Documento de Trabalho do FP-SADC sobre a Economia e a Sociedade Digital:

Relatório de Síntese

409 The Studios
Old Castle Brewery
6 Beach Road
Woodstock, 7925
Cape Town, South Africa
Phone: +27 21 447 6332
Fax: +27 21 447 9529
www.researchictafrica.net

Este é um Relatório de Síntese[1] de um Documento de Trabalho completo[2] que se foca nas considerações sobre a política e governança para os países em desenvolvimento para permitir o desenvolvimento de economias digitais inclusivas e sustentáveis. Elaborado pela Research ICT Africa, os documentos assentam nos pontos de entendimento mútuo do Memorando de Entendimento entre o Fórum Parlamentar da SADC e a Research ICT Africa. O Documento de Trabalho, e este Relatório de Síntese, fazem parte do processo destinado à elaboração de uma Lei Modelo do FP-SADC para a Economia Digital. O objectivo de uma tal Lei Modelo para a Economia e a Sociedade Digital é permitir aos países aproveitar os benefícios da economia digital, enquanto salvaguarda os direitos dos cidadãos e mitiga os possíveis riscos associados a tais desenvolvimentos. Este Relatório de Síntese irá resumir a informação principal do Documento de Trabalho para nortear o desenvolvimento adicional da Lei Modelo.

O Fórum Parlamentar da SADC e a Research ICT Africa estão gratos ao Centro Internacional de Pesquisa sobre o Desenvolvimento (IDRC) do Canadá, que tornou possível esta investigação e colaboração.

Parte A: Economia Digital

1. Introdução

A digitalização a uma escala global tem sido uma característica definidora do desenvolvimento socioeconómico no século XXI. As tendências globais de digitalização e agora de "dataficação" afectam todos os aspectos da actividade económica e social. Com a emergência de tecnologias avançadas que fundem os reinos físico e digital, a Internet das Coisas (IdC, ou IOT em Inglês), a inteligência artificial (IA) e as tecnologias de aprendizagem das máquinas permitem a recolha, o uso e a análise de vastas quantidades de dados digitais gerados pelas actividades pessoais, sociais e económicas *online*.

A economia global contemporânea caracteriza-se por processos de digitalização e "dataficação" em rápida mudança. Alguns dos desenvolvimentos foram graduais e alguns disruptivos, mas todos foram altamente desiguais. Actualmente, a geração, o processamento e a transmissão de informação definem de forma crítica quem beneficia do potencial transformador da digitalização. As plataformas globais têm sido as maiores beneficiárias e criadoras do novo valor criado por estes processos. O seu domínio dos mercados através do controlo dos dados, bem como da sua capacidade de criar e capturar valor [perpetuar] resultaram na sua concentração e consolidação num punhado de países e numa mão-cheia de empresas (UNCTAD 2019). E tal como os benefícios se acumulam de forma desigual, assim também os riscos e os danos da "digificação", que seguem muitos dos padrões de desigualdade social e de rendimento *offline*.

Estes desafios realçam a necessidade de os decisores políticos nos países em desenvolvimento verem a digitalização no contexto dos mercados globais e das cadeias de valor, mas também no seu contexto local, em que a falta de prontidão digital irá limitar a sua capacidade de aproveitamento destas novas tecnologias e processos e de mitigação dos riscos associados ao emprego, governança de dados e acesso a financiamento. Um aspecto fundamental para isto é a importância da inclusão digital de países em

[1] Este Relatório de Síntese baseia-se na versão 4 do Documento de Trabalho.

[2] O Documento de Trabalho contém a lista de referência completa.

desenvolvimento e de sectores vitais nas economias em desenvolvimento para aumentar a sua visibilidade no ecossistema da cadeia de valor mais abrangente.

Na era da digitalização, os dados assumiram um papel significativo no desenvolvimento socioeconómico, pois são considerados um recurso estratégico e crucial para as economias baseadas em dados – um processo agora referido como "dataficação". Mas embora os benefícios socioeconómicos da análise de grandes quantidades de dados não possam ser ignorados, são necessários enquadramentos de governança de dados para o processamento transparente e responsável da informação pessoal (antes da agregação) de forma a salvaguardar os direitos de acesso à informação e a privacidade. Isto tem também implicações em outros direitos fundamentais, o que pode ser considerado como um apelo à "justiça dos dados".

Embora exista um crescente reconhecimento da necessidade de protecção de dados nesta economia baseada em dados, particularmente para optimizar oportunidades de comércio interno e externo, globalmente a protecção de dados está altamente fragmentada, com abordagens regulatórias globais, regionais e nacionais divergentes. Um enquadramento que facilite a disponibilização de dados ao mesmo tempo que respeita os direitos de privacidade, a integridade dos dados e a disponibilidade é fundamental para a construção de um ambiente digital confiável e seguro e é uma pré-condição para a criação de uma economia digital equitativa e sustentável.

É por isso oportuno que o FP-SADC esteja a preparar um projecto de Lei Modelo para a comunidade económica regional. Tal como diz o relatório da Economia Digital UNCTAD 2019: O impacto líquido dependerá do nível de desenvolvimento e da prontidão digital dos países e das suas partes interessadas. Dependerá também das políticas adoptadas e implementadas aos níveis nacional, regional e internacional (UNCTAD 2019).

A próxima secção da Parte A do Relatório de Síntese localiza uma economia digital nacional no ecossistema digital global mais alargado e nos sistemas de governança global (no Documento de Trabalho é fornecida uma análise mais completa dos atributos principais da economia digital, os quais incluem os aspectos da desigualdade digital a que se aludiu acima).

A Parte B focar-se-á depois no contexto jurídico e providenciará uma estrutura para os decisores políticos e legisladores, delineando primeiro um enquadramento para considerar a transposição para as legislações nacionais de uma Lei Modelo da Economia Digital, definindo depois as principais implicações em termos de direitos humanos, e providenciando em seguida uma análise específica dos quadros jurídicos actualmente existentes na SADC.

A Parte C analisa as principais recomendações em termos de políticas, que decorrem do Documento de Trabalho, em três áreas temáticas principais: propriedade, controlo e acesso aos dados; segurança dos dados e interferência nos mesmos; e criação de valor baseada em dados.

2. Ecossistema Digital

Em linha com a ênfase que a agenda internacional para o desenvolvimento coloca nas tecnologias digitais como facilitadoras de desenvolvimento, as TIC foram também identificadas pela Comunidade de Desenvolvimento da África Austral (SADC) como elementos vitais para a construção de uma sociedade

mais inclusiva, ao eliminarem a pobreza e reduzirem a desigualdade nos países.[3] Porém, neste ambiente, as regras e políticas que se espera possam vir a facilitar o desenvolvimento têm de responder a uma realidade peculiar, marcada pela interconectividade e pela globalização. É necessária uma mudança fundamental de políticas de um ponto de vista das telecomunicações tradicionais que vê os desenvolvimentos digitais como ocorrendo no âmbito de um sector distinto, ou até como uma questão nacional, apenas. Em vez disso, a digitalização ocorre no interior de um ecossistema complexo que abrange a totalidade da economia e da sociedade a um nível nacional, ao mesmo tempo que está inextricavelmente conectado aos, e interligado com, os mercados globais e os sistemas de governança.

Conceptualizadas como um ecossistema (Figura 1), as relações entre os diferentes elementos e os resultados decorrentes das suas interacções podem ser avaliados para efeitos de políticas. Em vez de se focar na tecnologia em rápida mudança, esta abordagem coloca os utilizadores, cidadãos e consumidores no centro do ecossistema. Até mesmo onde a infra-estrutura está disponível, a acessibilidade em termos de custos das redes, dos serviços, das aplicações e dos conteúdos no ecossistema determinará o grau de acesso que aqueles terão ao ecossistema. Estes, por sua vez, são um resultado da estrutura do mercado e da eficácia da regulação, as quais são, elas próprias, determinadas pela política e pelo enquadramento jurídico nacionais.

Mas a capacidade dos cidadãos para utilizar estas tecnologias e serviços digitais para melhorar os seus meios de subsistência e o seu bem-estar será determinada não só por um acesso a um custo acessível ou até pela sua literacia digital para consumir o serviço, mas pela educação e pelas competências para fazê-lo de forma produtiva. O acesso a um custo acessível é o resultado de um ambiente político que incentiva a expansão das infra-estruturas e a regulação efectiva da concorrência dos operadores de rede e dos prestadores de serviços. Para que a política digital possa estimular o emprego e a inovação, é essencial que exista uma estratégia integrada de investimento e de desenvolvimento humano.

Isto requer um Estado facilitador que possa atrair investimentos privados produtivos e coordenar o fornecimento de bens públicos por parte dos sectores público e privado. Mas os resultados a nível nacional são cada vez mais afectados pelas instituições multilaterais de governança internacional, como a UIT, a Organização Mundial do Comércio, a Comissão das Nações Unidas para o Direito Comercial Internacional, bem como por novas formas de governança global, como a ICANN, uma organização sem estados-membros, responsável pela governança da Internet. As organizações regionais, como a União Africana, as comunidades económicas regionais, como a SADC, e as organizações regionais especializadas, como o Fórum Parlamentar da SADC e a Associação de Reguladores de Comunicações da África Austral (CRASA) têm um papel cada vez mais importante na harmonização de políticas e na integração de mercados neste ambiente globalizado.

