Document de travail de la SADC sur l'économie et la société numériques :

Rapport de synthèse

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

Le présent document est un rapport de synthèse[1] d'un document de travail complet[2] qui porte sur les considérations politiques et de gouvernance pour les pays en développement afin de permettre le développement d'économies numériques inclusives et durables. Rédigées par Research ICT Africa, les documents reprennent les points de compréhension mutuelle contenus dans le Mémorandum d'accord SADC Parliamentary Forum-Research ICT Africa. Le document de travail et le présent rapport de synthèse font partie du processus de rédaction d'une loi type de la SADC PF pour l'économie numérique. Les objectifs d'une telle loi type sur l'économie et la société numériques sont de permettre aux pays de tirer parti des avantages de l'économie numérique, tout en sauvegardant les droits des citoyens et en réduisant les risques potentiels associés à de tels développements. Le présent rapport de synthèse résumera les principaux renseignements contenus dans le document de travail pour éclairer la poursuite de la mobilisation sur la loi type.

Le Forum parlementaire de la SADC et Research ICT Africa sont reconnaissants au Centre canadien de recherches pour le développement international (CRDI) qui a rendu cette recherche et cette collaboration possibles.

Partie A : Économie numérique

1. Introduction

La numérisation à l'échelle mondiale a été une caractéristique déterminante du développement socio-économique du XXIe siècle. Les tendances mondiales de la numérisation et désormais de la « datafication » ont un impact sur tous les aspects de l'activité économique et sociale. Avec l'émergence de technologies avancées fusionnant les domaines physique et numérique, l'Internet des objets (IOT), l'intelligence artificielle (IA) et les technologies d'apprentissage automatique permettent la collecte, l'utilisation et l'analyse de vastes quantités de données numériques provenant de données des activités personnelles, sociales et commerciales en ligne.

Les changements rapides dans les processus de numérisation et de « datafication » caractérisent l'économie mondiale contemporaine. Certains développements ont été progressifs, d'autres perturbateurs, mais tous ont été très inégaux. Aujourd'hui, la génération, le traitement et la transmission de l'information définissent de manière critique qui bénéficie du potentiel transformatif de la numérisation. Les principaux bénéficiaires et créateurs de la nouvelle valeur créée par ces processus ont été les plateformes mondiales. Leur domination des marchés à travers le contrôle des données, ainsi que leur capacité à créer et à capter la valeur ajoutée constamment et ont mené à leur concentration et à leur consolidation dans un très petit nombre de pays et une poignée d'entreprises (CNUCED 2019). Et si les bénéfices s'accumulent de manière inégale, c'est aussi le cas des risques et des préjudices de la numérisation, qui obéissent à un grand nombre des modèles hors ligne d'inégalité sociale et de revenus.

Ces questions soulignent la nécessité pour les décideurs des pays en développement de considérer la numérisation dans le contexte des marchés mondiaux, des chaînes de valeur, mais aussi dans leur contexte local où le manque de préparation numérique limitera leur capacité à tirer parti de ces

1 Ce rapport de synthèse est fondé sur la version 4 du document de travail.

2 Le document de travail contient la liste complète des références.

nouvelles technologies et processus ainsi qu'à réduire les risques en termes d'emploi, de gouvernance des données et d'accès au financement. Pour cela, l'inclusion numérique des pays en développement et des secteurs critiques avec des économies en développement est fondamentale afin d'accroître leur visibilité dans l'écosystème plus large de la chaîne de valeur.

À l'ère de la numérisation, les données ont joué un rôle important dans le développement socio-économique, car elles sont considérées comme une ressource stratégique et critique pour les économies axées sur les données – phénomène appelé « datafication ». Mais si les avantages socio-économiques de l'analyse des mégadonnées ne peuvent être ignorés, des cadres de gouvernance des données pour un traitement transparent et responsable des renseignements personnels (avant l'agrégation) sont nécessaires pour protéger les droits d'accès à l'information et à la vie privée. Ceci a également une incidence sur d'autres droits fondamentaux et peut être considéré comme un appel à la « justice des données ».

Bien que l'on reconnaisse de plus en plus la nécessité de protéger les données dans cette économie axée sur les données, en particulier pour optimiser les possibilités de commerce intérieur et extérieur, la protection des données à l'échelle mondiale est très fragmentée, avec des approches réglementaires régionales, nationales et globales divergentes. Un cadre qui facilite l'accès aux données tout en respectant les droits à la vie privée, à l'intégrité et à la disponibilité des données est essentiel à l'établissement d'un environnement numérique fiable et sécurisé et constitue un prérequis à la création d'une économie numérique équitable et durable.

Le projet de loi type pour la communauté économique régionale par la SADC PF est donc opportun. Comme l'indique le rapport de la CNUCED sur l'économie numérique 2019 : l'incidence nette dépendra du niveau de développement et de préparation numérique des pays et de leurs parties prenantes. Elle dépendra également des politiques adoptées et mises en place aux niveaux national, régional et international (CNUCED 2019).

La section suivante de la partie A du rapport de synthèse positionne l'économie numérique nationale dans l'écosystème numérique mondial et les systèmes de gouvernance mondiale. (Le document de travail présente un examen plus complet des principaux attributs de l'économie numérique, notamment concernant les aspects de l'inégalité numérique évoqués ci-dessus).

La partie B se concentre ensuite sur le contexte juridique et fournit une structure aux décideurs et aux législateurs en définissant d'abord un cadre pour envisager l'incorporation d'une loi type de l'économie numérique, puis en décrivant les principales implications en matière de droits de l'homme et en fournissant un examen spécifique des cadres juridiques actuels au sein de la SADC.

La partie C examine les principales recommandations stratégiques découlant du document de travail relatives aux principaux domaines thématiques suivants : la propriété, le contrôle et l'accès aux données, la sécurité et l'interférence des données et la création de valeur à partir des données.

2. L'écosystème numérique

Conformément à l'accent mis par l'Agenda international du développement sur les technologies numériques comme vecteurs de développement, les TIC ont également été identifiées par la Communauté de développement de l'Afrique australe (SADC) comme des éléments essentiels pour construire une société plus inclusive, en éliminant la pauvreté et en réduisant les inégalités dans le pays. Cependant, dans cet environnement, les règles et les politiques qui souhaitent faciliter le développement

doivent répondre à une réalité particulière marquée par l'interconnexion et la mondialisation. Un changement fondamental de politique est nécessaire par rapport à la perspective des télécommunications traditionnelles qui considèrent que les développements numériques se produisent dans le cadre d'un secteur distinct, ou sont une question nationale, seulement. Au contraire, la numérisation se produit au sein d'un écosystème complexe qui couvre l'ensemble de l'économie et de la société au niveau national tout en étant inextricablement connecté et interconnecté avec les marchés mondiaux et les systèmes de gouvernance.[3]

Conceptualisés comme un écosystème (figure 1), les relations entre les différents éléments et les conséquences de leurs interactions peuvent être évalués à des fins politiques. Plutôt que de se focaliser sur l'évolution rapide de la technologie, cette approche place les utilisateurs, les citoyens et les consommateurs au centre de l'écosystème. Même là où l'infrastructure est disponible, leur accès à l'écosystème dépend du coût des réseaux, des services et des applications. Ces coûts à leur tour dépendent de la structure du marché et par l'efficacité de la réglementation déterminées par le cadre politique et juridique national.

