place of origin, political opinions, colour, creed, sex or marital status, but subject to the limitations contained in this Part, to each and all of the following, namely:</td>
<td></td>
</tr>
<tr>
<td>b. freedom of conscience, expression, assembly, movement and association;</td>
<td></td>
</tr>
<tr>
<td><strong>Article 20: Protection of freedom of expression</strong></td>
<td></td>
</tr>
<tr>
<td>1. Except with his own consent, no person shall be hindered in the enjoyment of his freedom of expression, that is to say, freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to impart and communicate ideas and information without interference, whether the communication be to the public generally or to any person or class of persons, and freedom from interference with his correspondence.</td>
<td></td>
</tr>
<tr>
<td>2. Subject to the provisions of this Constitution no law shall make any provision that derogates from freedom of the press.</td>
<td></td>
</tr>
<tr>
<td>3. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this Article to the extent that it is shown that the law in question makes provision—</td>
<td></td>
</tr>
<tr>
<td>a. that is reasonably required in the interests of defence, public safety, public order, public morality or public health; or</td>
<td></td>
</tr>
<tr>
<td>b. that is reasonably required for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the courts, regulating educational institutions in the interests of persons receiving instruction therein, or the registration of, or regulating the technical administration or the technical operation of, newspapers and other publications, telephony, telegraphy, posts, wireless broadcasting or television; or</td>
<td></td>
</tr>
<tr>
<td>c. that imposes restrictions on public officers; and except so far as that provision or, the thing done under the authority thereof as the case may be, is shown not to be reasonably justifiable in a democratic society.</td>
<td></td>
</tr>
<tr>
<td><strong>ZIMBAWE</strong></td>
<td><strong>Article 61, 62</strong></td>
</tr>
<tr>
<td><strong>Article 61. Freedom of expression and freedom of the media</strong></td>
<td></td>
</tr>
<tr>
<td>1. Every person has the right to freedom of expression, which includes—</td>
<td></td>
</tr>
<tr>
<td>a. freedom to seek, receive and communicate ideas and other information;</td>
<td></td>
</tr>
<tr>
<td>b. freedom of artistic expression and scientific research and creativity; and</td>
<td></td>
</tr>
<tr>
<td>2. Every person is entitled to freedom of the media, which freedom includes protection of the confidentiality of journalists’ sources of information.</td>
<td></td>
</tr>
<tr>
<td>3. Broadcasting and other electronic media of communication have freedom of establishment, subject only to State licensing procedures that—</td>
<td></td>
</tr>
<tr>
<td>a. are necessary to regulate the airwaves and other forms of signal distribution; and</td>
<td></td>
</tr>
<tr>
<td>b. are independent of control by government or by political or commercial interests.</td>
<td></td>
</tr>
<tr>
<td>4. All State-owned media of communication must—</td>
<td></td>
</tr>
<tr>
<td>a. be free to determine independently the editorial content of their broadcasts or other communications;</td>
<td></td>
</tr>
<tr>
<td>b. be impartial; and</td>
<td></td>
</tr>
<tr>
<td>c. afford fair opportunity for the presentation of divergent views and dissenting opinions.</td>
<td></td>
</tr>
<tr>
<td>5. Freedom of expression and freedom of the media exclude—</td>
<td></td>
</tr>
<tr>
<td>a. incitement to violence;</td>
<td></td>
</tr>
<tr>
<td>b. advocacy of hatred or hate speech;</td>
<td></td>
</tr>
<tr>
<td>c. malicious injury to a person’s reputation or dignity; or</td>
<td></td>
</tr>
<tr>
<td>d. malicious or unwarranted breach of a person’s right to privacy.</td>
<td></td>
</tr>
<tr>
<td><strong>Article 62. Access to information</strong></td>
<td></td>
</tr>
<tr>
<td>1. Every Zimbabwean citizen or permanent resident, including juristic persons and the Zimbabwean media, has the right of access to any information held by the State or by any institution or agency of government at every level, in so far as the information is required for the exercise or protection of a right.</td>
<td></td>
</tr>
<tr>
<td>2. Every person, including the Zimbabwean media, has the right of access to any information held by any person, including the State, in so far as the information is required for the exercise or protection of a right.</td>
<td></td>
</tr>
<tr>
<td>3. Every person has a right to the correction of information, or the deletion of untrue, erroneous or misleading information, which is held by the State or any institution or agency of the government at any level, and which relates to that person.</td>
