SADC PF Discussion Paper on the Digital Economy and Society:

Synthesis Report

409 The Studios
Old Castle Brewery
6 Beach Road
Woodstock, 7925
Cape Town, South Africa

This is a Synthesis Report[1] of a full Discussion Paper[2] that focuses on the policy and governance considerations for developing countries to enable the development of inclusive and sustainable digital economies . Drafted by Research ICT Africa, the papers build on the points of mutual understanding in the SADC Parliamentary Forum-Research ICT Africa Memorandum of Understanding. The Discussion Paper and this Synthesis Report, are part of the process of drafting a SADC PF Model Law for the Digital Economy. The objectives 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. This Synthesis Report will summarise the key information from the Discussion Paper to inform further engagement on the Model Law.

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.

Part A: Digital Economy

1. Introduction

Digitisation on a global scale has been a defining characteristic of socio-economic development in the 21st century. The global trends of digitalisation and now 'datafication' impact every aspect of social and economic activity. With the emergence of advanced technologies merging the physical and digital realms, the Internet of Things (IOT), 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.

Fast changing processes of digitalisation and 'datafication' characterise the contemporary global economy. Some of the developments have been incremental and some have been 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 and handful of companies (UNCTAD 2019). And just as benefits accrue unequally, so too do the risks and harms of digification, which follow many of the offline patterns of social and income inequality.

These challenges highlight the need for policymakers in developing countries to view digitalisation in the context of global markets and value chains but also in their local context where the lack of digital readiness will constrain their ability to leverage these new technologies and processes and to mitigate the risks associated to employment, data governance and access to finance. Fundamental to this is the importance of digital inclusion of developing countries and critical sectors within developing economies to increase their visibility in the wider value chain ecosystem.

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'.

[1] This Synthesis Report if based on version 4 of the Discussion Paper.

[2] The Discussion Paper contains the full reference list.

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, which can be considered as a call for 'data justice'.

While there is inceasing acknowledgement of the need for data protection in this data-driven economy, particularly to optimise opportunities for internal and external trade, globally data protection is highly fragmented, with diverging global, regional and national regulatory approaches. 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 creation of an equitable and sustainable digital economy.

It is timely therefore that SADC PF is preparing a draft model law for the regional economic community. As the UNCTAD 2019 Digital Economy report says: The net impact will 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 (UNCTAD 2019).

The next section of Part A of the Synthesis Report locates a national digital economy in the wider global digital ecosystem and systems of global governance (a fuller consideration of the key attributes of the digital economy, which include the aspects of digital inequality alluded to above is provided for in the Discussion Paper).

Part B then focuses on the legal context and provides structure for policymakers and legislators by first outlining a frame for considering the domestication of a Model Law of the Digital Economy, before outlining the key human rights implications, and then providing specific consideration of the legal frames within SADC currently.

Part C looks at key policy recommendations, which arise from the Discussion Paper, across three key thematic areas: data ownership, control and access; data security and interference; and data-driven value creation.

2. Digital Ecosystem

In line with the international development agenda's emphasis on digital technologies as enablers of development, ICTs have also been identified by the Southern African Development Community (SADC) as critical elements in building a more inclusive society, by eliminating poverty and reducing inequality in the country.[3] However, in this environment, the rules and policies that hope to facilitate development have to respond to a peculiar reality marked by interconnectedness and globalisation. An essential policy shift is required from a 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.

3 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_Met_meeting.pdf

Conceptualised as an ecosystem (Figure 1), the relationships between different elements and the outcomes resulting from their interactions can be assessed for policy purposes. Rather than focusing on the fast changing technology, this approach places users, citizens, and consumers at the centre of the ecosystem. Even where infrastructure is available the affordability of the networks, services, applications and content in the ecosystem will determine the degree to which they are able to access the ecosystem. These, in turn, are an outcome of the market structure and the effectiveness of the regulation, which are themselves determined by the national policy and legal framework.

But the ability of citizens to deploy these technologies and digital services to enhance their livlihoods 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 competiton regulation of network operator and service providers. For the digital policy to spur employment and innovation, an integrated strategy for investment and human development is essential.

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

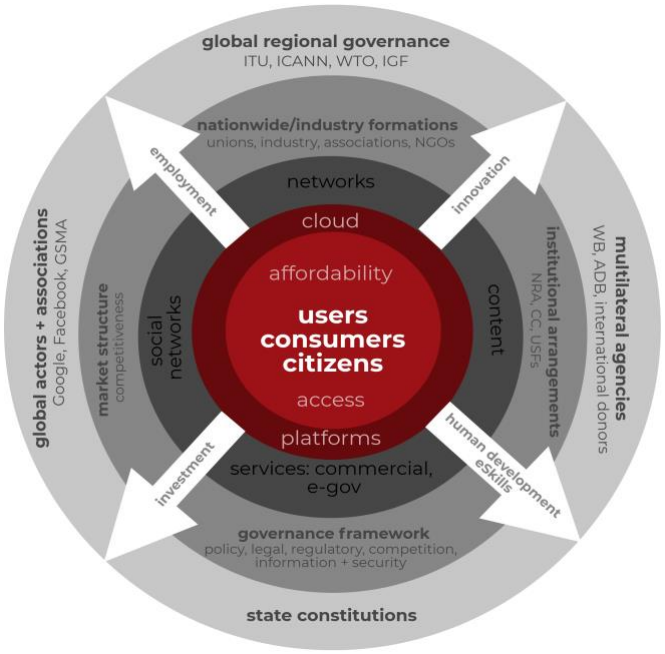

Figure 1: An *ecosystemic* view of the digital environment

The interconentions beween different components of the ecosystem highlight the need for policymakers in developing countries to view digitalisation in the context of global markets and value chains, but also in their local context where the lack of digital readiness will constrain their ability to leverage these new

technologies and processes, and to mitigate the risks associated 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, some even to enhance their prosperity, is widening.

Similarly, as more people who do have 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.

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).