Mais la capacité des citoyens à utiliser ces technologies et ces services numériques pour améliorer leur qualité de vie et leur bien-être sera déterminée non seulement par un accès abordable et par des connaissances numériques, mais aussi par l'éducation et l'acquisition de compétences pour le faire de façon productive. Un accès abordable s'obtient grâce à'un environnement politique qui favorise l'extension de l'infrastructure et met en place une réglementation efficace sur la concurrence entre les opérateurs de réseaux et entre les fournisseurs de services. Pour que la politique numérique stimule l'emploi et l'innovation, une stratégie intégrée pour l'investissement et le développement humain est essentielle.

Pour cela, il faut un État catalyseur capable d'attirer des investissements privés productifs et de coordonner la distribution des biens publics par les secteurs public et privé. Mais les résultats au niveau national sont de plus en plus influencés par les institutions multilatérales de gouvernance internationale, telles que l'UIT, l'Organisation mondiale du commerce, la Commission des Nations Unies pour le droit international, ainsi que par les nouvelles formes de gouvernance mondiale telles que l'ICANN, une organisation d'État non membre responsable de la gouvernance d'Internet. Les organisations régionales telles que l'Union africaine et les communautés économiques régionales, comme la SADC et les organisations régionales spécialisées via le Forum parlementaire de la SADC ainsi que l'Association des régulateurs des télécommunications de l'Afrique australe (CRASA) jouent un rôle de plus en plus important dans l'harmonisation des politiques et l'intégration du marché dans cet environnement mondialisé.

3 Voir, par exemple, récemment, en septembre 2018, les ministres des TIC de la SADC ont délibéré sur le fait que les TIC sont essentielles pour le développement durable de la région et ont fixé des objectifs spécifiques sur l'accès au haut débit, la cybersécurité, la connectivité rurale et la quatrième révolution industrielle. Déclaration aux médias :
https://www.sadc.int/files/3715/3806/1649/Media_Statement__ICT_Information_Transport_and_Met_meeting.pdf

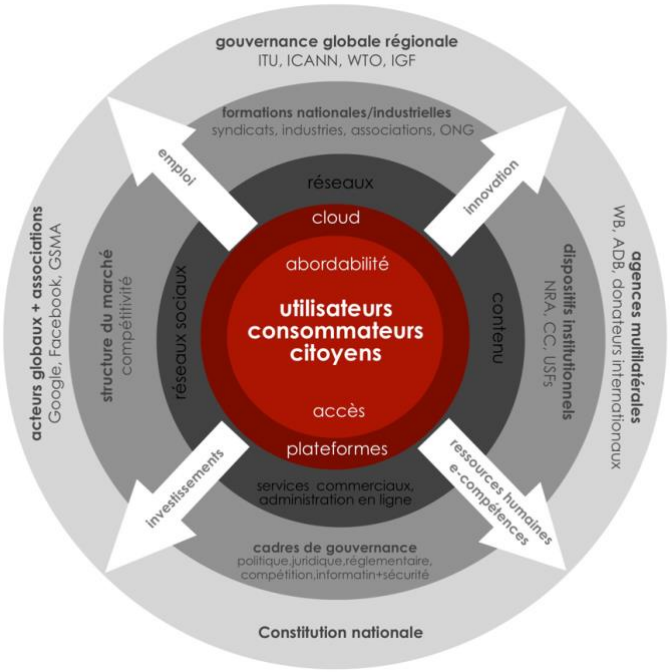


Figure 1 **: Vue écosystémique *de l'environnement numérique***

Les interconnexions entre les différentes composantes de l'écosystème conduisent à la nécessité pour les décideurs des pays en développement de considérer la numérisation dans le contexte des marchés mondiaux et des chaînes de valeur, mais aussi dans leur contexte local où le manque de préparation numérique limitera leur capacité à tirer parti de ces nouvelles technologies et de ces nouveaux processus, et à atténuer les risques associés à l'emploi, à la gouvernance des données et à l'accès au financement.

L'importance accordée à l'inclusion numérique et à l'égalité est fondamentale à cet égard. Paradoxalement, plus les gens sont connectés, plus l'inégalité numérique augmente. On ne distingue pas seulement ceux qui sont en ligne et ceux qui ne le sont pas (comme c'est le cas dans un environnement téléphonique et de texte de base), mais aussi ceux qui ont les ressources techniques et financières pour utiliser Internet de façon optimale et ceux qui sont « à peine » en ligne. On compte parmis ces derniers ceux qui n'ont qu'un accès partiel à des services de données de mauvaise qualité ou coûteux qui ne leur permettent pas d'être toujours actifs ou d'utiliser des services à forte intensité de données. L'écart se creuse entre ceux qui consomment passivement un nombre limité de services de base et ceux qui sont en mesure de mettre la technologie à profit pleinement et de façon productive, jusqu'à même parfois améliorer leur prospérité.

De même, de plus en plus de personnes qui n'ont pas la connaissance ou les compétences nécessaires pour exercer leurs droits entrent en ligne et sont plus vulnérables aux risques liés à l'utilisation de nouvelles applications, au recueil de renseignements personnels pour orienter la publicité à l'aide d'algorythmes ou à la façon dont les gouvernements peuvent les sonder.

La hausse des déplacements de revenus du travail vers le capital et la baisse des emplois de niveau intermédiaire dans de nombreux pays, communément appelée polarisation des salaires par les

économistes, suggèrent que les gains d'une utilisation accrue de la technologie ne seront pas partagés équitablement sans des interventions politiques importantes (Van Reenen, 2019).

Une stratégie nationale transversale est donc nécessaire afin que les pays en développement créent une économie numérique habilitante et équitable pour l'inclusion sociale et la prospérité économique ; pour éviter les préjudices liés à la surveillance permanente opérée par les plateformes monopolistiques mondiales et par l'État, pour protéger les droits des citoyens et pour créer un environnement sûr, sécuritaire et fiable indispensable à l'essor de l'économie numérique. Pour y parvenir, ces politiques devront découler de processus participatifs multipartites engageant société civile et secteur privé avec le gouvernement. Afin de répondre à la demande nationale et d'être en mesure de soutenir efficacement la concurrence dans l'économie mondiale , ces politiques nationales exigeront la coordination des secteurs public et privé. Cela impliquera :

- l'afflux d'investissements privés productifs pour améliorer l'infrastructure physique (y compris l'électricité et le haut débit) ;
- une réglementation économique efficace des fournisseurs d'infrastructures afin d'assurer une politique de concurrence équitable et un dispositif d'expérimentation réglementaire permettant de fournir des services haut débit à moindre coût ;
- des dispositions institutionnelles cohérentes concernant l'infrastructure, le contenu, les données et les problèmes de concurrence émergeants de manière à faire face à un système adaptatif d'information mondiale complexe, dispositions vis à vis desquelles la gouvernance nécessite des réponses nationales et mondiales ;
- des politiques visant à faire des données publiques et commerciales des actifs critiques pour les nouveaux entrants et des flux de données permettant un commerce transfrontalier tout en protégeant les informations privées des individus et en garantissant la sécurité et l'intégrité des systèmes nationaux ;
- des changements dans les programmes d'enseignement de base pour passer d'un apprentissage par cœur et d'un mode de pensée pouvant facilement être reproduits par des machines, à la création de connaissances critiques et créatives, mieux adaptées à l'environnement numérique dynamique, ainsi que des programmes transversaux de compétences numériques à grande échelle pour s'adapter et évoluer avec les nouvelles exigences en matière de main-d'œuvre ;
- un mécanisme de financement visant à étendre l'accès à ces nouveaux moyens de production pour l'intégration des chaînes d'approvisionnement, le commerce régional et la compétitivité mondiale et une harmonisation des cadres régionaux pour améliorer le commerce et permettre les flux de données transfrontaliers ; et
- la suppression à la fois de la fiscalité excessive des entreprises qui les décourage à investir dans les réseaux et de la taxation régressive des réseaux sociaux qui en freine l'utilisation par les pauvres ainsi que l'engagement dans la réforme du régime de fiscalité numérique international qui prévoit une taxation des produits et services numériques dans la juridiction dans laquelle les revenus sont générés, même quand le producteur n'est pas physiquement présent.