<td></td>
</tr>
<tr>
<td>4. Legislation must be enacted to give effect to this right, but may restrict access to information in the interests of defence, public security or professional confidentiality, to the extent that the restriction is fair, reasonable, necessary and justifiable in a democratic society based on openness, justice, human dignity, equality and freedom.</td>
<td></td>
</tr>
</tbody>
</table>
## Annexure 2C: Freedom of Expression

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>FREEDOM OF EXPRESSION</th>
<th>TEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ANGOLA</strong></td>
<td>Article 32, 40</td>
<td>1. The right to personal identity, civil capacity, nationality, a good name and reputation, likeness, free speech, and privacy in personal and family life shall be recognised for all.</td>
</tr>
<tr>
<td></td>
<td>Article 40</td>
<td>1. Everyone shall have the right to freely express, publicise and share their ideas and opinions through words, images or any other medium, as well as the right and the freedom to inform others, to inform themselves and to be informed, without hindrance or discrimination.</td>
</tr>
<tr>
<td><strong>BOTSWANA</strong></td>
<td>Article 3, 12</td>
<td>1. Exception with his or her own consent, no person shall be hindered in the enjoyment of his or her freedom of expression, that is to say, freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons) and freedom from interference with his or her correspondence.</td>
</tr>
</tbody>
</table>
|                                  | Article 12           | Preamble The Comorian people solemnly affirm their will...
|                                  |                      | They proclaim: ...freedom of expression and of assembly, freedom of association and freedom to organize trade unions, subject to respect for morals and public order; |
| **COMOROS**                      | Preamble             | Preamble The Comorian people solemnly affirm their will...
<p>|                                  |                      | They proclaim: ...freedom of expression and of assembly, freedom of association and freedom to organize trade unions, subject to respect for morals and public order; |
| <strong>DEMOCRATIC REPUBLIC OF CONGO</strong> | Article 23           | All persons have the right to freedom of expression. This right implies the freedom to express their opinions or their convictions, notably by speech, print and pictures, under reserve of respect for the law, for public order and for morality. |
|                                  | Article 4            | 1. Whereas every person in Lesotho is entitled, whatever his race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status to fundamental human rights and freedoms, that is to say, to each and all of the following— |
|                                  |                      | j. freedom of expression; |
|                                  | Article 14           | 1. Every person shall be entitled to, and (except with his own consent) shall not be hindered in his enjoyment of, freedom of expression, including freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons) and freedom from interference with his correspondence. |
|                                  |                      | 2. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision— a. in the interests of defence, public safety, public order, public morality or public health; or b. for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the courts, or regulating the technical administration or the technical operation of telephony, telegraphy, posts, wireless broadcasting or television; or c. for the purpose of imposing restrictions upon public officers. |
|                                  |                      | 3. A person shall not be permitted to rely in any judicial proceedings upon such a provision of law as is referred to in subsection (2) except to the extent to which he satisfies the court that that provision or, as the case may be, the thing done under the authority thereof does not abridge the freedom guaranteed by subsection (1) to a greater extent than is necessary in a practical sense in a democratic society in the interests of any of the matters specified in subsection (2)(a) or for any of the purposes specified in subsection (2)(b) or (c). |
|                                  |                      | 4. Any person who feels aggrieved by statements or ideas disseminated to the public in general by a medium of communication has the right to reply or to require a correction to be made using the same medium, under such conditions as the law may establish. |</p>