3 Ver, por exemplo, recentemente, em Setembro de 2018, os Ministros de TIC da SADC deliberaram que as TIC são vitais para o desenvolvimento sustentável da região, e definiram objectivos específicos sobre o acesso de banda larga, cibersegurança, conectividade rural e a quarta revolução industrial. Comunicado de Imprensa disponível em https://www.sadc.int/files/3715/3806/1649/Media_Statement__ICT_Information_Transport_and_Met_meeting.pdf

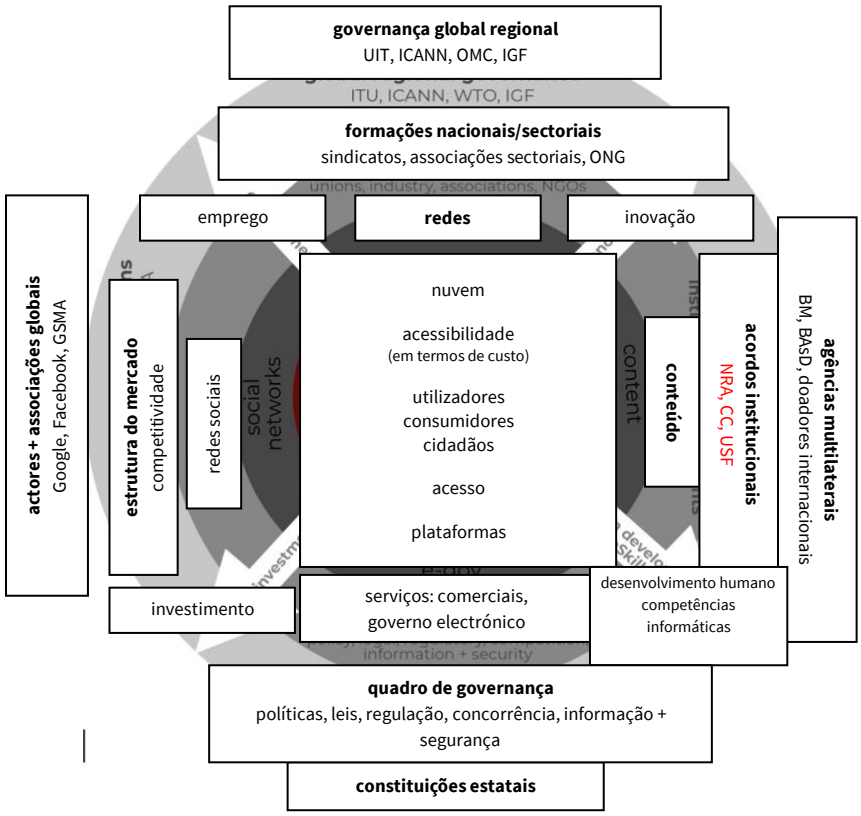

Figura 1: Uma visão *ecossistémica* do ambiente digital

As interconexões entre os diferentes componentes do ecossistema realçam a necessidade de os decisores políticos nos países em desenvolvimento verem a digitalização no contexto dos mercados e cadeias de valor globais, mas também no seu contexto local, onde a falta de prontidão digital irá limitar a sua capacidade de aproveitar estas novas tecnologias e processos e de mitigar os riscos associados ao emprego, governança de dados e acesso a financiamento.

Um aspecto fundamental nesta questão é a importância da inclusão e da igualdade digitais. Paradoxalmente, à medida que mais pessoas estão ligadas, a desigualdade digital está a aumentar. Isto não acontece apenas entre aqueles que estão *online* e aqueles que estão *offline* (como é o caso num ambiente de voz e texto simples), mas também entre aqueles que têm os recursos técnicos e financeiros para usar a Internet de maneira ideal, e aqueles que estão "escassamente" *online*. Estes últimos incluem aqueles que apenas têm um acesso parcial a serviços de dados de baixa qualidade ou muito caros que não lhes permitem estar "sempre ligados" ou usar serviços que requerem um consumo intenso de dados. O fosso entre aqueles que consomem passivamente um número limitado de serviços básicos e aqueles com a capacidade para dar à tecnologia um uso integral e produtivo, alguns até para melhorarem a sua prosperidade, está a aumentar.

Da mesma forma, à medida que estão *online* mais pessoas que não têm a consciência ou as competências para exercer os seus direitos, elas ficam mais vulneráveis aos riscos que acompanham o seu uso de novas aplicações e serviços que recolhem informação pessoal e usam algoritmos para dirigir a sua publicidade, ou às formas através das quais os governos podem controlá-las do que aquelas pessoas que têm esse conhecimento ou essas competências.

As crescentes deslocações de rendimento do trabalho para o capital e a queda nos empregos de nível intermédio em muitos países, um fenómeno comummente designado pelos economistas como polarização dos salários, sugerem que os ganhos de uma maior utilização da tecnologia não serão partilhados de forma equitativa sem significativas intervenções ao nível das políticas (Van Reenen, 2019).

É, portanto, necessária uma estratégia nacional transversal para os países em desenvolvimento para criar uma economia digital facilitadora e equitativa para a inclusão social e a prosperidade económica; para prevenir danos associados à vigilância permanente dos sujeitos dos dados por parte das plataformas monopolistas globais e pelo Estado; e para salvaguardar os direitos dos cidadãos, para criar o ambiente seguro, protegido e confiável necessário para o florescimento da economia digital. Para conseguir isto, as políticas terão de derivar de processos participados por múltiplas partes interessadas, nos quais a sociedade civil e o sector privado dialogam com o governo. Tais políticas nacionais irão requerer coordenação entre o sector público e o sector privado para dar resposta à procura nacional e para possibilitar competir eficazmente na economia global. Isto irá exigir:

- a atracção de investimento privado produtivo para a melhoria da infra-estrutura física (incluindo a energética e a de banda larga);
- a regulação económica efectiva dos fornecedores de infra-estruturas para garantir uma política de concorrência justa e uma experimentação regulatória para permitir o fornecimento de serviços de banda larga de baixo custo;
- mecanismos institucionais integrados para lidar com sistemas de informação globais adaptativos e complexos, incluindo infra-estrutura, conteúdo, dados, e novos problemas de concorrência, cuja governança exige respostas nacionais e globais;
- políticas para abrir quer os dados públicos quer os comerciais como activos críticos para novos participantes e fluxos de dados para permitir o comércio transfronteiriço, ao mesmo tempo que se protege a informação privada dos indivíduos e a segurança e a integridade dos sistemas nacionais;
- mudanças nos programas da educação básica afastando-os do ensino memorizado e de uma forma de pensamento que pode ser facilmente replicado pelas máquinas, direccionando-os para a construção de um conhecimento crítico e criativo mais adequado ao ambiente digital dinâmico, em conjunto com programas transversais de competências digitais de grande dimensão para alinhar e escalonar com os requisitos da nova mão-de-obra;
- mecanismos de financiamento para expandir o acesso a estes novos meios de produção para integração de cadeias de abastecimento, comércio regional e competitividade global, e para harmonizar os enquadramentos regionais para melhorar o comércio e permitir os fluxos transfronteiriços de dados; e
- eliminação da tributação excessiva sobre as empresas que desincentiva o investimento em redes e da tributação regressiva sobre redes sociais que reduz a utilização pelos pobres e empenho na reforma do regime de tributação digital global que pretende a tributação de produtos digitais e serviços na jurisdição na qual os rendimentos são gerados, mesmo que o produtor não possua aí uma presença física.

Nem o Documento de Trabalho nem o Relatório de Síntese são capazes de lidar em profundidade com todas as questões ligadas a políticas relacionadas com este ambiente facilitador. Em vez disso, eles focam-se nas considerações relativas a políticas e governança para os países em desenvolvimento aproveitarem os benefícios da maior eficiência, da melhoria da produtividade e da criação de valor

associados à economia digital baseada em dados, ao mesmo tempo que realçam a necessidade de corrigir a desigualdade digital como pré-condição para inclusão na economia digital. Isto é feito de forma a conceber um enquadramento ambiental e político ponderado que possa suportar, e implementar, os objectivos de um Direito da Economia Digital.

Parte B: Contexto Jurídico

3. Fundamentos para a Lei Modelo

A economia digital apresenta algumas oportunidades claras. Em África, actualmente, a contribuição da Internet para o crescimento do PIB permanece baixa. Mas, apesar disso, existem sinais de que as economias emergentes, em particular, podem desfrutar, no futuro, de benefícios reforçados, com a Internet a acrescentar um valor significativo ao PIB de África (Manyika, J., *et al.*, 2013).