A transversal national strategy is therefore required for developing countries 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 digital economy to flourish. To achieve this, policies will need to derive from participatory multistakeholders 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 to improve the 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 critical assets for new entrants and data flows to enable cross boarder trade, 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 wil 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 disincentvising network investment and regressive social network taxation dampening usage by the poor, and engagement with global digital taxation regime reform that is 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.

Neither the Discussion Paper nor the Synthesis Report are able to deal with all the policy issues related to this enabling environment at length. Instead, they focus 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. They do this in order to design a considered environmental and policy framework that can support, and implement, the objectives of a Digital Economy Law.

Part B: Legal Context

3. Foundations for the Model Law

The digital economy presents some clear opportunities. In Africa, the contribution of the Internet to GDP growth currently remains low. But there are nevertheless suggestions that emerging economies, in particular, may see amplified benefit moving forward with the Internet adding significant value to Africa's GDP (Manyika, J et al., 2013).

In the SADC, any discussion on potential opportunities for growth and gains resulting from the digital economy must be contextualised within the attendant risks of inequality and exclusion. In considering what the role of domestic legislatures may be in contributing to this digital economy, the strong regional legacy of human rights frameworks serves as a useful foundation for exploring interventions within this space, particularly given their ability to incorporate socio-political norms within economic policy.

In considering further the issues of relevance to considering the legislative remit for the digital economy, the Discussion Paper considers the fundamental components and conditions for a 'good' digital economy by establishing some key recommendations (detailed later), but also by positing a framework for considering what domestic laws would need to consider in implementing a Digital Economy Model Law. So, within this wider *ecosystemic* approach, the approach for this discussion on the policy and legislative framework required to optimise the digital economy can be outlined as:

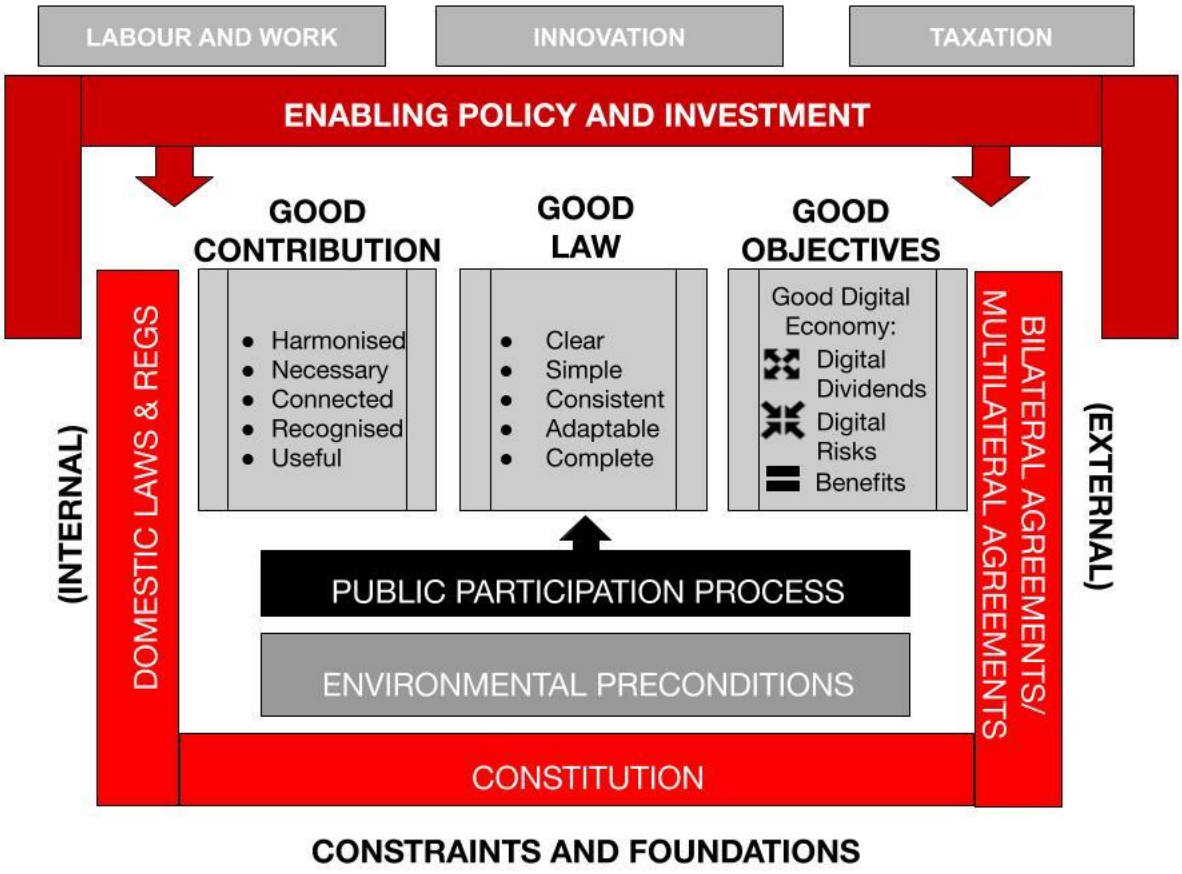

Figure 5: Diagram providing framework for development of a Model Law on Digital Economy

The framework acknowledges that a transversal national strategy is required for developing countries 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 digital economy to flourish. To achieve this, policies will need to derive from participatory multistakeholders processes in which civil society and the private sector engage with Government.

The objectives of the Model Law should not simply seek to encourage the digital economy, as encouraging the digital economy 'as is' will only increase digital risks and inequalities. 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.

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. The positions outlined below will be the first step toward considering principle-led drafting for the Model Law.

4. Human rights

Human rights[4] are, naturally, mutually reinforcing and inter-connected. Human rights principles, which are strongly driven across the region through both regional human rights bodies, as well as domestic legislatures and judiciaries, should serve as the normative standard for incorporating social imperatives within the economic climate of a Digital Economy Model Law.