<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>SECTION</th>
<th>TEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>MADAGASCAR</td>
<td>Article 10.</td>
<td>The freedoms of opinion and of expression, of communication, of the press, of association, of assembly, of circulation, of conscience and of religion are guaranteed to all and may only be limited by the respect for the freedoms and rights of others, and by the imperative of safeguarding the public order, the national dignity and the security of the State.</td>
</tr>
<tr>
<td>MALAWI</td>
<td>Article 35. Freedom of expression</td>
<td>Every person shall have the right to freedom of expression.</td>
</tr>
<tr>
<td>MAURITIUS</td>
<td>Article 3, 12</td>
<td>It is hereby recognised and declared that in Mauritius there have existed and shall continue to exist without discrimination by reason of race, place of origin, political opinions, colour, creed or sex, but subject to respect for the rights and freedoms of others and for the public interest, each and all of the following human rights and fundamental freedoms... b. freedom of conscience, of expression, of assembly and association and freedom to establish schools, and...</td>
</tr>
<tr>
<td>MOZAMBIQUE</td>
<td>Article 48</td>
<td>1. All citizens shall have the right to freedom of expression and to freedom of the press, as well as the right to information. 2. The exercise of freedom of expression, which consists of the ability to impart one’s opinions by all lawful means, and the exercise of the right to information shall not be restricted by censorship. 3. Freedom of the press shall include, in particular, the freedom of journalistic expression and creativity, access to sources of information, protection of independence and professional secrecy, and the right to establish newspapers, publications and other means of dissemination. 4. In the public sector media, the expression and confrontation of ideas from all currents of opinion shall be guaranteed. 5. The State shall guarantee the impartiality of the public sector media, as well as the independence of journalists from the Government, the Administration and other political powers. 6. The exercise of the rights and freedoms provided for in this article shall be governed by law on the basis of the imperative respect for the Constitution and for the dignity of the human person.</td>
</tr>
<tr>
<td>NAMIBIA</td>
<td>Article 21. Fundamental freedoms</td>
<td>1. All persons shall have the right to: a. freedom of speech and expression, which shall include freedom of the press and other media;...</td>
</tr>
<tr>
<td>SEYCHELLES</td>
<td>Article 22</td>
<td>1. Every person has a right to freedom of expression and for the purpose of this article this right includes the freedom to hold opinions and to seek, receive and impart ideas and information without interference. 2. The right under clause (1) may be subject to such restrictions as may be prescribed by a law and necessary in a democratic society- a. in the interest of defence, public safety, public order, public morality or public health; b. for protecting the reputation, rights and freedoms or private lives of persons; c. for preventing the disclosure of information received in confidence; d. for maintaining the authority and independence of the courts or the National Assembly; e. for regulating the technical administration, technical operation, or general efficiency of telephones, telegraphy, posts, wireless broadcasting, television, or other means of communication or regulating public exhibitions or public entertainment; or f. for the imposition of restrictions upon public officers.</td>
</tr>
<tr>
<td>SOUTH AFRICA</td>
<td>Article 16. Freedom of expression</td>
<td>1. Everyone has the right to freedom of expression, which includes- a. freedom of the press and other media; b. freedom to receive or impart information or ideas; c. freedom of artistic creativity; and d. academic freedom and freedom of scientific research. 2. The right in subsection (1) does not extend to- a. propaganda for war; b. incitement of imminent violence; or c. advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm.</td>
</tr>
<tr>
<td>COUNTRY</td>
<td>FREEDOM OF EXPRESSION</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SECTION</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TEXT</td>
<td></td>
</tr>
<tr>
<td><strong>SWAZILAND (ESWATINI)</strong></td>
<td>Article 24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. A person has a right of freedom of expression and opinion.</td>
<td></td>
</tr>
</tbody>
</table>