Ni le document de travail ni le rapport de synthèse ne sont en mesure de traiter en profondeur toutes les questions stratégiques liées à cet environnement habilitant. Ils se concentrent plutôt sur les considérations de politique et de gouvernance des pays en développement afin de tirer parti des

avantages d'une plus grande efficacité, d'une meilleure productivité et de la création de valeur associée à l'économie numérique axée sur les données, tout en soulignant la nécessité de rétablir l'inégalité numérique comme condition préalable à l'inclusion dans l'économie numérique. Ils le font afin de concevoir un cadre environnemental et stratégique qui puisse soutenir et appliquer les objectifs d'une loi type sur l'économie numérique.

Partie B : Contexte juridique

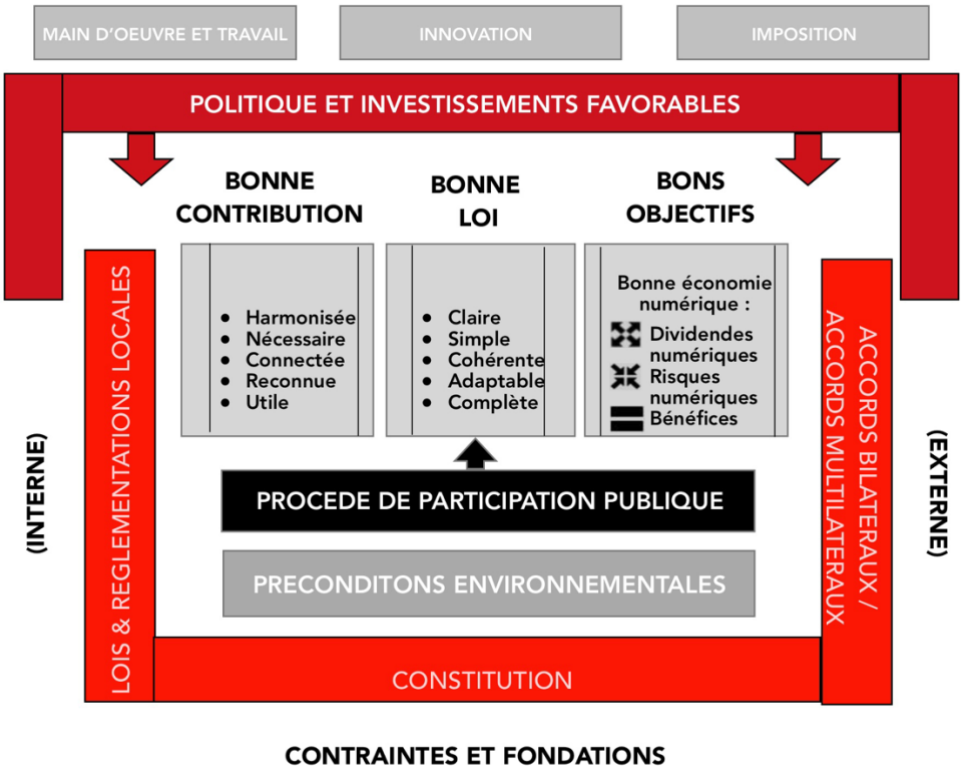
3. Fondements de la loi type

L'économie numérique présente des opportunités évidentes. En Afrique, la contribution d'Internet à la croissance du PIB reste actuellement faible. Certains suggèrent toutefois que les économies émergentes pourraient particulièrement progresser grâce à Internet et ajouter une valeur significative au PIB de l'Afrique (Manyika, J et al., 2013).

Au sein de la SADC, toute discussion sur les opportunités de croissance et les gains potentiels résultant de l'économie numérique doit être contextualisée en tenant compte des risques d'inégalité et d'exclusion qui en découlent. En ce qui concerne le rôle que peuvent jouer les législatures nationales dans leur contribution à cette économie numérique, le fort héritage régional des droits de l'homme constitue un fondement utile pour explorer les interventions dans cet espace, notamment en raison de leur capacité à intégrer des normes sociopolitiques dans la politique économique.

En ce qui concerne les questions de pertinence de la mission législative de l'économie numérique, le document de travail examine les composantes et les conditions fondamentales d'une « bonne » économie numérique en établissant quelques recommandations clés (détaillées plus loin), mais aussi en posant un cadre pour déterminer ce que les lois nationales devraient prendre en considération dans la mise en œuvre d'une loi type sur l'économie numérique. Ainsi, dans le cadre de cette approche *écosystémique* plus large, l'approche pour cette discussion sur le cadre politique et législatif nécessaire pour optimiser l'économie numérique peut être décrite comme suit:

Figure 5 : Schéma fournissant un cadre pour l'élaboration d'une loi modèle sur l'économie numérique



Le cadre admet la nécessité d'une stratégie nationale transversale pour que les pays en développement créent une économie numérique habilitante et équitable pour l'inclusion sociale et la prospérité économique ; pour éviter les préjudices liés à la surveillance permanente opérée par les plateformes monopolistiques mondiales et par l'État, pour préserver les droits des citoyens et pour créer un environnement sûr, sécuritaire et fiable indispensable à l'essor de l'économie numérique. Pour y parvenir, les politiques devront découler de processus participatifs multipartites engageant société civile et secteur privé avec le gouvernement.

Les objectifs de la Loi type ne doivent pas se limiter à encourager l'économie numérique, car encourager l'économie numérique telle qu'elle est ne fera qu'accroître les risques numériques et les inégalités. L'objectif devrait plutôt être de créer des lois et des politiques qui favorisent une « bonne » économie numérique, soit une économie numérique définie par :

- l'inclusion
- des objectifs en matière de droits de l'homme
- la compétitivité
- l'ouverture
- une réglementation et une planification
- la flexibilité
- l'habilitation des marchés nationaux

Pour ce faire, il est nécessaire d'établir des principes servant de base à l'élaboration des lois dans les contextes nationaux qui tiennent compte des objectifs de collaboration régionale et des fondements d'une bonne économie numérique qui profite à tous. Les points de vue décrits ci-dessous constitueront la première étape de l'élaboration d'une loi type basée sur ces principes.

4. Droits de l'homme

Les droits de l'homme se renforcent mutuellement naturellement et sont interreliés. Les principes des droits de l'homme, fortement dictés dans toute la région aussi bien par les organes des droits de l'homme de la région que par les législatures et les tribunaux nationaux devraient servir de norme pour intégrer les impératifs sociaux dans le contexte économique d'une loi type sur l'économie numérique. [4]

Étant donné l'importance conférée aux données et à l'information dans l'économie numérique, les droits du spectre des droits civilo-politiques les plus couramment cités sont les droits à la vie privée, à l'accès à l'information et à la liberté d'expression, particulièrement importants pour tenir compte des contraintes et des ambitions d'une loi type sur l'économie numérique. Certes, bien que ces droits soient particulièrement pertinents pour une économie numérique habilitante (par exemple, par rapport aux éléments facilitants tels que les télécommunications et Internet en tant qu'infrastructures numériques), les droits socio-économiques tels que le droit au travail et le droit à l'inégalité le sont certainement aussi. Toutefois, au moins pour l'exercice de fournir un cadre (notamment un cadre justiciable étant donné les limites de certains droits socio-économiques), le document se concentrera sur les composantes du spectre politique civil pour l'examen des dispositions constitutionnelles spécifiques au sein de la SADC et se tournera vers des catégorisations de droits plus larges dans le cadre du domaine d'action.