Given the data and information-centred landscape of the digital economy, references to rights that exist within the civil-political spectrum of rights is most common – and of particular reference in considering the constraints and ambitions of a Digital Economy Model Law are the rights of privacy, access to information and freedom of expression. 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 of relevance, such as the right to work and right to inequality. However, at least for the exercise of providing a frame (particularly a justiciable frame given limits of some socio-economic rights),

4 See Annexure 1.

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.

5. SADC domestic legislative mapping

Referring back to the Model Law Framework outlined in *Figure 5*, considering the legal context necessitates a reference to both relevant regional instruments (outlined in Annexure 1A), as well as key regional principles and guidelines (outlined in Annexure 1B). Additionally, the domestic legislative contexts for the different position areas must be considered. A preliminary mapping of such domestic constitutional and legislative instruments is available in the remaining Annexures.

While the Discussion Paper comprehensively considers both SADC instruments and SADC domestic laws, it is worth providing a cursory overview of key SADC-related domestication across the policy areas.

5.1 Data ownership, control and access

SADC Model Law on Data Protection

The Draft 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.

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 data protection authority (DPA), which is widely acknowledged as an essential element of an effective enforcement of data privacy laws. In South Africa, its 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). Failure to appoint a DPA in due time is repeatedly criticised for being a major impediment to effectively enforcing 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).

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 (Greenleaf, 2018). 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).

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 European Union, 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. Those are Democratic Republic of Congo, Mozambique, and Namibia.

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

certain categories of data; iii) territorial applicability of laws; iv) cross-border data transfers; v) data breach notification; vi) appointment of a Data Protection Officer (DPO); vii) development of Codes of Conduct or Ethics.

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 stand-alone 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 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.[5] There is also not a strong consistency in the provision of Regulators, which presents challenges both to the adaptability of the laws, but also limits access to recourse for businesses and citizens.

5.2 Data safety and interference

Domestic Legal Frameworks on Cybersecurity and Cybercrime

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 ratified 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.[6] 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.

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 as mentioned the South African Cybercrimes Bill 2017 is now awaiting Presidential signature), though the Computer Misuse Act in Seychelles and Namibia have been identified as inadequate for the

5 Interestingly, some of these countries have had their laws directly measured against the Model Law, and the result can be viewed here: http://www.africanplatform.org/fileadmin/Content/PDF/Resources/State-of-ATI-in-Africa-2017.pdf.

6 See here the brief discussion of the case provided previously under "2.1.1 Surveillance".

current technological landscape. 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.

Capability and country maturity assessments

An important consideration often raised in the context of cybersecurity is not just the risks it poses, but the capabilities of the state and its agencies to combat cybercrime. 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" (ITU, 2018).

5.3 Data-driven value creation

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).

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 IP and Copyright coordination (Nkomo, 2014) and may be able to overcome some shortcomings experienced by the African Regional Intellectual Property Organization (ARIPO). A number of SADC countries including South Africa, Angola, Mozambique and Madagascar are not members.

Part C: Policy Positions

6. Structure for policy sections

There are three broad areas under which we have organised policy position recommendations:

- 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 as an additional way of helping to organise 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:

Main Policy Area	Sub theme	Sub theme	Sub theme
Data ownership, control and access	Data protection and privacy	Data and information access	
Data safety and interference	Cybersecurity & Surveillance	Cybercrimes	Access restrictions
Data-driven value creation	E-commerce and e-transactions	Intellectual property and copyright	

Within the Discussion Paper, there are broader recommendations contained in the outlining of issues that precedes each recommendation section. In order to fully appreciate the context of the specific recommendations, but also to consider other broader areas that may be informed by principles within a Model Law, the fuller Policy Paper should be considered.

7. Policy options and recommendations: Data ownership, control and access

Policy Sub theme	Policy Issue	Recommendation
Surveillance	**Lawful data processing**	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. In the 4IR, 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).
	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 both their broader economic benefits, but also potentially the treatment or results of data particular to individual data subjects. This can be facilitated both through positive obligation in relation to the processing of data, but also through ensuring data subject rights include proactive rights to access, and have amended, their personal data.
	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 able to be re-identified. 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. On the other hand, 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, which would be facilitated by the DPA.
	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. 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.
	Security	Article 25 of the SADC Model Law 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 DPA why it delayed. The Article does not even place an obligation on the data controller to notify the data subject of a breach. Moreover, there is no requirement on the part of the data controller and data processor to disclose what information has been compromised. This is not in line with the Preamble, which calls for transparency and accountability on the part of the data controller and data processor. And importantly, placing these obligations on a data controller need not be onerous if a DPA 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. 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.
	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. It means a product is designed with privacy as a priority, along with whatever other purposes the system serves. The Draft SADC Model Law on Data Protection does not place emphasis on the principle of 'privacy by design', which is an important aspect to consider with regard to the 4IR. Therefore, we recommend that 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 meets the data protection requirements, while ensuring the protection of the rights of the data subject. 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.
	Data flows	The flow of data is a fundamental reality of the way in which digitalisation and globalisation have driven the digital economy. As more and more economic and social activities move online, the importance of data protection and privacy is increasingly recognized, not least in the context of international trade. Data protection is directly related to trade in goods and services in the digital economy. Insufficient protection can create negative market effects by reducing consumer confidence, and overly stringent protection can unduly restrict businesses, with adverse economic effects as a result. Ensuring that laws consider the global nature and scope of their application, and foster compatibility with other frameworks, is of utmost importance for global trade flows that increasingly rely on the Internet. Addressing the issue of cross-border data transfers using specific text and promoting one or more mechanisms that businesses can use to enable international data flows is crucial.