Na SADC, qualquer discussão sobre potenciais oportunidades para crescimento e ganhos resultantes da economia digital deve ser contextualizada no âmbito dos riscos associados de desigualdade e exclusão. Ao considerar qual poderá ser o papel dos parlamentos nacionais na contribuição para esta economia digital, o forte legado regional em termos de enquadramentos de direitos humanos serve como uma base útil para explorar intervenções no interior deste espaço, particularmente dada a sua capacidade de incorporar normas sociopolíticas nas políticas económicas.

Ao aprofundar a ponderação dos assuntos relevantes para analisar o mandato legislativo para a economia digital, o Documento de Trabalho avalia os componentes e as condições fundamentais para uma "boa" economia digital, estabelecendo algumas recomendações essenciais (pormenorizadas mais à frente), mas também propondo um enquadramento para avaliar o que as leis nacionais teriam de levar em consideração ao implementar uma Lei Modelo para a Economia Digital. Portanto, no âmbito desta abordagem *ecossistémica* mais alargada, a abordagem para esta discussão sobre os enquadramentos político e jurídico necessários para optimizar a economia digital pode ser descrita como:

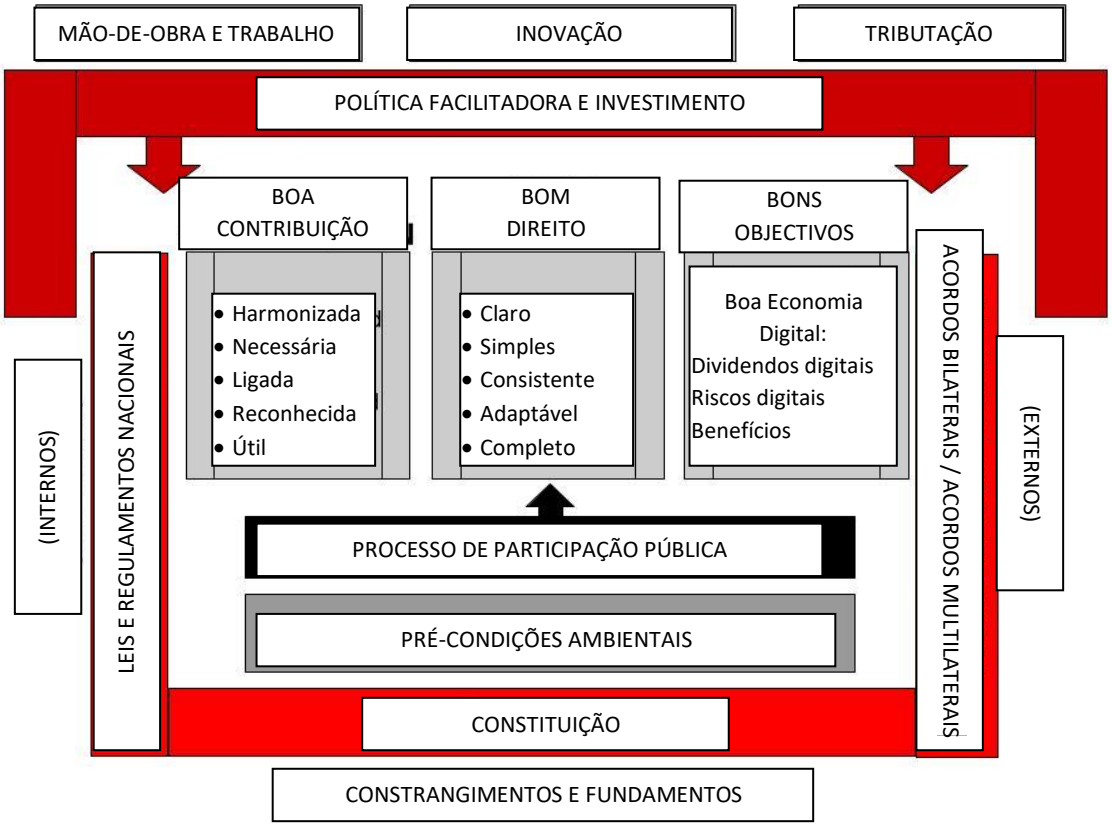

Figura 2: Diagrama do enquadramento para o desenvolvimento de uma Lei Modelo para a Economia Digital

O enquadramento reconhece que é necessária uma estratégia nacional transversal para os países em desenvolvimento para criarem uma economia digital facilitadora e equitativa para a inclusão social e a prosperidade económica; para prevenir danos associados à vigilância permanente dos sujeitos dos dados por parte das plataformas monopolistas globais e pelo Estado; e para salvaguardar os direitos dos cidadãos, para criar o ambiente seguro, protegido e confiável necessário para o florescimento da economia digital. Para conseguir isto, as políticas terão de derivar de processos participados por múltiplas partes interessadas, nos quais a sociedade civil e o sector privado dialogam com o governo.

Os objectivos da Lei Modelo não devem simplesmente procurar encorajar a economia digital, pois encorajar a economia digital "tal como está" irá apenas aumentar os riscos e as desigualdades digitais. Em vez disso, o objectivo deve ser criar uma lei e uma política que promovam uma "boa" economia digital, que será uma economia digital definida por:

- inclusividade;
- objectivos em termos de direitos humanos;
- competitividade;
- abertura;
- regulação e planeamento;
- flexibilidade; e
- facilitação dos mercados nacionais.

Para conseguir isto, é necessário estabelecer princípios que possam formar a base da produção legislativa nos contextos nacionais, conhecedores dos objectivos da colaboração regional, e as fundações de uma boa economia digital que possa beneficiar todos. As posições descritas abaixo serão o primeiro passo no sentido de considerar uma elaboração da Lei Modelo baseada em princípios.

4. Direitos humanos

Os direitos humanos[4], naturalmente, consolidam-se mutuamente e estão interligados. Os princípios dos direitos humanos, que são fortemente impulsionados por toda a região, quer através de entidades regionais de direitos humanos, quer dos parlamentos e dos sistemas judiciais nacionais, devem servir como o padrão normativo para a incorporação de imperativos sociais no âmbito do clima económico de uma Lei Modelo para a Economia Digital.

Dada a paisagem da economia digital, centrada nos dados e na informação, as referências a direitos existentes no leque de direitos cívico-políticos são bastante comuns – e de particular importância ao considerar os constrangimentos, e as ambições, de uma Lei Modelo para a Economia Digital, são os direitos de privacidade, de acesso à informação e de liberdade de expressão. É certo que, embora estes direitos tenham fortes ligações ao ambiente facilitador para a economia digital em particular (por exemplo, na sua associação a instrumentos facilitadores como as telecomunicações e a Internet enquanto infra-estruturas digitais), existem seguramente direitos socioeconómicos relevantes, tais como o direito ao trabalho e o direito à desigualdade. Porém, pelo menos para o exercício de providenciar um enquadramento (em particular um enquadramento jurídico, dados os limites de alguns direitos

4 Ver Anexo 1.

socioeconómicos), o documento focar-se-á em componentes do espectro cívico-político para analisar disposições constitucionais específicas no interior da SADC e debruçar-se-á sobre categorizações de direitos mais amplas sob as áreas de políticas.

5. Mapeamento legislativo nacional na SADC

Voltando ao Enquadramento da Lei Modelo descrito na *Figura 2* analisar o contexto jurídico necessita de uma referência para ambos os instrumentos regionais relevantes (descritos no Anexo 1A), bem como de princípios e linhas de orientação chave regionais (descritos no Anexo 1B). Além disso, têm de ser analisados os contextos legislativos nacionais para as diferentes áreas de posicionamento. Nos restantes anexos está disponível um mapeamento preliminar de tais instrumentos. constitucionais e legislativos nacionais.

Embora o Documento de Trabalho analise exaustivamente tanto os instrumentos da SADC como as leis nacionais da SADC, vale a pena providenciar uma panorâmica sumária da transposição para as legislações nacionais dos instrumentos da SADC, transversalmente a vários domínios políticos.

5.1 Propriedade, controlo e acesso aos dados

Lei Modelo da SADC sobre a Protecção de Dados

O Projecto de Lei Modelo da SADC sobre a Protecção de Dados (2013) inclui duas formulações principais. O artigo 43 regula os fluxos transfronteiriços de dados entre países da SADC que transpuseram a Lei Modelo para as suas legislações nacionais. Os artigos 44 e 45 regulam a transferência transfronteiriça de dados de um país da SADC que transpôs a Lei Modelo para a sua legislação nacional para um país que não integra a SADC ou para um Estado-Membro da SADC que não tenha transposto a Lei Modelo para a sua legislação nacional.