|                         | 2. A person shall not except with the free consent of that person be hindered in the enjoyment of the freedom of expression, which includes the freedom of the press and other media, that is to say—  
|                         | a. freedom to hold opinions without interference;  
|                         | b. freedom to receive ideas and information without interference;  
|                         | c. freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons); and  
|                         | d. freedom from interference with the correspondence of that person. |
|                         | …                   |
| **TANZANIA (UNITED REPUBLIC OF)** | Article 18 |
|                         | Every person—  
|                         | a. has a freedom of opinion and expression of his ideas;  
|                         | b. has a right to seek, receive and, or disseminate information regardless of national boundaries;  
|                         | c. has the freedom to communicate and a freedom with protection from interference from his communication;  
|                         | d. has a right to be informed at all times of various important events of life and activities of the people and also of issues of importance to the society. |
| **ZAMBIA**              | Article 11, 20      |
|                         | It is recognised and declared that every person in Zambia has been and shall continue to be entitled to the fundamental rights and freedoms of the individual, that is to say, the right, whatever his race, place of origin, political opinions, colour, creed, sex or marital status, but subject to the limitations contained in this Part, to each and all of the following, namely:  
|                         | …                   |
|                         | b. freedom of conscience, expression, assembly, movement and association; |
|                         | **Article 21: Protection of freedom of assembly and association**  
|                         | 1. Except with his own consent, no person shall be hindered in the enjoyment of his freedom of assembly and association, that is to say, his right to assemble freely and associate with other persons and in particular to form or belong to any political party, trade union or other association for the protection of his interests.  
|                         | 2. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this Article to the extent that it is shown that the law in question makes provision—  
|                         | a. that is reasonably required in the interests of defence, public safety, public order, public morality or public health;  
|                         | b. that is reasonably required for the purpose of protecting the rights or freedoms of other persons;  
|                         | c. that imposes restrictions upon public officers; or  
|                         | d. for the registration of political parties or trade unions in a register established by or under a law and for imposing reasonable conditions relating to the procedure for entry on such register including conditions as to the minimum number of persons necessary to constitute a trade union qualified for registration; and except so far as that provision or, the thing done under the authority thereof as the case may be, is shown not to be reasonably justifiable in a democratic society. |
| **ZIMBABWE**            | Article 61          |
|                         | 1. Every person has the right to freedom of expression, which includes—  
|                         | a. freedom to seek, receive and communicate ideas and other information;  
|                         | b. freedom of artistic expression and scientific research and creativity; and  
|                         | 2. Every person is entitled to freedom of the media, which freedom includes protection of the confidentiality of journalists’ sources of information.  
|                         | 3. Broadcasting and other electronic media of communication have freedom of establishment, subject only to State licensing procedures that—  
|                         | a. are necessary to regulate the airwaves and other forms of signal distribution; and  
|                         | b. are independent of control by government or by political or commercial interests.  
|                         | 4. All State-owned media of communication must—  
|                         | a. be free to determine independently the editorial content of their broadcasts or other communications;  
|                         | b. be impartial; and  
|                         | c. afford fair opportunity for the presentation of divergent views and dissenting opinions.  