	Cross-border co-operation, harmonisation and minimum standards	Limitations on cross-border data transfer could result in loss of business opportunities and reduce the ability of an organisation to trade internationally, leading to a reduced geographical footprint and market competitiveness loss. 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. A misconception on data protection harmonisation comes from the misunderstanding that harmonisation requires all national laws to be identical. This approach does not consider national differences in terms of existing frameworks, or advancement 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) data protection authorities are an important aspect in 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. A well-resourced and empowered DPA can help ease compliance burdens for the private and public sector.
	Effective remedies and administrative justice	Outside of notification procedures, data subjects need to be assured of adequate access to remedies. Yet this extends beyond access to a DPA. This is because in order to facilitate the adaptable generation of regulations, DPA's 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. But in order to facilitate this kind of flexibility, an adequate administrative justice paradigm is necessary to ensure accountability for such decisions. A further interesting component to this is the restriction, demonstrated in the South African law that prohibits automated decision-making. Within the AI context, these prohibitions are noteworthy.
	Data sovereignty	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; on the other hand, strong data sovereignty favours a state-led approach with an emphasis on safeguarding national security. However, data localisation goes beyond regulating the conditions for transfer, and obliges all personal data to be domestically held. These extreme may, however, interfere with digital economy objectives and should never replace the more fundamental step of data processing laws.
Data and information access	**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", but also in order 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 to certain standards. These generation obligations can go some way in 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 deemed "as the right to explainability" potentially generated from a composite of data subject rights in the European Union General Data Protection Regulation (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). 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*. 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.
	Data subject rights	Connected to the mandates of data protection and privacy, data subjects need rights that they can assert for seeking to enforce transparency. Positive data subject rights, which allow subjects to access, asses, review, and delete their information can be associated as much to data protection, as data access.
	Digital identity	Linked to personal data control is the need for data subjects to possess good digital identity. Digital identity is a central enabler for engaging in public and private digital services, as well as necessity for reaping forms of digital dividends In 2017 the World Bank, under its ID4D program, developed "Principles on Identification for Sustainable Development". Including guidance such as ensuring universal coverage and robust security, these Principles were then used as the foundation for the #Good ID movement. These kinds of principles should inform the establishment of both private and public sector-designed digital identity systems, which are supported by sufficient data governance frameworks (the role of data subject rights will support the establishment of good digital identity in South Africa). Contrary though to the listed benefits of good identity systems, bad identity systems may play a role in exclusion and even growth in lived inequalities for citizens. This reiterates the need for a DPA that support data justice imperatives being in place, supported by lawful data processes applicable to every actor in the digital identity value chain, whether public or private sector.

8. Policy options and recommendations: Data safety and interference

Policy Sub theme	Policy Issue	Recommendation
Cybersecurity & Surveillance	**Cybersecurity strategies**	The first stepping-stone for an effective cybersecurity policy and regulatory framework is a cybersecurity strategy, which should align to law. 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. Elements of the strategy which will need to align to law include: ❖ 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 cybersecurity strategy; ❖ Identify the mechanisms required to secure critical cyber infrastructure and ICT uptake; ❖ Identify critical services (in addition to critical infrastructures) that the strategy intends to make more secure and resilient; etc.
	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.
	Cross-border coordination and joint response	Fighting cyber-attacks require cross-border coordination. The European Union 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 cybersecurity readiness in order to proactively engage. These should also have a cybercrime focus.
Cybercrime	**Cyber law enforcement**	Cybercrime transcends national borders and requires transnational solutions and international, multi-national 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, cybercrime. The legal and regulatory authorities designated with carrying out activities to curb cybercrime must define what constitutes a cybercrime 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 unwittingly impinge on other rights. In particular, in the SADC region, caution must be exercised to avoid the criminalisation of speech. Legislation should provide some clarity in the form of a list of offences, which should include offences focused 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 related 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. So, for instance 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.
	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 prevent 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 cybercrime can only be assured by including training for court judges, prosecutors, lawyers, law enforcement officials, forensic specialists, and other investigators on cybercrime and cybersecurity challenges and regulation.
Access restrictions	**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.
	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. 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.

9. Policy options and recommendations: Data-driven value creation

Policy Sub theme	Policy Issue	Recommendation
E-commerce & E-transactions	**Role of regulators**	There are strong guidelines available in the SADC Mobile Money Guidelines on regulators for that specific subsect of digital economy concerns. As is fairly consistent within the digital economy framework, regulation requires balancing innovation and constraint. To allow for innovation, businesses can be given space through "Regulatory Sandboxes" to test out their products without the risk of potential legal liability. 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.
	Customs complexity and impact	The reduction of customs complexity through policy is a key way of facilitating regional e-commerce by improving logistics for both customer and business as well as costing and internal efficiencies for business. Importantly too, within the context of trade, tariff incongruency more broadly can presents risks of 'trade

		deflection'. 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. In spite of this, digital products are taxed as luxury goods in many countries, driving up costs; 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 offset the direct economic losses experienced by minimising taxation.
	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.
	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. 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. 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 (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.

Intellectual property & copyright	**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: a) in certain special cases; b) that do not conflict with the normal exploitation of the work; and c) 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. 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. 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.
	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.
	AI & IP	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.
	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.
	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).

Annexures

Annexure 1: Relevant African Regional Instruments

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

Instrument	Year	Applicable SADC Countries	Binding?
African Charter on Human and Peoples' Rights	1986	All	Yes
African Union Convention on Cyber-security and Personal Data Protection (Malabo Convention)	2014	Comoros (signatory), Mauritius (ratified), Mozambique (signatory), Namibia (ratified), Zambia (signatory)	No, currently insufficient ratifications
Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	1981	Mauritius	Yes
Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows.	2001	Mauritius	Yes
Council of Europe Convention on Cybercrime (Budapest Convention)	2001	Mauritius (ratified), South Africa (signatory)	Yes
International Covenant on Civil and Political Rights	1966	All except Comoros (signatory)	Yes

International Covenant on Economic, Social and Cultural Rights	1966	All, except Comoros (signatory), Botswana (not signed), Mozambique (not signed).	Yes