Enquadramentos Jurídicos Nacionais sobre a Privacidade de Dados na SADC

A África do Sul, Angola, o Botswana, o Lesoto, Madagáscar, as Maurícias e as Seychelles promulgaram leis sobre a protecção de dados. Porém, apenas a lei das Maurícias está plenamente em vigor, em especial no que diz respeito ao estabelecimento de uma autoridade independente de protecção de dados (APD), que é amplamente reconhecida como um elemento essencial para uma efectiva aplicação das leis relativas à privacidade de dados. Na África do Sul, o seu Regulador de Informação foi estabelecido, mas a Lei só está parcialmente em vigor (as secções 1, 112, 113 e o Cap. 5 Parte A começaram sob a proclamação N.º R. 25, 2014). A falha em nomear atempadamente uma APD é repetidamente apontada como sendo um impedimento principal à aplicação efectiva das leis de protecção de dados, e isto ocorre mais frequentemente em África do que em outros locais (Greenleaf, 2011). Um aspecto positivo é que todas as APD existentes gozam do estatuto de agências independentes (Greenleaf, 2011).

Outros países têm projectos-lei oficiais sobre a privacidade de dados e espera-se que brevemente vários deles venham a ser promulgados. Estes países são as Comores, o Reino de Eswatini, a Tanzânia, a Zâmbia e o Zimbabwe. A Zâmbia ractificou a Convenção sobre o Cibercrime e a Protecção de Dados da UA antes de promulgar uma lei sobre a privacidade de dados, que o Governo tinha aprovado em Julho de 2018 (Greenleaf, 2018). No Zimbabwe, a única lei que trata da Protecção de Dados, ou da protecção da privacidade pessoal, é a *Lei do Acesso à Informação e da Protecção da Privacidade* (2002).

Em 2013, a Tanzânia iniciou um processo de reforma jurídica com o objectivo de transpor a Lei Modelo da SADC para a lei nacional. Através do projecto HIPSSA, e com apoio financeiro, técnico e especializado da UIT, da Comissão Europeia e da União Europeia, a Tanzânia elaborou o seu primeiro projecto-lei

exaustivo sobre a protecção de dados, intitulado "Projecto-Lei sobre a Privacidade e a Protecção de Dados", que foi renomeado, em 2014, como "Projecto-Lei sobre a Protecção de Dados Pessoais". Os restantes países da SADC não têm leis independentes nem projectos-lei oficiais sobre a protecção de dados. Estes são Moçambique, a Namíbia e a República Democrática do Congo.

Os princípios mais importantes de protecção de dados que divergem entre as jurisdições da SADC incluem, portanto: i) o registo junto de uma Autoridade de Protecção de Dados (APD); ii) a autorização da APD para o processamento de certas categorias de Dados; iii) a aplicabilidade territorial das leis; iv) as transferências transfronteiriças de dados; v) a notificação de violação de dados; vi) a nomeação de um Responsável pela Protecção de Dados (RPD); vii) o desenvolvimento de Códigos de Conduta ou Ética.

Enquadramentos Jurídicos Nacionais sobre Acesso à Informação na SADC

A Lei Modelo sobre o Acesso à Informação para África é um importante instrumento de referência na região. Designadamente, a Lei Modelo coloca uma forte ênfase em disposições de divulgação proactiva direccionadas e pormenorizadas.

Na SADC, a África do Sul, Angola, o Malawi, Moçambique, as Seychelles, a Tanzânia e o Zimbabwe têm leis autónomas sobre o acesso à informação (embora, mais uma vez, tenha havido críticas, provenientes de alguns quadrantes, acerca da lei do Zimbabwe, por fazer mais para restringir, do que para facilitar, o acesso).

Tem havido campanhas árduas em toda a região em defesa de leis de acesso à informação, e há anos que países como o Botswana, as Maurícias, a Namíbia e a Zâmbia não têm notoriamente sido capazes de aprovar projectos-lei sobre o acesso à informação (o Lesoto, Madagáscar e a Suazilândia têm também projectos-lei em progresso). As Comores não têm, actualmente, qualquer legislação no horizonte.

A maior parte destas leis não possui disposições exaustivas sobre divulgação proactiva, apesar da Lei Modelo.[5] Também não existe uma forte consistência na provisão de Reguladores, o que coloca desafios à adaptabilidade das leis, limitando também o acesso a recurso por parte das empresas e dos cidadãos.

5.2 Segurança dos dados e interferência nos mesmos

Enquadramentos Jurídicos Nacionais sobre Cibersegurança e Cibercrime

Para além da legislação focada especificamente no cibercrime, o Malawi, a Zâmbia e o Zimbabwe possuem leis mais abrangentes sobre a cibersegurança. Angola também promulgou, em 2017, uma lei de cibersegurança sobre a protecção das redes de informação. O Projecto-Lei sobre Cibercrime da África do Sul (dividido do controverso Projecto-Lei sobre Cibercrimes e Cibersegurança, de 2017) aguarda a promulgação presidencial. Entretanto, as Comores e a República Democrática do Congo não têm qualquer legislação proposta ou ractificada sobre cibersegurança. Relativamente à vigilância e à intercepção de comunicações, em particular, a África do Sul e o Zimbabwe têm legislação expressamente dedicada à intercepção de comunicações. Vale a pena, neste contexto, considerar a recente sentença na África do Sul relacionada com a legislação sobre intercepção, *Centro de Jornalismo de Investigação Amabhungane NPC e Outro* v. *Ministério da Justiça e dos Serviços Prisionais* [2019] ZAGPPHC 384.[6] O tribunal considerou que certos aspectos da lei são inconstitucionais, porque os

5 Curiosamente, alguns destes países viram as suas leis serem directamemte comparadas com a Lei Modelo, e o resultado pode ser consultado aqui: http://www.africanplatform.org/fileadmin/Content/PDF/Resources/State-of-ATI-in-Africa-2017.pdf.

6 Ver aqui a breve discussão do caso providenciada anteriormente no título "2.1.1 Vigilância".

aspectos procedimentais descritos para conseguir obter permissões nos termos da Lei estavam em geral insuficientemente pormenorizados e não conseguiam proporcionar a adequada supervisão dos pedidos.

Foram promulgados projectos-lei dedicadas ao cibercrime em Madagáscar em 2014, nas Maurícias em 2003, nas Seychelles em 1998, na Namíbia em 1988, no Zimbabwe em 2004 e 2019, e na África do Sul e na Zâmbia em 2004 e 2018 (embora, tal como mencionado, o Projecto-Lei sobre Cibercrimes de 2017 da África do Sul se encontre agora a aguardar a promulgação presidencial), embora a Lei sobre o Uso Informático Indevido nas Seychelles e na Namíbia tenha sido identificada como inadequada para o cenário tecnológico actual. Projectos-lei sobre cibercrime, embora ainda não ractificados, foram também introduzidos no Botswana em 2018, em Eswatini em 2014, e na Namíbia, no Lesoto e nas Seychelles em 2013.

Avaliações da capacidade e da maturidade dos países

Um aspecto importante frequentemente referido no contexto da cibersegurança é não apenas os riscos que coloca, mas as capacidades do Estado e das suas agências para combater o cibercrime. O Índice Global da Cibersegurança (UIT, 2018) indica que apenas as Maurícias demonstraram um alto nível de empenho em todos os cinco pilares do seu índice. De facto, nem Angola, nem a República Democrática do Congo, nem o Lesoto participaram no estudo de 2018, e têm todos uma classificação de “baixo”, como países que apenas começaram a dar início a compromissos relativamente à cibersegurança (outros países da SADC com classificação de “baixo” incluem as Comores, Madagáscar, o Malawi, Moçambique, a Namíbia, as Seychelles, a Suazilândia e o Zimbabwe). A África do Sul, o Botswana, a Tanzânia e a Zâmbia estão classificados como países de nível “médio”, “que desenvolveram compromissos complexos e estão envolvidos em programas e iniciativas de cibersegurança”.

5.3 Criação de valor baseada em dados

Prontidão em termos de comércio electrónico

Segundo o Índice de Comércio Electrónico de 2018 da UNCTAD, a média regional em África foi de 30, muito abaixo da média mundial de 55 (UNCTAD, 2018). Porém, desde 2014 “a África subsaariana tem ultrapassado o crescimento global em três dos indicadores usados no índice” (UNCTAD, 2018).

Dinheiro móvel e pagamentos electrónicos

O Projecto dos Sistemas de Pagamento é um projecto bastante activo na SADC, em reconhecimento directo dos benefícios da economia digital que podem ser facilitados pelo pagamento digital. Este projecto foi desenvolvido sob a Subcomissão de Pagamentos do Gabinete do Comité de Governadores dos Bancos Centrais (CCBG) da SADC (Abrahams, 2017). Além disso, as Orientações sobre Dinheiro Móvel (que seguiram uma revisão solicitada pela CCBG) providenciam úteis orientações jurídicas e regulatórias, adoptando um modelo em que as licenças de dinheiro móvel só podem ser concedidas por um banco central (Abrahams, 2017).