4 Voir l'annexe 1

5. Cartographie législative nationale de la SADC

Pour revenir au cadre de la loi type présenté à la *figure 5*, l'étude du cadre légal nécessite de se référer à la fois aux instruments pertinents de la région (décrits à l'annexe 1A), et à ses principes et lignes directrices clés (décrits à l'annexe 1B). De plus, il faut tenir compte des contextes législatifs nationaux pour les différentes zones. Une cartographie préliminaire de ces instruments constitutionnels et législatifs nationaux est disponible dans les autres Annexes.

Bien que le document de travail examine de façon exhaustive les instruments et les lois nationales de la SADC, il convient de fournir un aperçu rapide de l'intégration de celle-ci dans tous les domaines politiques.

5.1 Propriété, contrôle et accès aux données

Loi type de la SADC sur la protection des données

Le projet de loi type de la SADC sur la protection des données (2013) comprend deux formulations principales. L'article 43 régit le flux transfrontalier de données entre les pays de la SADC qui ont adopté la loi type. Les articles 44 et 45 régissent le transfert transfrontalier de données d'un pays de la SADC qui a adopté la loi type vers un pays non membre de la SADC ou vers un État membre qui n'a pas transposé la loi type.

Cadres juridiques nationaux sur la confidentialité des données dans la CCDA

L'Angola, le Botswana, le Lesotho, Madagascar, Maurice, les Seychelles et l'Afrique du Sud ont adopté des lois sur la protection des données. Toutefois, seule la loi de Maurice est pleinement en vigueur, notamment en ce qui concerne la création d'une autorité de protection des données indépendante (DPA), largement reconnue comme élément essentiel à l'application efficace des lois sur la protection des données. En Afrique du Sud, un régulateur de l'information a été créé, mais la loi n'est que partiellement en vigueur (articles 1; 112; 113 et le chapitre 5, partie A, ont commencé par la proclamation no R. 25, 2014). Le fait de ne pas nommer une DPA dans les délais est maintes fois critiqué pour être un obstacle majeur à l'application efficace des lois sur la protection des données, et ce défaut s'observe plus souvent en Afrique qu'ailleurs (Greenleaf, 2011). Un fait positif est que tous les DPA existantes jouissent du statut d'organismes indépendants (Greenleaf, 2011).

D'autres pays ont des projets de loi officiels sur la protection des données, et on s'attend à ce qu'un certain nombre d'entre eux soient adoptés bientôt. Il s'agit des Comores, du Royaume d'Eswatini, de la Tanzanie, de la Zambie et du Zimbabwe. La Zambie a signé la Convention de l'Union Africaine sur la cyber-sécurité et la protection des données personnelles avant d'adopter une loi sur la confidentialité des données que le gouvernement avait approuvée en juillet 2018 (Greenleaf, 2018). Au Zimbabwe, la seule loi en lien avec la protection des données ou de la vie personnelle est *celle sur l'accès à l'information et la protection de la vie privée* (2002).

En 2013, la Tanzanie s'est engagée dans un processus de réforme juridique dans le but de transposer la loi type de la SADC en une loi nationale. Dans le cadre du projet HIPSSA et avec le soutien financier, technique et d'experts de l'UIT, de la Commission européenne et de l'Union européenne, la Tanzanie a créé son premier projet de loi approfondi sur la protection des données intitulé « Projet de loi sur la protection de la vie privée et des données », qui a été rebaptisé en 2014 « Projet de loi sur la protection des données personnelles ». Les autres pays de la SADC n'ont pas de lois spécifiques sur la protection des

données ou de projets de loi officiels. Il s'agit de la République démocratique du Congo, du Mozambique et de la Namibie.

Les principaux principes de protection des données personnelles qui diffèrent entre les juridictions de la SADC incluent donc : i) l'enregistrement auprès d'une autorité de protection des données (DPA); ii) l'autorisation de la DPA pour le traitement de certaines catégories de Données ; iii) l'applicabilité territoriale des lois; iv) les transferts transfrontaliers de données; v) la notification de la violation de données; vi) la nomination d'un délégué à la protection des données (DPO); vii) l'élaboration de codes de conduite ou d'éthique.

Cadres juridiques nationaux sur l'accès à l'information dans la SADC

La Loi type sur l'accès à l'information pour l'Afrique est un instrument de référence important dans la région. Notamment, la loi type met fortement l'accent sur des dispositions de divulgation proactive ciblées et détaillées.

Au sein de la SADC, l'Angola, le Malawi, le Mozambique, les Seychelles, l'Afrique du Sud, la Tanzanie et le Zimbabwe disposent de lois spécifiques sur l'accès à l'information (quoique la loi zimbabwéenne soit critiquée par certains pour en restreindre l'accès plutôt que de le faciliter).

Plusieurs campagnes n'ont cessé de lutter pour l'instauration de lois sur l'accès à l'information dans la région et des pays comme le Botswana, Maurice, la Namibie et la Zambie, n'ont pas adopté de projets de loi sur l'accès à l'information depuis de nombreuses années. (le Lesotho, Madagascar et le Royaume d'Eswatini ont des projets de loi en cours). Les Comores ne prévoient actuellement aucune loi.

La plupart de ces lois n'ont pas de dispositions exhaustives sur la divulgation proactive, en dépit de la loi type.[5] Il n'existe pas non plus de forte consistance quant à la mise à disposition d'agents régulateurs qui pose des problèmes pour l'adaptabilité des lois, mais aussi limite l'accès aux recours pour les entreprises et les citoyens.

5.2 Sécurité et interférence des données

Cadres juridiques nationaux sur la cybersécurité et la cybercriminalité

Au-delà de la législation portant spécifiquement sur la cybercriminalité, le Malawi, la Zambie et le Zimbabwe ont des lois plus larges en matière de cybersécurité. L'Angola a également adopté en 2017 une loi de cybersécurité concernant la protection des réseaux d'information. Le projet de loi sud-africain sur la cybercriminalité (séparé du projet de loi controversé sur la cybercriminalité et la cybersécurité de 2017) attend la signature du président. Les Comores et la République démocratique du Congo n'ont pas ratifié ou proposé de législation en matière de cybersécurité. En ce qui concerne en particulier la surveillance et l'interception des communications, l'Afrique du Sud et le Zimbabwe ont une législation spécifique sur l'interception des communications. Dans ce contexte, il convient d'examiner le récent jugement sur la législation sud-africaine en matière d'interception, *Amabhungane Centre for Investigative*

5 Il est intéressant de noter que certains de ces pays ont vu leurs lois directement comparées à la Loi type, et le résultat peut être consulté ici : http://www.africanplatform.org/fileadmin/Content/PDF/Resources/State-of-ATI-in-Africa-2017.pdf.

Journalism NPC et Minister of Justice and Correctional Services and Others [2019] ZAGPPHC 384.[6] La cour a jugé inconstitutionnels certains aspects de la loi car les aspects procéduraux décrits pour obtenir des autorisations en vertu de la loi étaient généralement insuffisamment détaillés et ne prévoyaient pas une surveillance satisfaisante des demandes.