|                         | 5. Freedom of expression and freedom of the media exclude—  
|                         | a. incitement to violence;  
|                         | b. advocacy of hatred or hate speech;  
|                         | c. malicious injury to a person’s reputation or dignity; or  
|                         | d. malicious or unwarranted breach of a person’s right to privacy. |
### Annexure 3: SADC Legislative Mapping

#### Annexure 3A: Data Ownership, Control and Access

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>DATA PROTECTION</th>
<th>ACCESS TO INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LEGISLATION</td>
<td>INSTITUTIONS</td>
</tr>
<tr>
<td></td>
<td>LAW</td>
<td>INSTITUTIONAL BODIES</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REGULATORY BODIES</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LAW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INSTITUTIONAL BODIES</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REGULATORY BODIES</td>
</tr>
<tr>
<td>ANGOLA</td>
<td>Personal Data Protection Law 22/11; Electronic Communications and Information Society Services Law 23/10; Protection of Information Systems and Networks Law 7/17; Decree No.214/16 (DPA)</td>
<td>The Ministry of Telecommunications and Information Technology</td>
</tr>
<tr>
<td>BOTSWANA</td>
<td>Data Protection Act (2018)</td>
<td>Ministry of Transport and Communications</td>
</tr>
<tr>
<td>COMOROS</td>
<td>Data Protection Bill (?)</td>
<td>Ministry of Transport, Post and Telecommunications, Information and Communication Technologies</td>
</tr>
<tr>
<td>DEMOCRATIC REPUBLIC OF CONGO</td>
<td>Telecommunications and ICT Bill</td>
<td>Ministere des Postes, Telecommunications, Nouvelles Technologies de l'Information &amp; de la Communication</td>
</tr>
<tr>
<td>COUNTRY</td>
<td>DATA PROTECTION</td>
<td>INSTITUTIONS</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td></td>
<td>LAW</td>
<td>INSTITUTIONAL BODIES</td>
</tr>
<tr>
<td></td>
<td>LEGISLATION</td>
<td>REGULATORY BODIES</td>
</tr>
<tr>
<td>NAMIBIA</td>
<td>Data Protection Bill</td>
<td>Ministry of Information and Communication Technology (MICT)</td>
</tr>
<tr>
<td>SEYCHELLES</td>
<td>The Data Protection Act (Act No 9) (2003)</td>
<td>Department of Information and Communication Technology</td>
</tr>
<tr>
<td>SOUTH AFRICA</td>
<td>Protection of Personal Information Act</td>
<td>Department of Telecommunications and Postal Services</td>
</tr>
<tr>
<td>ZAMBIA</td>
<td>Electronic Communications and Transactions Act, Data Protection (Repeal) Bill (2016)</td>
<td>Ministry of Communications and Transport</td>
</tr>
<tr>
<td>ZIMBABWE</td>
<td>The Access to Information and Protection of Privacy Act, Revised National Policy for Information Communication Technology (2016)</td>
<td>Minister of Information, Publicity, and Broadcasting Services</td>
</tr>
<tr>
<td></td>
<td>Cybercrime, Cybersecurity and Data Protection Bill 2019</td>
<td>Media and Information Commission; The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ)</td>
</tr>
</tbody>
</table>
## Annexure 3B: Data Interference

<table>
<thead>
<tr>
<th>SADC COUNTRIES</th>
<th>LEGAL FRAMEWORK</th>
<th>CSERT / CIRT</th>
<th>INSTITUTIONAL ARRANGEMENT</th>
<th>STANDARDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANGOLA</td>
<td>The Law on Protection of Networks and Information Systems (Law no. 7/17), 2017. The 2011 Law on Electronic Communications and Information Company Services</td>
<td>Plans were announced in July 2019</td>
<td>The Ministry of Telecommunications and Information Technology, regulated by the Angolan Institute for Communications (INACOM)</td>
<td>None</td>
</tr>
<tr>
<td>BOTSWANA</td>
<td>Cybercrime and Computer Related Crimes Act, 2007; Cybercrime and Computer Related Crimes Act, 2018 (draft)</td>
<td>In phase T of implementation. Governmental, &amp; recognised by ITU.</td>
<td>Ministry of Transport and Communications, regulated by BOCRA (Botswana Communications Regulatory Authority)</td>
<td>Mentioned in strategy, shared responsibility</td>
</tr>
<tr>