Enquadramentos Jurídicos Nacionais sobre PI e Direitos de Autor

Todas as jurisdições da SADC têm uma forma de legislação de direitos de autor e patentes com uma forte tendência para ter as leis enquadradas num contexto industrial e comercial. As análises contextuais parecem indicar que os desafios não se encontram necessariamente numa lacuna de instrumentos legais, mas antes na acessibilidade desses instrumentos para permitir aos criadores e aos inovadores gerarem valor (bem como, de forma mais geral, em ambientes insuficientemente facilitadores da inovação) (Phiri, 2008). Estudos feitos um pouco por todo o continente sugerem que a maior parte dos

países africanos possui direitos suficientes para os criadores, mas não tem excepções e limitações adequadas (Armstrong *et al.*, 2010).

Integrações regionais

Enquanto bloco comercial, a SADC está bem adaptada para a coordenação de PI e de Direitos de Autor (Nkomo, 2014), e pode ser capaz de ultrapassar algumas insuficiências sentidas pela Organização Regional Africana da Propriedade Intelectual (ARIPO). Vários países da SADC, incluindo a África do Sul, Angola, Moçambique e Madagáscar não são membros desta organização.

Parte C: Posições em Termos de Políticas

6. Estrutura das secções relativas a políticas

Existem três áreas gerais sob as quais organizámos as recomendações relativas a posições em termos de políticas:

- propriedade, controlo e acesso aos dados;
- segurança dos dados e interferência nos mesmos; e
- criação de valor baseada em dados.

Dentro de cada um destes temas em termos de políticas gerais, existem subtemas como uma forma suplementar de ajudar a organizar as opções em termos de políticas. Isto ajuda a dar resposta à complexidade do conteúdo, mas segue também as áreas funcionais legislativas tradicionais, que podem ajudar a avaliar como estas áreas se poderão aplicar num contexto nacional:

Área de Política Principal	Subtema	Subtema	Subtema
Propriedade, controlo e acesso aos dados	Protecção dos dados e privacidade	Acesso aos dados e à informação	
Segurança dos dados e interferência nos mesmos	Cibersegurança e Vigilância	Cibercrimes	Restrições de acesso
Criação de valor baseada em dados	Comércio electrónico e transacções electrónicas	Propriedade intelectual e direitos de autor	

No Documento de Trabalho, existem recomendações mais gerais contidas na descrição dos assuntos que precede cada secção de recomendações. De forma a apreciar integralmente o contexto das recomendações específicas, mas também para avaliar outras áreas gerais que possam ser norteadas pelos princípios de uma Lei Modelo, deverá ser considerado o Documento de Orientação mais completo.

7. Opções e recomendações em termos de políticas: Propriedade, controlo e acesso aos dados

Subtema da Política	Tópico da Política	Recomendação
Vigilância	**Processamento lícito de dados**	Tipicamente, as leis preparadas para proteger a privacidade dos indivíduos em termos de informação prevêem orientações e limites à forma como essa informação

		pode ou não pode ser processada. Os princípios do processamento da protecção de dados podem incluir: • limitações à recolha; • especificação dos fins; • limitação do uso; • qualidade dos dados; • salvaguardas de segurança; • abertura (que inclui a comunicação de incidentes, uma importante correlação com os imperativos em termos de cibersegurança e cibercrime); e • responsabilidade. E durante todo este processamento, os direitos dos sujeitos dos dados têm de ser cumpridos e respeitados, correspondendo estas obrigações a uma variedade de direitos dos sujeitos dos dados. Algumas destas áreas de políticas serão especificadas em maior pormenor mais à frente.
	Minimização dos dados	O Projecto de Lei Modelo da SADC sobre Protecção de Dados trata das "regras gerais para o processamento de dados pessoais" e coloca a ênfase no direito do controlador dos dados de recolher apenas informação pessoal para um fim específico e legítimo. Na 4.ª Revolução Industrial (4IR), a protecção da privacidade não pode ser concretizada restringindo simplesmente a recolha de dados ou restringindo a utilização de computadores ou de tecnologias em rede. De forma a equilibrar as consequências negativas de regular excessivamente a privacidade restringindo a utilização das TIC, tem de ser encontrado um equilíbrio entre minimizar a recolha de dados pessoais e permitir o livre fluxo de dados pessoais para dar resposta às necessidades de análise de grandes volumes de informação e de produção de conhecimento, para aproveitar as oportunidades das economias e sociedades baseadas em dados (Brankovic e Estivill-Castro, 1998). Um ponto importante a ter em conta neste enquadramento é a avaliação dos benefícios públicos directos que podem ser facilitados pela transferência de dados, particularmente no âmbito da área da investigação, mas também para facilitar o comércio (e a avaliação de risco).
	Integridade dos dados	Ligada ao entendimento de que os dados podem ter benefícios económicos e públicos está a ideia de que os direitos dos sujeitos dos dados são importantes não apenas para garantir a privacidade, mas também para ajudar a contribuir para, e a sustentar, a integridade dos dados. A integridade dos dados refere-se à precisão e consistência dos dados, o que tem claramente impacto nos seus benefícios económicos mais amplos, mas também, potencialmente, no tratamento ou nos resultados de dados específicos de sujeitos dos dados individuais. Isto pode ser facilitado através de obrigações positivas relativamente ao processamento de dados, mas também através da garantia de que os direitos dos sujeitos dos dados incluem direitos proactivos de aceder aos, e de solicitar a alteração dos, seus dados pessoais.
	Dados pessoais não identificados e anonimizados	A maioria dos regulamentos de protecção de dados sugerem que os dados não identificados não são dados pessoais, porque não pertencem a um indivíduo identificável. Mas os dados não identificados são cada vez mais passíveis de poderem ser novamente identificados. Isto requer, portanto, mais escrutínio dos métodos de agregação de dados e tratamento por terceiros dos dados agregados para minimizar as ameaças de má utilização dos dados não identificados. Por outro lado, os dados anonimizados permanecem anonimizados e não colocam grandes

		preocupações à regulação de dados pessoais, embora o controlo exclusivo dos dados anonimizados possa levantar preocupações em termos de concorrência. Deverão ser desenvolvidos indicadores práticos para as empresas compreenderem como facilitar as opções, dada a centralidade da construção de confiança na esfera da privacidade, o que seria facilitado pela APD.
	Consentimento	O consentimento subjaz a muito do processamento lícito, enquanto mecanismo-chave para definir a permissão por parte dos indivíduos para a utilização dos seus dados pessoais. Enquanto "acto" permissivo central, o que constitui consentimento é excepcionalmente importante; e a natureza desse consentimento é que o mesmo deve ser voluntário e informado. O ambiente digital apresenta desafios significativos relativamente ao que pode querer dizer a realidade do consentimento informado. No entanto, uma APD devidamente capacitada que possa providenciar as melhores práticas quer para os colectores quer para os processos, ao mesmo tempo que providencia orientação sobre as ferramentas tecnológicas disponíveis para o público poder melhorar a realidade da concessão de consentimento, pode ser fundamental.
	Segurança	O Artigo 25 da Lei Modelo da SADC refere-se às violações de segurança e exige uma comunicação sem demoras indevidas. Mas a Lei Modelo não especifica o que constituiria uma violação de segurança, ou demora indevida, ou o que seria considerado como causa razoável para demora. Além disso, não estabelece, para o controlador de dados, a obrigação de explicar à APD o porquê da demora. O Artigo nem sequer estabelece a obrigação de o controlador de dados ter de notificar o sujeito dos dados da ocorrência de uma violação. Além disso, não existe nenhuma exigência de que o controlador de dados e o processador de dados tenham de divulgar qual a informação que foi comprometida. Isto não está em consonância com o Preâmbulo, o qual apela à transparência e responsabilidade por parte do controlador de dados e do processador de dados. E, muito importante, estabelecer estas obrigações para um controlador de dados não tem de ser oneroso se existir uma APD que possa providenciar orientação. Os controladores de dados podem definir procedimentos de notificação quando cumprem inicialmente as obrigações relativas a dados pessoais de modo a que, na maioria dos casos, isto só necessite de ser feito uma única vez. O controlador de dados deve notificar a APD e o sujeito dos dados acerca da informação que foi comprometida e sugerir formas de se salvaguardarem de ataques. Isto deve-se ao facto de a própria empresa estar mais bem colocada para compreender a natureza e a extensão da violação. Sem criar estas formas de obrigações positivas, as leis não serão capazes de providenciar uma transparência adequada.
	Privacidade desde a concepção	A privacidade desde a concepção é a abordagem adoptada quando se desenvolvem tecnologias e sistemas digitais, através da qual a privacidade é incorporada por defeito nas tecnologias e nos sistemas durante o processo de concepção e desenvolvimento. Significa que um produto é concebido com a privacidade como prioridade, juntamente com quaisquer outros propósitos que o sistema sirva. O Projecto de Lei Modelo da SADC sobre Protecção de Dados não coloca ênfase no princípio da "privacidade desde a concepção", que é um aspecto importante a considerar no que diz respeito à 4.ª Revolução Industrial (4IR). Assim, recomendamos que em vez de estabelecer "obrigações de caixas de verificação" para o controlador de dados, a ênfase deve estar em solicitar ao controlador de dados que não só cumpra simplesmente os regulamentos de protecção de dados que lhe foram impostos, mas também que implemente medidas e procedimentos técnicos e organizacionais adequados de uma forma tal que todas as actividades de processamento de dados, incluindo a recolha, armazenamento e uso dos dados,