Des lois dédiées à la cybercriminalité ont été promulguées à Madagascar en 2014, à Maurice en 2003, aux Seychelles en 1998, en Namibie en 1988, au Zimbabwe en 2004 et en 2019, et en Afrique du Sud et en Zambie en 2004 et 2018 (bien que, comme mentionné, le projet de loi sud-africain 2017 sur la cybercriminalité soit en attente de la signature du président), quoique la loi sur l'utilisation abusive d'ordinateurs aux Seychelles et en Namibie ait été identifiée comme inadéquate pour le contexte technologique actuel. Des projets de loi sur la cybercriminalité non encore ratifiés ont également été déposés au Botswana en 2018, à Eswatini e et en Namibie en 2014, au Lesotho et aux Seychelles en 2013.

Évaluation des capacités et de la maturité des pays

Une considération importante souvent soulevée dans le contexte de la cybersécurité au delà des risques qu'elle suggère concerne les capacités de l'État et de ses institutions à lutter contre la cybercriminalité. L'Indice mondial de cybersécurité (UIT, 2018) indique que seule l'île Maurice démontre un engagement élevé pour ses cinq piliers. Ni l'Angola, ni la République démocratique du Congo ni le Lesotho n'ont en effet participé à l'étude de 2018, et tous sont classés « faibles », car ces pays ont tout juste commencé à prendre des engagements en matière de cybersécurité (Les autres pays de la SADC classés « faible » sont les Comores, Madagascar, le Malawi, le Mozambique, la Namibie, les Seychelles, le Royaume d'Eswatini et le Zimbabwe). Le Botswana, l'Afrique du Sud, la Tanzanie et la Zambie sont classés comme des pays « moyens », « qui ont pris des engagements complexes et se sont engagés dans des programmes et des initiatives de cybersécurité".

5.3 Création de valeur basée sur les données

Préparation au cybercommerce

Selon l'indice du commerce électronique de la CNUCED 2018, la moyenne régionale pour l'Afrique était de 30, ce qui était bien inférieur à la moyenne mondiale de 55 (CNUCED, 2018). Toutefois, depuis 2014, « l'Afrique subsaharienne a dépassé la croissance mondiale pour trois des indicateurs utilisés dans l'indice » (CNUCED, 2018).

Monnaie mobile et paiement électronique

Le Projet des systèmes de paiement est très actif dans la SADC, le paiement numérique étant reconnu comme facvorisant les bénéfices de l'économie numérique. Celui-ci a été élaboré par le sous-comité des paiements du bureau du Comité des Gouverneurs des Banques Centrales (CCBG) de la SADC (Abrahams, 2017). De plus, les lignes directrices sur l'argent mobile (qui ont fait suite à un examen commandé par le CCBG) fournissent des lignes directrices juridiques et réglementaires précieuses, adoptant un modèle où les licences d'argent mobile ne peuvent être accordées que par une banque centrale (Abrahams, 2017).

Cadres juridiques nationaux sur la PI et le droit d'auteur

6 Voir ici la brève analyse du cas fournie précédemment sous « 2.1.1 Surveillance ».

Toutes les juridictions de la SADC appliquent une forme de législation sur le droit d'auteur et les brevets qui a une forte tendance à inscrire les lois dans un contexte industriel et commercial. Les examens contextuels semblent indiquer que les difficultés ne relèvent pas nécessairement d'une lacune dans les instruments juridiques, mais plutôt de leur accessibilité pour permettre aux créateurs et aux innovateurs d'en tirer profit. (ainsi que du manque d'environnements propices à l'innovation plus généralement) (Phiri, 2008). Des recherches menées à travers le continent suggèrent que la plupart des pays africains disposent de droits suffisants pour les créateurs mais ne disposent pas d'exceptions et de limites appropriées (Armstrong et al., 2010).

Intégrations régionales

La SADC, en tant que bloc commercial, est adaptée à la coordination de la propriété intellectuelle et du droit d'auteur (Nkomo, 2014) et pourrait être en mesure de surmonter certaines lacunes de l'Organisation régionale africaine de la propriété Intellectuelle (ARIPO). Plusieurs pays de la SADC, dont l'Afrique du Sud, l'Angola, le Mozambique et Madagascar, n'ent sont pas membres.

Partie C : Positions de principe

6. Structure des sections des politiques

Il y a trois grands domaines dans lesquels nous avons organisé des recommandations de position politique :

- Propriété, contrôle et accès des données
- Sécurité des données et interférence
- Création de valeur fondée sur les données

Dans chacun de ces grands thèmes politiques, des sous-thèmes contribuent à faciliter l'organisation des options politiques. Ceci permet d'acorder la complexité du contenu, mais aussi de respecter les domaines fonctionnels législatifs traditionnels, ce qui peut aider à envisager l'application de ces domaines dans un contexte national :

Principal domaine politique	Sous-thème	Sous-thème	Sous-thème
Propriété, contrôle et accès des données	Protection des données et vie privée	Accès aux données et à l'information	
Sécurité des données et interférence	Cybersécurité et surveillance	Cybercrimes	Restrictions d'accès
Création de valeur basée sur les données	Commerce électronique et transactions électroniques	Propriété intellectuelle et droit d'auteur	

Le document de travail contient des recommandations plus générales qui décrivent les enjeux qui précèdent chaque section de recommandation. Afin de mieux apprécier le contexte des recommandations spécifiques, mais aussi de considérer d'autres domaines plus vastes qui peuvent reposer sur des principes dans une loi type, le document d'orientation plus complet devra être consulté.

7. Options et recommandations stratégiques : Propriété, contrôle et accès des données

Sous-thème Politiques	Question de politique	Recommandation
Surveillance	**Traitement légal des données**	Habituellement, les lois mises en place pour protéger les informations privées des personnes consistent à imposer des guides et des limites sur la façon dont ces renseignements peuvent ou ne peuvent pas être utilisés. Les principes de traitement des données peuvent inclure : • les limites dans la collecte ; • la spécification du but ; • la limitation de l'utilisation ; • la qualité des données ; • les mesures de sécurité ; • l'ouverture (qui comprend le signalement des incidents, fortement corrélé avec les impératifs de cybersécurité et de cybercriminalité) ; • la responsabilité. Et lors de ce traitement, les droits des personnes concernées doivent être conformément respectés, ces obligations couvrant une variété de leurs droits. Certains de ces domaines sont spécifiés plus en détail plus loin.
	Minimisation des données	Le projet de loi type de la SADC sur la protection des données porte sur les « règles générales de traitement des données à caractère personnel » et met l'accent sur le droit du contrôleur des données à recueillir uniquement des informations personnelles à des fins spécifiques et légitimes. Dans le 4IR, la protection de la vie privée ne peut pas passer simplement par une limitation de la collecte de données ou de l'utilisation des ordinateurs et de la technologie de réseau. Afin d'atténuer les conséquences négatives d'une réglementation excessive de la vie privée limitant l'utilisation des TIC, il est nécessaire de trouver un équilibre entre la réduction au minimum de la collecte de données personnelles et la libre circulation de celles-ci tout en répondant aux besoins d'analyse d'importants volumes d'information et de production de connaissances, afin de tirer parti au mieux des économies et sociétés axées sur les données (Brankovic et Estivill-Castro, 1998). Une considération importante dans ce cadre est l'examen des bénéfices publics directs que le transfert de données peut engendrer, en particulier dans le domaine de la recherche, mais aussi du commerce (et l'évaluation des risques).
	Intégrité des données	Du fait que les données puissent générer des bénéfices économiques et publics, les droits des personnes concernées ne sont pas importants uniquement pour assurer la protection de la vie privée, mais aussi pour assurer et maintenir l'intégrité des données. L'intégrité des données fait référence à leur exactitude et à leur cohérence, qui influent à la fois clairement sur les bénéfices économiques globaux qu'elles produisent, mais aussi potentiellement sur le traitement ou les résultats des données propres à chaque personne concernée. Ceci peut être garanti à la fois par des obligations positives en ce qui concerne le traitement des données, mais