<td>COMOROS</td>
<td>No legislation</td>
<td>None</td>
<td>Ministry of Transport, Post and Telecommunications, Information and Communication Technologies, and regulation by National Authority for Regulation of Information and Communication Technologies</td>
<td>None</td>
</tr>
<tr>
<td>DEMOCRATIC REPUBLIC CONGO</td>
<td>Law no. 013/2002 governs the telecommunication sector</td>
<td>None</td>
<td>Ministere des postes, telecommunications, nouvelles technologies de l’information &amp; de la communication</td>
<td>None</td>
</tr>
<tr>
<td>ESWATINI</td>
<td>Draft bill - computer and cybercrime Bill awaiting adoption since at least 2014</td>
<td>None</td>
<td>Ministry of Information, Communications and Technology oversees, under which there is a Computer Services Department</td>
<td>None</td>
</tr>
<tr>
<td>LESOTHO</td>
<td>Draft bill - Computer and Cyber Crime Bill since at least 2013</td>
<td>None</td>
<td>Ministry of Communications, Science &amp; Technology</td>
<td>None</td>
</tr>
<tr>
<td>MADAGASCAR</td>
<td>Loi No. 2014-006 sur la lutte contre la cybercriminalité, 2014 Cybercrime law.</td>
<td>No, but incident response is provided ad hoc by telecom operators</td>
<td>Ministry of Posts, Telecommunications and New Technologies (NPTDN), and Regulatory Authority for Communication Technologies (ARTEC)</td>
<td>No coordination</td>
</tr>
</tbody>
</table>
| MALAWI         | - Communications Act 2018 (No. 34 of 2018)  
- Electronic Transactions and Cyber Security Act 2016 (No. 33 of 2016) | 'Malawi CERT' is in design phase, at Macra, some ITU consultation | Ministry of ICT, and for regulation, Malawi Communications Regulatory Authority (Macra) | Malawi Bureau of Standards |
| MAURITIUS      | Computer Misuse and Cybercrime Act, 2003  
Information and Communication Technologies Act 2001  
Data Protection Act No. 20, 2017 | CERT-MU, managed by National Computer Board (within ICT Authority) | ICT Authority. The ministry of Technology, Communication and Innovation. 1T Security Unit. National Computer Board | Mauritius Standards Bureau |
<p>| MOZAMBIQUE     | Electronic Transactions Act, 2018 | Morenet (academia) | Minister for Transport and Communications, regulated by Instituto Nacional das Comunicações de Moçambique (INCM) | INCM responsible |</p>
<table>
<thead>
<tr>
<th>SADC COUNTRIES</th>
<th>LEGAL FRAMEWORK</th>
<th>CSERT / CIRT</th>
<th>INSTITUTIONAL ARRANGEMENT</th>
<th>STANDARDS</th>
</tr>
</thead>
</table>
| **NAMIBIA**    | - Communications Act 2009  
- Use of Electronic Transaction and Communication Act (draft) 2010  
- Cybercrime bill (Drafted 2013 as a result of HIPSSA)  
- Computer Misuse Act of 1988 | None | Communications Regulatory Authority of Namibia (CRAN)  
Ministry of Information and Communication Technology | Ministry of ICT responsible |
| **SEYCHELLES** | Computer Misuse Act No. 17 of 1998, Cybercrimes and other related crimes (draft) bill 2013 | None | Department of Information and Communication Technology, has an IT division under office of president |
| **SOUTH AFRICA** | - Electronic communication and Transactions Act No 25 of 2002  
- Regulation of Interception of Communications and Provision of communication-related Information Act of 2002  
- Cyber Crimes Bill, 2017 | ECS-CSIRT (under State Security Authority) + Sectoral CIRTs - Standard Bank CIRT, SANReN CSIRT, UCT CIRT | Department of Telecommunications and Postal Services (Chief Director of Cybersecurity Operations), and National Cybersecurity Hub. National Cybersecurity Advisory Council, Independent Communications Authority of South Africa, Cybersecurity Response Committee (Proposed) |
| **TANZANIA**   | Electronic and Postal Act (EPICA) no 32/2010 Cybercrimes Act, 2015 | TZ-CERT, established by ITU, within the TCRA | The United Republic of Tanzania Ministry of Works, Transport and Communication, Tanzania Communication Regulatory Authority (TCRA) has a Department of Information Communication Technology | Mentioned in ICT policy |
| **ZAMBIA**     | Electronic Communication and Transactions Act (ECT Act) 21, 2009  
Computer Misuse and Crimes Act No. 15, 2004  