		cumpram os requisitos de protecção de dados, garantindo ao mesmo tempo a protecção dos direitos do sujeito dos dados. Estas formas de obrigações positivas para as empresas são capazes de coagir de um modo muito prático as mudanças nas práticas de protecção de dados, mas não têm de ser altamente punitivas.
	Fluxos de dados	O fluxo de dados é uma realidade fundamental da forma como a digitalização e a globalização têm impulsionado a economia digital. À medida que mais e mais actividades económicas e sociais se deslocam para o mundo *online*, a importância da protecção de dados e da privacidade é cada vez mais reconhecida, especialmente no contexto do comércio internacional. A protecção de dados está directamemte relacionada com o comércio de bens e serviços na economia digital. A protecção insuficiente pode criar efeitos negativos no mercado ao reduzir a confiança dos consumidores, e uma protecção demasiado rigorosa pode restringir as actividades das empresas de forma indevida, tendo como resultado efeitos económicos adversos. Garantir que as leis têm em consideração a natureza e o âmbito globais da sua aplicação, e fomentar a compatibilidade com outros enquadramentos, é da maior importância para os fluxos do comércio global que cada vez mais dependem da Internet. É crucial dar resposta à questão das transferências transfronteiriças de dados usando texto específico e promovendo um ou mais mecanismos que as empresas possam usar para facilitar os fluxos internacionais de dados.
	Cooperação transfronteiriça, harmonização e padrões mínimos	As limitações à transferência transfronteiriça de dados podem resultar em oportunidades de negócio perdidas e reduzir a capacidade de uma organização fazer comércio a nível internacional, levando a uma presença geográfica reduzida e à perda de competitividade nos mercados. Mas uma regulação de dados que esteja sincronizada com a de outras jurisdições contribui para a confiança mútua e lança as bases para uma troca de dados confiável, incluindo (mas não limitada a) dados pessoais. Uma ideia errada sobre a harmonização da protecção de dados provém da não compreensão de que a harmonização requer que todas as leis nacionais sejam idênticas. Esta abordagem não leva em consideração as diferenças nacionais em termos de enquadramentos existentes, ou dos avanços na inovação tecnológica. A harmonização deve, antes, ser procurada através da compatibilidade entre as legislações nacionais, com base num conjunto acordado de princípios fundamentais de protecção de dados.
	Autoridades de Protecção de Dados	Autoridades de protecção de dados independentes, acessíveis e com disponibilidade de recursos (quer em termos de recursos financeiros, quer em termos de recursos humanos) são um aspecto importante na concretização do equilíbrio entre a elaboração de regras flexível e uma supervisão responsável. A eficácia das APD também depende da extensão das suas competências estabelecida na Lei que as implementa, nomeadamente no que diz respeito à capacidade de investigação e de emissão de ordens vinculativas relativamente ao seu mandato. Uma APD capacitada e bem dotada de recursos pode ajudar a suavizar os ónus da conformidade para o sector privado e o sector público.
	Remédios eficazes e justiça administrativa	Para lá dos procedimentos de notificação, os sujeitos dos dados devem ter a garantia de que possuem um acesso adequado a remédios. Porém, isto estende-se para lá do acesso a uma APD. Isto é assim porque, de forma a facilitar a elaboração adaptável de regulamentos, as APD precisam de ser capacitadas adequadamente. Por exemplo, capacitar uma APD para permitir exclusões ponderadas ajuda a prevenir que as obrigações positivas geradas sejam inadequadamente onerosas

		para diferentes formas de negócios. Porém, de forma a facilitar este tipo de flexibilidade, é necessário um paradigma de justiça administrativa adequado que possa garantir a responsabilização por tais decisões. Um outro componente interessante é a restrição, a qual está demonstrada na lei sul-africana que proíbe a tomada de decisões automatizada. No contexto da IA, estas proibições são dignas de nota.
	Soberania dos dados	Existem duas abordagens sobre a soberania dos dados, uma fraca e outra forte: por um lado, uma soberania dos dados fraca refere-se às iniciativas de protecção de dados promovidas pelo sector privado com a ênfase nos aspectos dos direitos digitais da soberania dos dados; por outro lado, uma soberania dos dados forte favorece uma abordagem liderada pelo Estado, com a ênfase na salvaguarda da segurança nacional. Contudo, a localização dos dados vai para além da regulação das condições para a transferência, e obriga a que todos os dados pessoais sejam detidos ao nível nacional. Este extremo pode, porém, interferir com os objectivos da economia digital e nunca deverá substituir o passo mais fundamental das leis de processamento de dados.
Acesso aos dados e à informação	**Dados abertos**	As leis sobre o acesso à informação devem possuir uma orientação clara acerca dos dados abertos. Embora as políticas de dados abertos sejam um passo necessário para garantir dados governamentais abertos a nível nacional, uma orientação legislativa pode ajudar a criar um ambiente mais facilitador para a aprovação de tais políticas públicas. No âmbito destes enquadramentos, os governos "… devem dar prioridade à recolha de dados qualitativos e quantitativos desagregados por género sobre a participação das mulheres na economia digital de forma a nortear o diálogo significativo e a elaboração de políticas", mas também para melhorar os benefícios positivos dos dados governamentais (UNECA, 2019). Por outras palavras, as obrigações devem estender-se para lá da mera divulgação, de forma a incluírem a obrigação positiva de gerar dados de certos tipos e de acordo com certos padrões. Estas obrigações de geração podem contribuir significativamente para criar a harmonização em questões de biometria e da recolha de outros dados por parte do Estado.
	Explicabilidade, transparência e algoritmos	Existem desafios à transparência, práticos e normativos, que são gerados através do crescimento nos serviços de tomada de decisões automatizada e baseados em algoritmos. Uma solução relativamente aos algoritmos é considerada como "o direito à explicabilidade" potencialmente gerado a partir de um composto de direitos do sujeito dos dados no Regulamento Geral de Protecção de Dados da União Europeia (RGPD), o qual requer que os colectores de dados pessoais expliquem aos sujeitos dos dados como é que os dados estão a ser processados e utilizados (o que pode explicar a parcialidade dos algoritmos). Outra forma de assegurar a transparência no âmbito dos algoritmos é prevenindo a tomada de decisões automatizada (tal como a proibição contra a tomada de decisões automatizada constante da secção 17 da Lei de Protecção da Informação Pessoal, 2013). Enquanto estas proibições têm, obviamente, algumas excepções, elas procuram dar resposta a um aspecto muito específico da transparência

		algorítmica: as *decisões* tomadas com base em algoritmos que são baseados em *dados pessoais*. Pode também ser muito instrutivo considerar como os paradigmas existentes de acesso à informação podem ser alterados ou utilizados para servir alguns dos fins descritos.
	Direitos dos sujeitos dos dados	Ligados aos mandatos de protecção de dados e privacidade, os sujeitos dos dados precisam de direitos que eles possam afirmar para procurar impor a transparência. Os direitos positivos dos sujeitos dos dados, que permitem aos sujeitos aceder, avaliar, rever e eliminar a sua informação, podem ser associados tanto à protecção de dados como ao acesso aos dados.
	Identidade digital	Ligado ao controlo dos dados pessoais está o direito dos sujeitos dos dados a ter uma boa identidade digital. A identidade digital é um facilitador essencial para se poder usufruir de serviços digitais públicos e privados, bem como uma necessidade para se poder colher as formas de dividendos digitais. Em 2017, o Banco Mundial, no âmbito do seu programa ID4D, desenvolveu "Princípios de Identificação para o Desenvolvimento Sustentável". Incluindo orientações como garantir cobertura universal e segurança robusta, estes Princípios foram depois usados como as bases para o movimento #Boa ID. Estes tipos de princípios devem nortear o estabelecimento de sistemas de identidade digital concebidos pelo sector público e pelo sector privado, os quais são sustentados por enquadramentos adequados de governança de dados (o papel dos direitos dos sujeitos dos dados sustentará o estabelecimento da boa identidade digital na África do Sul). Contrariamente, porém, aos benefícios elencados dos sistemas de boa identidade, os sistemas de má identidade podem desempenhar um papel na exclusão e, até, no crescimento das desigualdades vividas para os cidadãos. Isto reitera a necessidade de uma APD que sustente a existência dos imperativos de justiça de dados, suportados por processos de dados lícitos aplicáveis a cada interveniente na cadeia de valor da identidade digital, quer seja no sector público ou no sector privado.