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

Institutional Home	Title	Year
African Union	Declaration on Internet Governance	2018
African Union	Declaration of Principles on Freedom of Expression in Africa	2002
African Union	Declaration on Internet Governance	2018
African Union	Model Law on Access to Information	2013
African Union Commission and Internet Society	Personal Data Protection Guidelines for Africa	2018
Civil Society	African Declaration on Internet Rights and Freedoms	2016
Civil Society	Manila Principles on Intermediary Liability	2015
Southern African Development Community	Draft Model Law on Computer Crime and Cybercrime	2013
Southern African Development Community	Draft Model Law on Data Protection	2013
Southern African Development Community	Draft Model Law on Electronic Transactions and Electronic Communications	2013
Southern African Development Community	Mobile Money Guidelines	2016
United Nations	Guiding Principles on Business and Human Rights (Ruggie Principles)	2011
United Nations, General Assembly	The right to privacy in the digital age	2013

United Nations, Human Rights Council	The promotion, protection and enjoyment of human rights on the Internet	2012

Annexure 2: SADC Constitutional Mapping

Annexure 2A: Right to Privacy

Country	Privacy		
	Section	Text	Note
Angola	Article 32	**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	**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 (domicile)	**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	**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	**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-- … b. the right to personal liberty;	Reference to personal and information privacy (in a freedom of expression context).

		… 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. ….	

Madagascar	Article 13	**Article 13.** Any individual is assured of the inviolability of their person, their domicile and of the secrecy of their correspondence. …	Reference to personal and communications privacy.
Malawi	Article 21	**Article 21. Privacy** Every person shall have the right to personal privacy, which shall include the right not to be subject to— a. searches of his or her person, home or property; b. the seizure of private possessions; or c. interference with private communications, including mail and all forms of telecommunications.	Reference to personal and communications privacy.
Mauritius	Article 3, 9	**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 … 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. **Article 9. Protection for privacy of home and other property** 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. 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, 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; b. for the purpose of protecting the rights or freedoms of other persons; c. to enable an officer or agent of the Government or a local authority, or a body	Reference to privacy of the home and property, not in relation to information.

		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 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.	
Mozambique	Right 41, 71	**Article 41. Other individual rights** 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. **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.	Reference to information privacy and, noteworthy, data privacy.
Namibia	Article 13	**Article 13. Privacy** 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. 2. Searches of the person or the homes of individuals shall only be justified: a. where these are authorised by a competent judicial officer; b. in cases where delay in obtaining such judicial authority carries with it the danger of	Reference to personal and communications privacy.

		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.	
Seychelles	Article 20	**Article 20.** 1. Every person has a right not to be subjected- 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; 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. …	Reference to personal and communications privacy.
South Africa	Section 14	**Section 14. Privacy** Everyone has the right to privacy, which includes the right not to have a. their person or home searched; b. their property searched; c. their possessions seized; or d. the privacy of their communications infringed.	Reference to personal and communications privacy.
Swaziland (Eswatini)	Article 14, 22	**Article 14. Fundamental rights and freedoms of the individual** 1. The fundamental human rights and freedoms of the individual enshrined in this Chapter are hereby declared and guaranteed, namely – … c. protection of the privacy of the home and other property rights of the individual; … **Article 22. Protection against arbitrary search or entry** 1. A person shall not be subjected – a. to the search of the person or the property of that person; b. to the entry by others on the premises of that person; c. to the search of the private communications of that person, except with the free consent of that person first obtained. …	Reference to privacy of the home and some communications privacy.
Tanzania (United Republic of)	Article 16	**Article 16. Right to privacy and personal security** 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. 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	Reference to personal privacy and communications privacy.

		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.	
Zambia	Article 11, 17	**Article 11: Fundamental rights and freedoms** 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: … d. protection for the privacy of his home and other property and from deprivation of property without compensation; … **Article 17: Protection for privacy of home and other property** 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. …	Reference to privacy of the home and property, not in relation to information.
Zimbabwe	Article 57	**Article 57. Right to privacy** Every person has the right to privacy, which includes the right not to have-- a. their home, premises or property entered without their permission; b. their person, home, premises or property searched; c. their possessions seized; d. the privacy of their communications infringed; or e. their health condition disclosed.	Reference to personal privacy and communications privacy.

Annexure 2B: Right to Access Information

Country	Access to Information	
	Section	Text
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 there of is shown not to be reasonably justifiable in a democratic society.
Comoros	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 audiovisual 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 4, 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. …
Madagascar	Article 10, 11	**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.
Malawi	Article 34,35,36,37	**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.
Mauritius	Article 3, 12	**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. ….
Mozambique	Article 48, 49, 71, 253	**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.

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; …
Seychelles	Article 22, 28	**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. **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 (Eswaitini)	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; 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	**Article 11: Fundamental rights and freedoms** 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 20: 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 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. 2. Subject to the provisions of this Constitution no law shall make any provision that derogates from freedom of the press. 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— 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 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 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.
Zimbabwe	Article 61, 62	**Article 61. Freedom of expression and freedom of the media** 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. **Article 62. Access to information** 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 in the interests of public accountability. 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. 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. 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.

Annexure 2C: Freedom of Expression

Country	Freedom of Expression	
	Section	Text
Angola	Article 32, 40	**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. **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. …
Botswana	Article 3, 12	**Article 3. Fundamental rights and freedoms of the individual** Whereas every person in Botswana is entitled to the fundamental rights and freedoms of the individual, that is to say, the right, whatever his or her 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 to each and all of the following, namely— … b. freedom of conscience, of expression and of assembly and association; … 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 communication be to the public generally or to any person or class of persons) and freedom from interference with his or her correspondence. …
Comoros	Preamble	**Preamble** The Comorian people solemnly affirm their will …Human and Peoples' Rights, as well as by the international conventions, particularly those relating to childrens' and women's' rights. 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; …
Democratic Republic of Congo	Article 23	**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.
Lesotho	Article 4, 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. 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.

Madagascar	Article 10,	**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.
Malawi	Article 35	**Article 35. Freedom of expression** Every person shall have the right to freedom of expression.
Mauritius	Article 3, 12	**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. …
Mozambique	Article 48	**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.
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; ….