		aussi en veillant à ce que les droits des personnes concernées prévoient des droits proactifs d'accès à leurs données personnelles et que celles-ci soient modifiées.
	Données personnelles dépersonnalisées et anonymisées	La plupart des règlements sur la protection des données suggèrent que les données anonymisées ne sont pas des données personnelles, car elles n'appartiennent pas à une personne identifiable. Mais les données dépersonnalisées sont de plus en plus susceptibles d'être réidentifiées. Cela implique donc un examen plus approfondi des méthodes d'agrégation de données et de leur traitement par des tiers afin de réduire au minimum les risques de mauvaise utilisation des données anonymisées. D'un autre côté, les données anonymisées restent anonymisées et ne posent pas de problèmes majeurs pour la réglementation des données à caractère personnel, bien que le contrôle exclusif des données anonymisées puisse soulever des problèmes de concurrence. Compte tenu de l'importance de l'instauration d'un climat de confiance dans la sphère de la protection de la vie privée, des indicateurs pratiques devraient être élaborés afin que les entreprises comprennent comment faciliter les options et ceci devrait être facilité par la DPA.
	Consentement	Le consentement sous-tend en grande partie le traitement licite étant donné son rôle clé pour obtenir l'autorisation des personnes quant à l'utilisation de leurs données personnelles. Étant l'acte permissif central, ce qui constitue le consentement revêt une importance exceptionnelle ; et ce consentement doit être volontaire et éclairé. L'environnement numérique questionne de manière considérable la signification réelle du consentement éclairé. Cependant, une DPA compétente peut jouer un rôle déterminant en fournissant des pratiques exemplaires aux collecteurs et aux processus, tout en délivrant des conseils sur les outils technologiques disponibles pour le public pour que le consentement soit mieux obtenu.
	Sécurité	L'article 25 de la loi type de la SADC fait référence aux atteintes à la sécurité et en exige le signalement sans retard indu. Mais la loi type ne précise pas ce qui constituerait une atteinte à la sécurité, ou un retard indu, ou ce qui serait considéré comme un motif raisonnable de retard. De plus, elle n'oblige pas le responsable du traitement à expliquer à la DPA les raisons de son retard. L'article n'oblige même pas le contrôleur des données à notifier la violation à la personne concernée. De plus, le contrôleur des données et le processeur des données ne sont pas tenus d'indiquer les renseignements qui ont été compromis. Ceci n'est pas conforme au Préambule, qui appelle à la transparence et à la responsabilité de la part du contrôleur des données et du processeur des données. Et surtout, le fait d'imposer ces obligations à un contrôleur des données n'est pas nécessairement onéreux étant donné l'existance d'une DPA pour donner des directives. Les contrôleurs des données peuvent établir des procédures de notification en se conformant aux obligations en matière de données à caractère personnel, de sorte que leur tâche soit simplifiée. Le contrôleur des données doit informer la DPA et la personne concernée des informations qui ont été compromises et leur suggérer des moyens de se protéger contre les attaques. En effet, l'entreprise elle-même est la mieux placée pour comprendre la nature et l'étendue de la violation. Sans la création de ces formes d'obligations positives, les lois n'assurent pas une transparence suffisante.
	Protection de la vie privée dès la conception	Le concept de « Privacy by design » est l'approche adoptée lors du développement de technologies et de systèmes numériques qui intégre la protection de la vie privée par défaut à la technologie et aux systèmes pendant le processus de conception et de développement. Cela signifie que lors de la conception d'un

		produit, la priorité est donnée à la protection de la vie privée, aussi bien qu'à toute autre fin que le système sert. Le projet de loi type de la SADC sur la protection des données ne met pas l'accent sur le principe de « Privacy by design », qui est un aspect important à considérer en ce qui concerne les 4IR. Par conséquent, nous recommandons qu'au lieu que le contrôleur des données ait de simples « case à cocher », en plus de se conformer aux règlements de protection des données qui lui sont imposés, il mette en œuvre des mesures et procédures techniques et organisationnelles appropriées de manière à ce que toutes les activités de traitement des données, y compris la collecte, le stockage et l'utilisation des données, répondent aux exigences en matière de protection des données, tout en assurant la protection des droits des personnes. Ces formes d'obligations positives pour les entreprises peuvent contraindre concrètement la pratique de la protection des données, mais ne doivent pas nécessairement être très punitives.
	Flux de données	Le flux de données est une réalité fondamentale de la façon dont la numérisation et la mondialisation ont conduit à l'économie numérique. Alors que de plus en plus d'activités économiques et sociales passent au virtuel, l'importance de la protection des données et de la vie privée est de plus en plus reconnue, notamment dans le contexte du commerce international. La protection des données est directement liée au commerce de biens et de services dans l'économie numérique. Une protection insuffisante peut avoir des effets négatifs sur le marché en réduisant la confiance des consommateurs et une protection trop stricte peut restreindre excessivement les entreprises, entraînant des effets économiques négatifs. Veiller à ce que les lois considèrent la nature et la portée mondiales de leur application et favorisent la compatibilité avec d'autres cadres est de la plus haute importance pour les flux commerciaux mondiaux qui dépendent de plus en plus d'Internet. Il est essentiel de se pencher sur la question des transferts transfrontaliers de données au moyen de textes précis et de promouvoir un ou plusieurs mécanismes que les entreprises puissent utiliser pour faciliter les flux de données internationaux.
	Coopération transfrontalière, harmonisation et normes minimales	Les limitations du transfert transfrontalier de données pourraient entraîner la perte d'opportunités commerciales et réduire la possibilité de commerce international d'une organisation, provoquant une réduction de l'empreinte géographique et une perte de compétitivité du marché. Mais la réglementation des données qui est synchrone avec d'autres juridictions contribue à la confiance mutuelle et pose les bases d'un échange de données fiable, y compris (mais sans s'y limiter) des données personnelles. Une conception erronée de l'harmonisation en matière de protection des données provient du malentendu selon lequel l'harmonisation exige que toutes les législations nationales soient identiques. Cette approche ne tient pas compte des différences nationales en termes de cadres existants ou de progrès de l'innovation technologique. L'harmonisation devrait plutôt être pensée comme une compatibilité entre les législations nationales, sur la base d'un ensemble de principes de base convenus en matière de protection des données.
	Autorités de protection des données	Avoir des autorités de protection des données indépendantes, accessibles et disposant de ressources suffisantes (tant financières qu'humaines) est un aspect important pour atteindre l'équilibre entre un établissement de règles souples et une surveillance responsable. L'efficacité des DPA dépend également de la mesure