Cybersecurity and Cybercrimes Bill, 2018 | zmCIRT, set up by the ITU in 2012, managed by the Zambia ICT Authority | Ministry of Communications and Transport, Zambia ICT Authority | Zambia ICT Authority responsible |
## Annexure 3C: Data-driven Value Creation

<table>
<thead>
<tr>
<th>Country</th>
<th>E-commerce and E-transactions</th>
<th>Intellectual Property and Copyright</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legislation</strong></td>
<td><strong>Institutions</strong></td>
<td><strong>Regulatory Bodies</strong></td>
</tr>
<tr>
<td><strong>Laws</strong></td>
<td><strong>Institutional Bodies</strong></td>
<td><strong>Regulatory Bodies</strong></td>
</tr>
<tr>
<td>Country</td>
<td>E-Commerce and E-Transactions</td>
<td>Intellectual Property and Copyright</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Legislation</td>
<td>Institutions</td>
</tr>
<tr>
<td></td>
<td>Laws</td>
<td>Institutional Bodies</td>
</tr>
<tr>
<td>MADAGASCAR</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MALAWI</td>
<td>电子交易和网络犯罪法，2016</td>
<td>CERN, CFTC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trademarks Act, 2018 (Act No. 2 of 2018); Copyright Act, 2018 (Act No. 26 of 2018); Patent Act (Chapter 49:02) (1986); Registered Designs Act (Chapter 49:05) (1986); Merchandise Marks Act (Chapter 49:04) (1966)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAURITIUS</td>
<td>电子交易法（2000，2009年修订）;网络安全法（2004年）</td>
<td>ICT Authority:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Patent, Industrial Designs and Trademarks Act, 2002; The Copyright Act, 2014; Geographical Indications Act, 2002; Layout-Designs (Topographies) of Integrated Circuits Act, 2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MOZAMBIQUE</td>
<td>电子交易法（2017）</td>
<td>Instituto Nacional de Tecnologias de Informacao y Comunicacion (INTIC)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Industrial Property Code (approved by Decree No. 47/2015); Law No. 4/2001 of February 27, 2001 (Copyright Act)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAMIBIA</td>
<td>电子交易和网络犯罪法案（2017）</td>
<td>Namibian Competition Commission</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Industrial Property Act, 2012 (Act No. 1 of 2012); Copyright Act, 2014 (Act No. 5 of 1994); Trade and SME Development (MITSMED); Ministry of Industrialization, Trade and SME Development (MITSMED); Business and Intellectual Property Authority (BIPA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEYCHELLES</td>
<td>电子交易法（2003）</td>
<td>Department of Information Communications and Technology in the Ministry of National Development (DC)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Controller of Certifying Authorities: Advisory Committee</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

THE DIGITAL ECONOMY AND SOCIETY
97
<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>E-COMMERCE AND E-TRANSACTIONS</th>
<th>INTELLECTUAL PROPERTY AND COPYRIGHT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LEGISLATION</td>
<td>INSTITUTIONS</td>
</tr>
<tr>
<td></td>
<td>LAWS</td>
<td>REGULATORY BODIES</td>
</tr>
<tr>
<td></td>
<td>SOUTH AFRICA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Electronic Communications and Transactions Act (ECT); Protection of Personal Information Act</td>
<td>Department of Communications</td>
</tr>
<tr>
<td></td>
<td>SWAZILAND (ESWATINI)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Electronic Communications and Transactions Bill (2017)</td>
<td>Eswatini Communications Commission (ESCOM)(?)</td>
</tr>
<tr>
<td></td>
<td>TANZANIA (UNITED REPUBLIC OF)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Electronic Transactions Act (2015)</td>
<td>The United Republic of Tanzania Ministry of Works, Transport and Communication</td>
</tr>
<tr>
<td></td>
<td>ZAMBIA</td>
<td></td>
</tr>
<tr>
<td>COUNTRY</td>
<td>E-COMMERCE AND E-TRANSACTIONS</td>
<td>INTELLECTUAL PROPERTY AND COPYRIGHT</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td>LEGISLATION</td>
<td>INSTITUTIONS</td>
</tr>
</tbody>
</table>