Seychelles	Article 22	**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.
South Africa	Article 16	**Article 16. Freedom of expression** 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.
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 boundaires; 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	**Article 11: Fundamental rights and freedoms** 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	**Article 61. Freedom of expression and freedom of the media** 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

Country	Data Protection			Access to Information		
	Legislation	Institutions		Legislation	Institutions	
	Law	Institutional Bodies	Regulatory Bodies	Law	nstitutional Bodies	Regulatory Bodies
Angola	Personal Data Protection Law 22/11; Electronic Communications and Information Society Services Law 23/11; Protection of Information Systems and Networks Law 7/17; Decree No.214/16 (DPA)	The Ministry of Telecommunications and Information Technology	Data Protection Agency (inactive); Angolan Regulatory Body for Social Communication (ERCA); Angolan Institute for Communications (INACOM)	Law 11/02 on Access to Documents held by Public Authorities (AKA "Freedom of information Act") (2002)	The Ministry of Telecommunications and Information Technology	Angolan Regulatory Body for Social Communication (ERCA); Angolan Institute for Communications (INACOM)
Botswana	Data Protection Act (2018)	Ministry of Transport and Communications	Information and Data Protection Commission (inactive); BOCRA (Botswana Communications Regulatory Authority)	Freedom of Information Bill (2010)	Ministry of Transport and Communications	The Press Council of Botswana (w/ Media Complaints Committee); BOCRA (Botswana Communications Regulatory Authority)
Comoros	Data Protection Bill (?)	Ministry of Transport, Post and Telecommunications, Information and Communication Technologies	The National Regulation Authority of Information and Communications Technology (ANRTIC)		Ministry of Transport, Post and Telecommunications, Information and Communication Technologies	The National Regulation Authority of Information and Communications Technology (ANRTIC)
Democratic Republic of Congo	Telecommunications and ICT Bill	Ministere des Postes,Télécommunications, Nouvelles Technologies de l'Information & de la Communication	L'autorite de regulation de la poste et des telecommunications	Access to Information Bill 2015	Ministere des Postes,Télécommunications, Nouvelles Technologies de l'Information & de la Communication	L'autorite de regulation de la poste et des telecommunications

Lesotho	Data Protection Act, 2013	Ministry of Communications, Science & Technology	Lesotho's Data Protection Commission (inactive)	Access and Receipt of Information Bill (2000)	Ministry of Communications, Science & Technology	
Madagascar	Law No. 2014-038 (Data Protection Law) (2014)	Ministry of Posts, Telecommunications and New Technologies (NPTDN)	Commission Malagasy sur l'Informatique et des Libertés (inactive); Regulatory Authority for Communication Technologies (ARTEC)	Access to Information Bill (2006); The Conseil pour la Sauvegarde de l'Intrégrité (CSI) promotes ATI and transparency.	Ministry of Posts, Telecommunications and New Technologies (NPTDN)	Regulatory Authority for Communication Technologies (ARTEC)
Malawi	Electronic Transactions and Cyber Security Act, 2016; The Communications Act, 2016	Ministry of ICT	Malawi Communications Regulatory Authority	Access to Information Act (2016)	Ministry of ICT	Malawi Communications Regulatory Authority
Mauritius	Data Protection Act (2017)	The ministry of Technology, Communication and Innovation.	Office of the Data Protection Commissioner; ICT Authority	Promises of FOIA over the past 9 years	The ministry of Technology, Communication and Innovation.	ICT Authority
Mozambique	Law n.º 3/2017 (The Electronic Transactions Law) (2017)	Minister for Transport and Communications	Instituto Nacional das Comunicações de Moçambique (INCM)	Access to Information Act (2014)	Minister for Transport and Communications	Instituto Nacional das Comunicações de Moçambique (INCM)
Namibia	Data Protection Bill	Ministry of Information and Communication Technology (MICT)		Access to Information Bill, 2019	Ministry of Information and Communication Technology (MICT)	
Seychelles	The Data Protection Act (Act No 9) (2003)	Department of Information and Communication Technology	Data Protection Commissioner (inactive); Seychelles Media Commission	Access to Information Act (2018)	Department of Information and Communication Technology	Information Commission; Seychelles Media Commission
South Africa	Protection of Personal Information Act	Department of Telecommunications and Postal Services	Office of the Information Regulator	Promotions of Access to Information Act	Department of Telecommunications and Postal Services	Office of the Information Regulator
Swaziland (Eswatini)	Data Protection Bill (2017)	Ministry of Information, Communications and Technology	Swaziland Communications Commission	Public Service Act (2018); Official Secrets Act; Freedom of Information and	Ministry of Information, Communications and Technology	

				Protection of Privacy Bill		
Tanzania (United Republic of)	The Electronic and Postal Communications Act (2010), Data Protection Bill (2014)	The United Republic of Tanzania Ministry of Works, Transport and Communication	Tanzania Communication Regulatory Authority (TCRA)	Access to Information Act (2016)	The United Republic of Tanzania Ministry of Works, Transport and Communication	
Zambia	Electronic Communications and Transactions Act, Data Protection (Repeal) Bill (2018)	Ministry of Communications and Transport	Zambia Information and Communication Technology Authority	Access to Information Bill (2002)	Ministry of Communications and Transport	
Zimbabwe	The Access to Information and Protection of Privacy Act, Revised National Policy for Information Communication Technology (2016) Cybercrime, Cybersecurity and Data Protection Bill 2019	Minister of Information, Publicity, and Broadcasting Services	Media and Information Commission; The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ)	The Access to Information and Protection of Privacy Act 2002 Freedom of Information Bill 2019	Minister of Information, Publicity, and Broadcasting Services	Media and Information Commission; The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ)