		dans laquelle la loi habilitante leur a donné les moyens d'enquêter et de rendre des ordonnances exécutoires relativement à leur mandat. Une DPA dotée de ressources et de pouvoirs suffisants peut contribuer à alléger le fardeau d'observation pour les secteurs privé et public.
	Recours efficaces et justice administrative	En dehors des procédures de notification, les personnes concernées doivent être assurées d'un accès adéquat aux recours. Toutefois, cela nécessite plus qu'un accès à une DPA. En effet, afin de faciliter la production de règlements adaptables, la DPA doit aussi être adéquatement habilitée. Par exemple, le fait de permettre à une DPA d'autoriser des exclusions étudiées évite que les obligations positives générées soient trop onéreuses pour différentes formes d'entreprise. Mais pour faciliter ce type de flexibilité, un paradigme de justice administrative approprié est nécessaire afin d'assurer la responsabilisation dans la prise de décision. Un autre élément intéressant est la restriction présente dans la loi sud-africaine qui interdit la prise de décision automatisée. Dans le contexte de l'IA, ces interdictions sont dignes de mention.
	Souveraineté des données	Il existe deux approches de la souveraineté faible et forte des données : d'une part, la souveraineté faible des données concerne les initiatives de protection des données menées par le secteur privé et mettant l'accent sur les aspects de la souveraineté des données liés aux droits numériques ; D'autre part, une forte souveraineté en matière de données favorise une approche dirigée par l'État, qui met l'accent sur la protection de la sécurité nationale. Cependant, la localisation des données va au-delà de la régulation des conditions de transfert et oblige à détenir toutes les données personnelles au niveau national. Ces exigences extrêmes peuvent toutefois interférer avec les objectifs de l'économie numérique et ne devraient jamais remplacer l'étape la plus fondamentale de création de lois sur le traitement des données.
Accès aux données et à l'information	**Open data**	Les lois sur l'accès à l'information devraient contenir des directives claires sur l'open data. Bien que la mise en place de politiques sur les open data soient une étape nécessaire pour assurer la transparence des open data gouvernementales à l'échelle nationale, un environnement plus propice à l'adoption de telles politiques publiques pourrait être créé grâce à des directives législatives. Dans ces cadres, les gouvernements « […] devraient donner la priorité à la collecte de données qualitatives et quantitatives sur la participation des femmes à l'économie numérique afin d'initier un dialogue constructif et l'élaboration de politiques »., mais aussi afin d'augmenter les bénéfices des données gouvernementales (UNECA, 2019). En d'autres termes, les obligations devraient s'étendre au-delà de la simple divulgation à l'inclusion de l'obligation positive de générer des données de certains types et selon certaines normes. Ces obligations en matière de production peuvent contribuer d'une certaine façon à l'harmonisation des questions de collecte de données biométriques et autres par l'État.
	Explication, transparence et algorithmes	Des problèmes de transparence, à la fois pratiques et normatifs, découlent de la prépondérance de la prise de décision automatisée et des services algorithmiques. Une solution relative aux algorithmes peut être « le droit à l'explicitation »

		potentiellement généré à partir d'un ensemble de droits de la personne dans le Règlement général sur la protection des données (RGPD) de l'Union européenne, qui exige que les collecteurs de données personnelles expliquent aux personnes concernées comment les données sont traitées et utilisées (ce qui pourrait expliquer les biais algorithmiques). Une autre façon d'assurer la transparence des algorithmes consiste à empêcher la prise de décisions automatisée (comme l'interdiction de la prise de décisions automatisée, décrite à l'article 17 de la Loi de 2013 sur la protection des renseignements personnels). Bien que ces interdictions comportent bien sûr des exceptions, elles abordent un aspect très spécifique de transparence algorithmique : *les décisions* prises sur la base d'algorithmes basés sur des *données personnelles.* Il peut également être instructif d'examiner comment les paradigmes d'accès à l'information existants peuvent être modifiés ou utilisés pour servir certaines des fins décrites.
	Droits des personnes concernées	Concernant les mandats de protection des données et de confidentialité, les personnes concernées ont besoin de droits qu'elles puissent faire valoir pour faire respecter la transparence. Les droits des personnes concernées, qui leur permettent d'accéder, d'évaluer, d'examiner et de supprimer leurs informations, peuvent être associés autant à la protection des données qu'à l'accès aux données.
	Identité numérique	Le contrôle des données personnelles est lié à la nécessité pour les personnes concernées d'avoir une identité numérique positive. L'identité numérique est un vecteur central pour l'engagement dans les services numériques publics et privés, tout comme la nécessité de récolter des formes de dividendes numériques. En 2017, la Banque mondiale, dans le cadre de son programme ID4D, a élaboré des « Principes d'identification pour le développement durable ». Assurant une couverture universelle et une sécurité robuste, ces principes ont ensuite servi de fondement au mouvement #Good ID. Ces types de principes devraient éclairer la mise en place de systèmes d'identité numérique conçus à la fois par le secteur privé et le secteur public, qui possèdent des cadres de gouvernance des données suffisants. (Le rôle des droits des personnes concernées soutiendra l'établissement d'une bonne identité numérique en Afrique du Sud). Face aux avantages des bons systèmes d'identité énumérés, les mauvais systèmes d'identité en revanche peuvent être source d'exclusion et, même, peuvent faire augmenter les inégalités entre les citoyens. Ceci renforce la nécessité d'une DPA qui défende les impératifs de justice en matière de données, via un processus de traitement licite des données applicable à chaque acteur de la chaîne de valeur de l'identité numérique, qu'il s'agisse du secteur public ou du secteur privé.

8. Options stratégiques et recommandations : Sécurité et interférence des données

Sous-thème Politiques	Question de politique	Recommandation
Cybersécurité et surveillance	**Stratégies de cybersécurité**	La première étape pour avoir une politique et un cadre réglementaire efficaces en matière de cybersécurité est d'avoir une stratégie de cybersécurité s'harmonisant avec la loi. Les États membres en tant que contributeurs aux réglementations devraient publier une stratégie nationale de cybersécurité qui prévoit les possibilités économiques inclusives et les risques associés à l'adoption des TIC. Les éléments de la stratégie qui devront être harmonisés avec la loi comprennent : • Désigner une autorité compétente et délimiter clairement son autorité ; • Identifier les principales entités gouvernementales impactées ou responsables de la mise en œuvre de la stratégie nationale de cybersécurité ; • Déterminer les mécanismes nécessaires pour sécuriser l'infrastructure cybernétique critique et l'adoption des TIC ; • Déterminer les services critiques (en plus des infrastructures critiques) que la stratégie vise à rendre plus sécuritaires et robustes ; etc.
	Intervention en cas d'incident, signalement et partage de données	Pour faire face à d'éventuelles catastrophes cybernétiques naturelles ou d'origine humaine affectant des services critiques et des infrastructures d'information, chaque État membre doit avoir une capacité nationale efficace de réponse aux incidents. Les États membres doivent créer et maintenir en place des équipes nationales d'intervention en cas d'incident lié à la sécurité informatique (CSIRT) ou des équipes d'intervention en cas d'urgence informatique (CECRT). Les CSIRT devraient servir un large public national (au-delà du gouvernement et des fournisseurs d'infrastructures critiques), au travers par exemple des obligations proactives en matière de signalement des incidents (un facteur clé pour lutter contre les cybermenaces). Pour ce faire, les CSIRT devraient recueillir des données consistantes sur les types d'incidents et de risques. Les CSIRT devraient également faciliter l'échange d'information horizontal entre les organismes gouvernementaux, en tant qu'acte de défense de la sécurité nationale. Le régime d'accès à l'information peut également favoriser l'échange de renseignements.
	Coordination transfrontalière et intervention conjointe	La lutte contre les cyberattaques nécessite une coordination transfrontalière. L'Union européenne a récemment mis en place un régime de sanctions pour les cyberattaques, modèle que la SADC pourrait reproduire. Bien qu'il s'agisse davantage d'une question d'organisation régionale, les législatures nationales