8. Opções e recomendações em termos de políticas: Segurança dos dados e interferência nos mesmos

Subtema das políticas	Tópico das políticas	Recomendação
Cibersegurança e Vigilância	**Estratégias de cibersegurança**	O primeiro passo para uma política de cibersegurança e um quadro regulatório eficazes é uma estratégia de cibersegurança, a qual deve estar alinhada com a lei. Enquanto contribuintes para outros esforços regulatórios, os Estados-Membros devem publicar uma estratégia nacional para a cibersegurança que dê resposta às oportunidades económicas inclusivas e

		aos riscos associados à implantação das TIC. Os elementos da estratégia que se devem alinhar com a lei, incluem: ❖ nomeação de uma autoridade competente e a clara definição da sua autoridade; identificação das principais entidades governamentais afectadas e/ou responsáveis pela implementação da estratégia nacional para a cibersegurança; ❖ identificação dos mecanismos necessários para proteger a infra-estrutura informática crítica e a implantação das TIC; ❖ identificação de serviços críticos (além das infra-estruturas críticas) que a estratégia tenciona tornar mais seguras e resilientes; etc.
	Resposta a incidentes, comunicação e partilha de dados	Na eventualidade de desastres informáticos de origem natural ou humana que afectem serviços críticos e infra-estruturas de informação, cada Estado-Membro precisa de ter uma capacidade nacional eficaz de resposta a incidentes. Os Estados-Membros devem estabelecer e manter Equipas Nacionais de Resposta a Incidentes de Segurança Informática (ENRISI) ou Equipas de Resposta a Emergências Informáticas (EREI). As ENRISI devem servir um público nacional alargado (para além do governo e dos fornecedores de infra-estruturas críticas), como as obrigações proactivas relativas à comunicação de incidentes (um factor essencial no combate às ciberameaças). Para este fim, as ENRISI devem recolher dados de qualidade sobre os tipos de incidentes e riscos. As ENRISI devem também facilitar a partilha de informação horizontalmente de forma transversal pelas agências governamentais, enquanto acto de segurança nacional. O regime de acesso à informação também pode facilitar a partilha de informação.
	Coordenação transfronteiriça e resposta conjunta	Combater os ciberataques requer coordenação transfronteiriça. A União Europeia estabeleceu recentemente um regime de sanções conjuntas para os ciberataques, o qual é um modelo que a SADC poderá replicar. Embora esta seja uma questão que tem mais a ver com a organização regional, os parlamentos nacionais terão de garantir um nível de base de prontidão de cibersegurança de forma a possibilitar um envolvimento proactivo. Estes deverão também ter um enfoque no cibercrime.
Cibercrime	**Aplicação da lei relativa ao cibercrime**	O cibercrime transcende as fronteiras nacionais e requer soluções transnacionais e abordagens internacionais, multinacionais e regionais. Ao desenvolverem as capacidades de aplicação da lei para combater o cibercrime através da ractificação de tratados, da cooperação internacional, do desenvolvimento de capacidades, da implementação de programas anti-botnet e outras iniciativas, os países podem mitigar os seus ciber-riscos e impulsionar o crescimento económico futuro. Os Estados-Membros devem mostrar um empenho internacional em proteger a sociedade contra o cibercrime e construir proactivamente capacidade nacional de aplicação da lei relativa ao cibercrime, desenvolvendo legislação e quadros regulatórios. Isto assume a forma de um envolvimento em fóruns internacionais dedicados a dar resposta às questões do cibercrime internacional bem como

		ao estabelecimento de mecanismos nacionais jurídicos e regulatórios para combater, e processar judicialmente, o cibercrime. As autoridades jurídicas e regulatórias designadas para realizar actividades para travar o cibercrime têm de definir aquilo que constitui um cibercrime e capacitar as entidades governamentais com os mecanismos, o conhecimento especializado e os recursos para investigar e processar judicialmente de forma eficaz as actividades de cibercrime.
	Criminalização	Uma ênfase exagerada na criminalização pode desviar o foco dos componentes de prevenção na produção legislativa nesta área. Isto é particularmente importante no contexto regional, pois uma sobrecriminalização pode depois inadvertidamente obstruir outros direitos. Em particular, na região da SADC, deve ter-se muita cautela para evitar a criminalização do discurso. A legislação deve providenciar alguma clareza sob a forma de uma lista de infracções, a qual deverá incluir infracções relacionadas com o assegurar da integridade dos sistemas informáticos. Especificamente, a legislação deve, além disso, prever a criminalização da posse e transmissão de pornografia infantil e da obtenção de acesso a *websites* de pornografia infantil. Deverá ser incluída uma excepção que permita às autoridades policiais conduzirem investigações. A legislação deverá também prever a criminalização da produção intencional e ilegal, da venda e de actos associados relacionados com pornografia infantil.
	Investigação criminal e automatização	A investigação dos crimes deve ter em consideração as realidades digitais. Para começar, a legislação deve garantir que a admissibilidade e a inviolabilidade das provas digitais sejam protegidas para que se possa combater o crime eficazmente. Assim, por exemplo, a lei procedimental deve incluir disposições relativas à preservação de dados, ordem de produção, busca e apreensão, recolha em tempo real, extradição, assistência mútua e a limitação do uso das provas. E nesta área, a lei deve garantir que a tomada de decisões automatizada e a recolha de dados pelas autoridades policiais não pode prejudicar o público injustamente.
	Segurança organizacional	Considerando as questões de imunização coletiva quanto à cibersegurança e de vulnerabilidades de comércio que foram discutidas, é importante criar obrigações positivas para as empresas para que implementem a segurança. No entanto, de modo a evitar que tais obrigações se possam tornar demasiadamente opressivas, as mesmas devem estar ligadas a um regime regulatório junto de uma autoridade regulatória que seja capaz de garantir que as obrigações são flexíveis e apropriadas.
	Educação e sensibilização	O estabelecimento de uma capacidade institucional madura para combater o cibercrime só pode ser assegurado se for incluída formação sobre o cibercrime e os desafios e a regulação da cibersegurança para juízes, procuradores, advogados, agentes da autoridade, especialistas forenses e outros investigadores de cibercrime.

Restrições de acesso	**Normas de retirada e direitos humanos**	Embora os procedimentos de notificação e retirada estejam normalmente incorporados na legislação relacionada com electrónica e informática – e providenciem uma forma de intervenção específica consoante os casos – é possível incluir considerações acerca dos direitos humanos e do Estado de Direito em tais processos, integrando considerações sobre o "equilíbrio justo".
	Respeito pela legalidade, proporcionalidade e necessidade	Os padrões normativos para avaliar a interferência no acesso à Internet podem ser extraídos dos direitos humanos internacionais. Considerações como a proporcionalidade e a necessidade podem ser usadas para guiar as acções de possíveis intervenções legais ou de políticas, todas sob a pré-condição de que seja estabelecida a legalidade. A necessidade significa que quaisquer restrições ao acesso à Internet devem estar limitadas a medidas que sejam estrita e demonstravelmente necessárias para alcançar um fim legítimo. Deve ser demonstrado que nenhuma outra medida conseguiria atingir efeitos semelhantes com maior eficiência e menos danos colaterais. Quaisquer restrições ao acesso à Internet devem também ser proporcionais. Uma avaliação da proporcionalidade deve garantir que a restrição é "o instrumento menos intrusivo entre aqueles que poderão alcançar o resultado pretendido". A limitação deve dirigir-se a um objectivo específico e não deve afectar indevidamente outros direitos das pessoas visadas. Porém, qualquer tentativa de interferir com o acesso terá de ser entendida no contexto da Declaração Conjunta sobre a Liberdade de Expressão e a Internet, a qual co-declarava com o então Relator Especial da ACHPR (Comissão Africana para os Direitos Humanos e dos Povos) sobre Liberdade de Expressão e Acesso à Informação, o adv. Pansy Tlakula, que: > Cortar o acesso à Internet, ou a partes da Internet, a populações inteiras ou a segmentos do público (encerrando a Internet) nunca pode ter justificação, incluindo por motivos de ordem pública ou de segurança nacional. O mesmo se aplica a abrandamentos impostos à Internet ou a partes da Internet.