Annexure 3B: Data interference

SADC Countries	Legal Framework	CSERT / CIRT	Institutional Arrangement	Standards
Angola	The Law on Protection of Networks and Information Systems (Law no. 7/17), 2017. The 2011 Law on Electronic Communications and Information Company Services	Plans were announced in July 2019	The Ministry of Telecommunications and Information Technology, regulated by the Angolan Institute for Communications (INACOM)	None
Botswana	Cybercrime and Computer Related Crimes Act, 2007: Cybercrime and Computer Related Crimes Act, 2018 (draft)	In 'phase 1' of implementation. Governmental, & recognised by ITU.	Ministry of Transport and Communications, regulated by BOCRA (Botswana Communications Regulatory Authority)	Mentioned in strategy, shared responsibility
Comoros	No legislation	None	Ministry of Transport, Post and Telecommunications, Information and Communication Technologies, and regulation by National Authority for Regulation of Information and Communication Technologies	None
Democratic Republic Congo	Law no. 013/2002 governs the telecommunication sector	None	Ministere des postes,télécommunications, nouvelles technologies de l'information & de la communication	None
Eswatini	Draft bill - computer and cybercrime Bill awaiting adoption since at least 2014	None	Ministry of Information, Communications and Technology oversees, under which there is a Computer Services Department	None
Lesotho	Draft bill - Computer and Cyber Crime Bill since at least 2013	None	Ministry of Communications, Science & Technology	

Madagascar	Loi n°2014-006 sur la lutte contre la cybercriminalité, 2014 Cybercrime law.	No, but incident response is provided ad hoc by telecom operators	Ministry of Posts, Telecommunications and New Technologies (NPTDN), and Regulatory Authority for Communication Technologies (ARTEC)	No coordination
Malawi	- Communications Act 2016 (No. 34 of 2016) - 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. 'IT Security Unit'. National Computer Board	Mauritius Standards Bureau
Mozambique	Electronic Transactions Act, 2018	Morenet (academia)	Minister for Transport and Communications, regulated by Instituto Nacional das Comunicações de Moçambique (INCM)	INCM responsible
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, Cyber crimes 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 and Cyber Security 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 (EPOCA) no 3/2010 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. 13, 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
Zimbabwe	Computer Crime and Cyber Crime Bill; Criminal Law (Codification and Reform) Act 23, 2004; Interception of Communications Act [Chapter 11:20] and the Postal and Telecommunications Act [Chapter 12:05] 2004; Cybercrime, Cyber Security and Data Protection Bill, 2019	None	Ministry of Information Communication Technology, Postal and Courier Services (has a minister of cyber security), The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ)	Responsibility of POTRAZ

Annexure 3C: Data-driven Value Creation

Country	E-commerce and E-transactions			Intellectual Property and Copyright		
	Legislation	Institutions		Legislation	Institutions	
	Laws	Institutional Bodies	Regulatory Bodies	Laws	Institutional Bodies	Regulatory Bodies
Angola	Information Society Technologies and Services' Regulation (Presidential Decree 202/11, 22 July); Retail Commerce Organisation, Execution and Functioning' Regulation (Presidential Decree no. 263/10, 25 November)		Electronic Communication Regulatory Body; BNA (?)	Law No. 15/14 of July 31, 2014, on Copyright and Related Rights; Law No. 4/90 of March 10, 1990 on Author's Rights; Law No. 3/92 of February 28, 1992, on Industrial Property; Information Society Technologies and Services' Regulation (Presidential Decree 202/11, 22 July 2011)	Ministry of Culture; Ministry of Industry	Instituto Angolano da Propriedade Industrial (IAPI); National Directorate for Copyrights and Related Rights
Botswana	Electronic Communications and Transactions Act (2014), National e-commerce strategy (2018)		Botswana Communications Regulatory Authority (BROCA)	Industrial Property Act, 2010 (Act No. 8 of 2010); Copyright and Neighboring Rights Act, 2000 (Chapter 68:02, as amended by Act No. 6 of 2006); Copyright and Neighboring Rights Regulations, 2007 (S.I. No. 11 of 2007)	Ministry of Investment, Trade and Industry	Companies and Intellectual Property Authority (CIPA)
Comoros	Draft law			Bangui Agreement, 2013; Law No. 64-1360 of December 31, 1964, on Trademarks and Service Marks (1964); Law of March 11, 1957, on Literary and Artistic Property (1957); Law of July 14, 1909, on Designs and Models (1909); Law of July 5, 1844, on Patents for Inventions (1844)	Ministry of Youth, Employment, of the Workforce Development, Culture, and Sport; Ministry of Economy, Planning, Energy, Tourism, Private Sector of the Investments and Land Affairs	Comorian Office of Intellectual Property (OCPI)

Democratic Republic of Congo	Draft law	Ministry of Communications, Science and Technology		Law No. 82-001 of January 7, 1982 on Industrial Property (1982); Ordinance-Law No. 86-033 on the Protection of Copyright and Neighboring Rights (1986)	Secretariat General of Culture; Directorate of Research, Planning and International Cultural Relations; Ministry of Culture and the Arts; Directorate of Industrial Property Secretariat for industry and small and medium enterprises (IPMEA); Ministry of Industry and SMEs	Congolese Patent and Trademark Office
Lesotho	Electronic Transactions and Electronic Commerce Bill (2013)			Industrial Property Order, 1989 (Order No. 5 of 1989, as last amended by Act No. 4 of 1997); Copyright Order, 1989 (Order No.13 of 1989)	Ministry of Law, Constitutional Affairs and Human Rights	Registrar General's Office
Madagascar	Law N° 2014-024 on Electronic Transactions (2015); Law N° 2014-025 on Electronic Signature (2015)		Competition Council Directorate for Competition and Market Regulation (DCRM)	Law No. 94-036 of September 18, 1995, on Literary and Artistic Property (1994); Decree No. 98-434 of June 16, 1998, on the Status and Functioning of the Malagasy Copyright Office (OMDA) (1998); Decree No. 98-435 of June 16, 1998, on General Rules for the Collection of Copyright and Neighboring Rights (1998); Ordinance No. 89-019 of July 31, 1989, establishing Arrangements for the Protection of Industrial Property (1992)	Ministry of Communication and Culture (OMDA); Ministry of Industry, Trade and Craft (OMAPI)	Malagasy Copyright Office; Malagasy Industrial Property Office
Malawi	Electronic Transactions and Cyber Security Act, 2016		CERN, CFTC	Trademarks Act, 2018 (Act No. 2 of 2018) (2018); Copyright Act, 2016 (Act No. 26 of 2016) (2017); Patents Act (Chapter 49:02) (1986); Registered Designs Act (Chapter 49:05) (1985);	Department of the Registrar General (Ministry of Justice and Constitutional Affairs); Ministry of Youth, Sports, Culture & Community Development	Copyright Society of Malawi (COSOMA)

				Merchandise Marks Act (Chapter 49:04) (1966)		
Mauritius	Electronic Transactions Act (ETA) (2000, amended 2009); Data Protection Act (2004)		ICT Authority;	The Patent, Industrial Designs and Trademarks Act, 2002; The Copyright Act, 2014; Geographical Indications Act, 2002; Layout-Designs (Topographies) of Integrated Circuits Act, 2002	Regional Integration and International Trade (Ministry of Foreign Affairs)	Industrial Property Office (IPO)
Mozambique	Electronic Transactions Act (2017)		Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC)	Industrial Property Code (approved by Decree No. 47/2015); Law No. 4/2001 of February 27, 2001 (Copyright Law)	National Institute of Book and Records (Ministry of Culture and Tourism); Industrial Property Institute (Ministry of Industry and Commerce)	
Namibia	Electronic Transactions and Cybercrime Bill (2017)		Namibian Competition Commission	Industrial Property Act, 2012 (Act No. 1 of 2012) (2018); Copyright and Neighbouring Rights Protection Act, 1994 (Act No. 6 of 1994) (1994)	Ministry of Industrialization, Trade and SME Development (MITSMED); Ministry of Industrialization, Trade and SME Development (MITSMED)	Business and Intellectual Property Authority (BIPA); Business and Intellectual Property Authority (BIPA)
Seychelles	Electronic Transactions Act (2000)	Department of Information Communications and Technology in the Ministry of National Development (DIC)	Controller of Certifying Authorities; Advisory Committee	Industrial Property Act 2014 (Act No. 7 of 2014) (2015); Copyright Act, 2014 (Act No. 5 of 2014) (2014)	Intellectual Property Office (Registration Division, Department of Legal Affairs, President's Office); Ministry of Finance, Trade, Investment and Economic Planning;	
South Africa	The Electronic Communications and Transactions Act (ECT); Protection of Personal Information Act	Department of Communications	Consumer Affairs Committee; Independent Communication Authority of South Africa (ICASA)	Copyright Act 1978 (Amendment Bill before President).	Companies and Intellectual Property Commission (CIPC) (Department of Trade and Industry)	

Swaziland (Eswaitini)	The Electronic Communications and Transactions Bill (2017)		Eswatini Communications Commission (ESCCOM) (?)	Intellectual Property Tribunal Act, 2018; Patents, Utility Models and Industrial Designs Act, 1997 (1997); Trade Marks Act, 1981 (1981); Merchandise Marks Act, 1937 (1937); Copyright (Rome Convention) Act, 1933 (1933); Copyright (Prohibited Importation) Act, 1918 (1918); Copyright Act, 1912 (1912)	Intellectual Property Office (Ministry of Commerce Industry and Trade)	
Tanzania (United Republic of)	The Electronic Transactions Act (2015)	The United Republic of Tanzania Ministry of Works, Transport and Communication		The Zanzibar Industrial Property Act, 2008 (Act No. 4 of 2008) (2008); The Zanzibar Copyright Act, 2003 (2003); Copyright and Neighbouring Rights Act, 1999 (1999); The Patents (Registration) Act (1995); The Trade and Service Marks Act, 1986 (1986); Merchandise Marks Act, 1963 (Act No. 20 of 1963) (1963)	Copyright Society of Zanzibar (COSOZA) (Ministry of Youth, Culture, Arts and Sports); The Copyright Society of Tanzania (COSOTA) (Ministry of Industry and Trade); Business Registrations and Licensing Agency (BRELA) (Ministry of Industry and Trade; Zanzibar Business and Property Registration Agency (BPRA) (Ministry of Industry and Trade)	
Zambia	Electronic Communications and Transactions Act (2009)		Zambia Information and Communication Technology Authority; Accreditation Authority	The Industrial Designs Act, 2016 (Act No. 22 of 2016) (2016); The Layout-Designs of Integrated Circuits Act, 2016 (Act No. 6 of 2016) (2016); The Patents Act, 2016 (Act No. 40 of 2016) (2016); The Protection of Traditional Knowledge, Genetic Resources and Expressions of Folklore Act, 2016 (Act No. 16 of 2016) (2016); The Copyright and Performance Rights Act, 1994 (Act No. 44 of 1994) (1994), The Merchandise Marks Act (Chapter 405) (1994);	Patents and Companies Registration Agency (PACRA) (Ministry of Commerce, Trade and Industry)	

				The Trade Marks Act (Chapter 401) (1994)		
Zimbabwe	Electronic Transactions and Electronic Commerce Bill (2013)			Trade Marks Act (Chapter 26:04, as amended up to Act No. 3 of 2016) (2016); Copyright and Neighbouring Rights Act (Chapter 26:05, as amended up to Act No. 32 of 2004) (2004); Patents Act (Chapter 26:03, as amended up to Act No. 14/2002) (2002); Industrial Designs Act (Chapter 26:02, as amended up to Act No. 25 of 2001) (2001), Integrated Circuit Layout Designs Act (Chapter 26:07) (2001); Merchandise Marks Act (Chapter 14:13) (2001); Intellectual Property Policy and Implementation Strategy [2018-2022]	Zimbabwe Intellectual Property Office (ZIPO) (Ministry of Justice, Legal and Parliamentary Affairs)	