9. Opções e recomendações em termos de políticas: Criação de valor baseada em dados

Subtema das políticas	Tópico das políticas	Recomendação
Comércio electrónico e transacções electrónicas	**Papel dos reguladores**	Nas Orientações da SADC sobre Dinheiro Móvel há fortes orientações disponíveis sobre reguladores para este subconjunto de preocupações da economia digital. Como é bastante consistente no quadro da economia digital, a regulação requer um equilíbrio entre inovação e restrição. Para permitir a inovação, pode ser dado espaço às empresas através de "Áreas de Teste Regulatórias", nas quais

		poderão testar os seus produtos sem o risco de potencial responsabilidade legal. O Projecto de Lei Modelo da SADC sobre Transacções Electrónicas e Comércio Electrónico (2013) regista mais especificamente a forma como a regulação, na sua relação com os componentes da transacção electrónica, pode ajudar a providenciar clareza jurídica.
	Complexidade aduaneira e impacto aduaneiro	A redução da complexidade aduaneira através das políticas é uma forma principal de facilitar o comércio electrónico regional, ao melhorar tanto a logística para os clientes e as empresas, como os custos e as eficiências internas das empresas. Muito importante, também, neste contexto, a incongruência das pautas aduaneiras, de forma mais ampla, pode apresentar riscos de desvio dos fluxos comerciais. Para permitir um ambiente aduaneiro ainda mais propício será também necessária a infra-estrutura de TIC requerida, a capacitação das autoridades, e garantir que os comerciantes transnacionais estão a par dos procedimentos aduaneiros digitais. Estudos do lado da procura demonstraram que o custo dos dispositivos é um obstáculo principal à utilização da Internet em África. Apesar disto, em muitos países os produtos digitais são tributados como se fossem artigos de luxo, o que faz aumentar os custos, e estes são muitas vezes mais agravados ainda com taxas aduaneiras adicionais. Os ganhos em dividendos digitais provenientes da melhoria do acesso a dispositivos e, portanto, da conectividade, têm o potencial de compensar as perdas económicas directas provocadas pela redução da tributação.
	Protecção dos consumidores	É vital fomentar a confiança entre os consumidores e as empresas de comércio electrónico, particularmente porque o comprador e o vendedor estão "deslocados". A chave são os mecanismos de resolução de litígios – quer as empresas quer os sistemas de pagamento devem providenciar meios para isto. Alguns princípios adicionais para dar prioridade à protecção dos consumidores, são: • práticas empresariais e publicitárias justas (pensar, por exemplo, na clareza da colocação de produtos paga em contextos de redes sociais); • divulgações apropriadas e integrais (como a rotulagem); • processos eficazes para confirmação de transacções e pagamentos que se foquem na clareza para os consumidores; • medidas proactivas para dar resposta aos riscos de privacidade e segurança; • segurança dos produtos ao longo das cadeias de abastecimento do comércio electrónico; • períodos de reflexão para os consumidores; e • acesso relevante a mecanismos eficazes de resolução de litígios, que podem incluir a resolução de litígios *online*.
	Encriptação	A encriptação torna-se importante enquanto método de capacitar os utilizadores para se protegerem a si próprios do cibercrime. Pode ser a encriptação das comunicações, mas também pode ser usada no âmbito das

		transações. Porém, a encriptação apresenta um conflito interessante: embora melhore, obviamente, a segurança *online* do indivíduo, as autoridades policiais queixam-se de que ela dificulta a sua capacidade de investigação. Emergem duas abordagens principais: alguns países defendem legislação que obrigue as empresas tecnológicas e de comunicações a desencriptar os dados dos clientes, enquanto outros (os Países Baixos, a Estónia) expressaram o seu apoio a uma forte encriptação. Alguns afirmam que exigir "portas de serviço de encriptação" ao nível do bloco regional, se puder ser garantida uma autoridade regional de supervisão fortemente capacitada, poderia permitir a aplicação da lei, preservando ao mesmo tempo a integridade das comunicações. No entanto, não existem ainda quaisquer métodos viáveis que garantam que uma fragilidade projetada num sistema de encriptação não possa vir a ser explorada por pessoas mal-intencionadas. Uma vez que muitos dos intervenientes globais, quer estatais quer não estatais, que ameaçam a segurança das comunicações e transacções digitais na África Austral têm capacidades tecnológicas superiores a quase todos os intervenientes comerciais (e à maior parte dos intervenientes estatais) da região, exigir a introdução de fragilidades projetadas tornará a região vulnerável a intervenientes mal-intencionados – e ao mesmo tempo desencorajará as empresas inovadoras tecnologicamente de operarem na região.
Propriedade intelectual e direitos de autor	**Excepções aos direitos de autor**	Uma vez que os direitos de autor existem automaticamente, definir quando se aplicam as excepções às regras gerais torna-se o ponto de intersecção mais importante para a lei. Os instrumentos internacionais (*Convenção de Berna*, 1886) estabeleceram fundamentalmente um teste de três factores, por vezes referido como um teste de três passos, definindo que as excepções e as limitações aos direitos exclusivos são permitidas: > a) em certos casos especiais; b) que não entrem em conflito com a normal exploração do trabalho; e c) não prejudiquem despropositadamente os interesses legítimos do autor/detentor dos direitos. Embora o significado preciso de cada um dos passos permaneça em discussão, o teste poderá talvez ser mais bem resumido e clarificado da seguinte forma: as excepções e limitações aos direitos de autor são permitidas se (1) não forem indevidamente vagas, (2) não privarem os detentores dos direitos de um rendimento tangível em áreas nas quais os detentores dos direitos normalmente obtêm tal rendimento a partir dos direitos de autor, e (3) não prejudiquem os interesses dos detentores dos direitos de uma forma desproporcionada. Estas excepções devem procurar incorporar as considerações das políticas públicas e, no âmbito dos contextos digital e de desenvolvimento, devem focar-se fortemente no papel da expansão da educação e da inclusão dos cidadãos para ajudar a combater os desafios da desigualdade que podem surgir no contexto da economia digital. As disposições sobre o uso justo e sobre transacções justas podem depois existir enquanto exclusões mais gerais e flexíveis, que se aplicarão quando não estiver disponível nenhuma outra limitação aos direitos de autor. Isto permitirá flexibilidade num mundo tecnológico em rápida evolução.

		Além das excepções de carácter geral, certas excepções específicas são importantes para a economia digital: • excepções para permitir a aprendizagem *online*; • excepções para o uso transfronteiriço de conteúdo que inclua conteúdo usado sob uma excepção no país de origem; • excepções para permitir a interoperabilidade dos sistemas de TIC; • excepções para permitir a reparação e a protecção de coisas que incorporem *software*.
	Dispositivos ligados à Internet	Devem estar preparadas disposições de segurança específicas para a Internet das Coisas. Por exemplo, podem ser criados requisitos que obriguem os dispositivos ligados à Internet a terem uma palavra-passe específica do dispositivo, a qual pode ser alterada pelo utilizador. Deve haver também obrigações positivas para o fornecedor de um dispositivo ligado à Internet para que forneça um ponto de contacto para a notificação de problemas de segurança.
	IA e PI	Embora este seja um desafio relativamente recente em termos de políticas, os riscos para os inovadores e empreendedores são elevados. Alguns passos proactivos poderão ser: • estabelecer que os direitos de autor apenas se aplicam aos produtos criativos de autores humanos; • autorizar o uso de trabalhos com direitos de autor para permitir a análise avançada de informação, como o treino de algoritmos de IA; • exigir que os requerentes de patentes divulguem a utilização de IA nas invenções em desenvolvimento.
	Responsabilidade dos prestadores de serviços	Devem ser concedidas limitações de responsabilidade aos Prestadores de Serviços. Para os Prestadores de Serviços envolvidos no alojamento de conteúdos, a limitação de responsabilidade deve estar condicionada ao cumprimento de uma notificação e requisito de notificação em que as reclamações são enviadas ao Prestador de Serviços, o qual por sua vez notifica a pessoa que carregou o conteúdo. Se a pessoa que carregou o conteúdo admite a reclamação ou não responder, o Prestador de Serviços pode então remover o conteúdo. Se a pessoa que carregou o conteúdo contestar a reclamação, o Prestador de Serviços informa o reclamante dos dados de contacto da pessoa que carregou o conteúdo e da sua respectiva defesa. O reclamante pode então recorrer aos tribunais ou a outra entidade de resolução de litígios para a resolução da reclamação.
	Mecanismos de aplicação	Independentemente da forma como as excepções possam ser redigidas, uma consideração essencial é a criação de vias para que os criadores possam exercer o seu direito de lucrar com o seu trabalho. A harmonização permanece

		importante, tal como a educação para os direitos e o acesso a mecanismos de justiça (questões que podem ser tratadas através da regulação orientada).

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; … g. the right to respect for private and family life; …	Reference to personal and information privacy (in a freedom of expression context).

		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	Reference to personal and communications privacy.

		c. interference with private communications, including mail and all forms of telecommunications.	
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 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.	Reference to privacy of the home and property, not in relation to information.

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 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.	Reference to personal and communications privacy.
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 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.	Reference to personal privacy and communications privacy.
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 Protection of Privacy Bill	Ministry of Information, Communications and Technology	

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	Congolese Patent and Trademark Office

					Property Secretariat for industry and small and medium enterprises (IPMEA); Ministry of Industry and SMEs	
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); Merchandise Marks Act (Chapter 49:04) (1966)	Department of the Registrar General (Ministry of Justice and Constitutional Affairs); Ministry of Youth, Sports, Culture & Community Development	Copyright Society of Malawi (COSOMA)
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); The Trade Marks Act (Chapter 401) (1994)	Patents and Companies Registration Agency (PACRA) (Ministry of Commerce, Trade and Industry)	
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	Zimbabwe Intellectual Property Office (ZIPO) (Ministry of Justice, Legal and Parliamentary Affairs)	

				Designs Act (Chapter 26:07) (2001); Merchandise Marks Act (Chapter 14:13) (2001); Intellectual Property Policy and Implementation Strategy [2018-2022]		