		devront garantir un niveau de préparation de base en matière de cybersécurité afin de s'engager de façon proactive. Celles-ci devront également s'intéresser à la cybercriminalité.
Cybercriminalité	**Application de la loi cybernétique**	La cybercriminalité transcende les frontières nationales et exige des solutions transnationales et des approches internationales, multinationales et régionales. En développant les capacités d'application de la loi pour lutter contre la cybercriminalité par la ratification des documents des traités, la coopération internationale, le renforcement des moyens, la mise en œuvre de programmes anti-botnet ainsi que d'autres initiatives, les pays peuvent limiter les cyberrisques et stimuler la croissance économique future. Les États membres devraient montrer leur engagement international à protéger la société contre la cybercriminalité et renforcer de manière proactive la capacité nationale d'application de la loi en élaborant des lois et des cadres réglementaires. Ceci se traduit par une participation à des forums internationaux dédiés à la lutte contre les cybercrimes internationaux ainsi qu'à la définition de mécanismes juridiques et réglementaires nationaux pour combattre et poursuivre les cybercrimes. Les autorités juridiques et réglementaires désignées pour mener des activités de lutte contre la cybercriminalité doivent définir ce qui constitue une cybercriminalité et donner aux entités gouvernementales les moyens, l'expertise et les ressources nécessaires pour enquêter et réprimer efficacement les activités de cybercriminalité.
	Criminalisation	Une surdétermination de la criminalisation peut nuire aux composantes préventives de l'élaboration des lois dans ce domaine. Ceci doit être particulièrement pris en compte dans le contexte régional, car la criminalisation excessive peut entraver involontairement d'autres droits. En particulier, dans la région de la SADC, une prudence est nécessaire pour éviter la criminalisation de la parole. La législation doit préciser clairement les infractions via une liste d'infractions, qui devrait comprendre des infractions liées à l'intégrité des systèmes informatiques. Plus précisément, la législation devrait également inclure la criminalisation de la possession et de la transmission de pédopornographie et l'accès aux sites Web de pédopornographie. Une dérogation permettant aux organismes d'application de la loi de mener des enquêtes devrait être intégrée. Celle-ci devrait inclure des dispositions pour criminaliser la production et la vente de pédopornographie et les actes intentionnels et illégaux liés à la pédopornographie.
	Enquêtes criminelles et automatisation	Les enquêtes sur les crimes doivent tenir compte des réalités numériques. Tout d'abord, la loi doit garantir la protection de la recevabilité et du caractère sacré de la preuve numérique pour lutter efficacement contre la criminalité. Ainsi, par exemple, le droit procédural devrait satisfaire des considérations relatives à la préservation des données, à l'ordonnance de production, à la perquisition et

		à la saisie, à la collecte en temps réel, à l'extradition, à l'entraide et à la limitation de l'utilisation de la preuve. Et dans ce domaine, la loi doit veiller à ce que la prise de décision automatisée et la collecte de données auprès des organismes d'application de la loi ne soit pas préjudiciable pour le public.
	Sécurité organisationnelle	Compte tenu des questions d'immunisation collective liées à la cybersécurité et des vulnérabilités commerciales abordées, il est important de créer des obligations positives pour les entreprises afin de garantir la sécurité. Toutefois, pour que ces obligations ne soient pas trop oppressives, elles devraient être sous-tendues par un régime de réglementation avec une autorité de réglementation capable de veiller à ce que les obligations soient flexibles et appropriées.
	Éducation et sensibilisation	L'élaboration d'une capacité institutionnelle mature pour lutter contre la cybercriminalité ne peut être assurée qu'en offrant une formation aux juges des tribunaux, aux procureurs, aux avocats, aux responsables de l'application de la loi, aux spécialistes judiciaires et aux autres enquêteurs sur la cybercriminalité et la cybercriminalité.
Restrictions d'accès	**Retraits et normes relatives aux droits de la personne**	Si les procédures de notification et de retrait sont généralement intégrées à la législation électronique - et fournissent une notice d'intervention propre à chaque cas - il est possible d'y inclure des considérations relatives aux droits de la personne et à la primauté du droit en y intégrant des considérations d'équilibre équitable.
	Application régulière de la loi, proportionnalité et nécessité	Les règles normatives pour considérer l'interférence avec l'accès à Internet peuvent venir des droits humains internationaux. Des considérations telles que la proportionnalité et la nécessité pourraient être utilisées pour guider les actions d'interventions possibles en droit ou en politique, toutes sous réserve de l'établissement de conditions préalables de légalité. La nécessité signifie que toute restriction de l'accès à Internet doit se limiter à des mesures qui sont strictement et manifestement nécessaires pour atteindre un objectif légitime. Il doit être démontré qu'aucune autre mesure ne produirait des effets similaires avec plus d'efficacité et moins de dommages collatéraux. Toute restriction de l'accès à Internet doit également être proportionnelle. Une évaluation de la proportionnalité devrait garantir que la restriction est « l'instrument le moins intrusif parmi ceux qui permettraient d'atteindre le résultat souhaité ». La limitation doit viser un objectif précis et ne pas empiéter indûment sur les autres droits des personnes ciblées. Cependant, toute tentative d'entrave à l'accès devra être comprise dans le contexte de la Déclaration conjointe sur la liberté d'expression et l'Internet, qui a co-déclaré avec Adv. Pansy Tlakula en qualité de Rapporteure spéciale sur la liberté d'expression en Afrique et la Résolution CADH que : La suppression de l'accès à Internet, ou à des parties d'Internet, pour des populations ou des segments entiers du public (fermeture d'Internet) ne peut

		jamais être justifiée, y compris pour des raisons d'ordre public ou de sécurité nationale. Il en va de même pour les ralentissements imposés à Internet ou à des parties d'Internet.

9. Options stratégiques et recommandations : Création de valeur axée sur les données

Sous-thème Politiques	Question de politique	Recommandation
Commerce électronique et transactions électroniques	**Rôle des organismes de réglementation**	Les SADC Mobile Money Guidelines contiennent des directives fortes sur les organismes de réglementation pour cette sous-catégorie précise de l'économie numérique. Comme il le convient dans le cadre de l'économie numérique, la réglementation exige un équilibre entre l'innovation et la contrainte. Pour favoriser l'innovation, de l'espace peut être offert aux entreprises grâce aux bacs à sable réglementaires pour tester leurs produits sans risque de responsabilité juridique. Le projet de loi type de la SADC sur les transactions électroniques et le commerce électronique (2013) souligne plus spécifiquement comment la réglementation relative aux composants de la transaction électronique devrait aider à assurer une clarté juridique.
	Complexité et impact des douanes	Des politiques visant à réduire la complexité douanière constituraient un moyen essentiel de faciliter le commerce électronique régional en améliorant à la fois la logistique pour les clients et les entreprises ainsi que les coûts et l'efficacité interne pour les entreprises. Il est également important de noter que, plus largement, l'incompatibilité des tarifs de douane peut présenter des risques de détournement des flux commerciaux. Pour permettre un environnement douanier propice, il faudra également disposer de l'infrastructure TIC requise, habiliter des fonctionnaires et veiller à ce que les commerçants transfrontaliers soient sensibilisés aux procédures de douane numérique. La recherche axée sur la demande a démontré que le coût des dispositifs constitue un obstacle majeur à l'utilisation d'Internet en Afrique. Malgré cela, les produits numériques sont taxés comme des produits de luxe dans de nombreux pays, ce qui entraîne une hausse des coûts, souvent amplifiée par des taxes douanières supplémentaires. Les gains en dividendes numériques résultant de l'amélioration de l'accès aux appareils, et donc de la connectivité, ont le potentiel de compenser les pertes économiques directes subies en minimisant la fiscalité.
	Protection des consommateurs	Il est essentiel de favoriser la confiance entre les consommateurs et les entreprises de commerce électronique, en particulier parce que l'acheteur et le vendeur sont « déplacés ». La solution réside dans les mécanismes de résolution des litiges – tant les entreprises que les passerelles de paiement devraient fournir des moyens à cet

		effet. D'autres principes de priorisation de la protection des consommateurs comprennent : • Des pratiques commerciales et publicitaires équitables (pensez par exemple à la transparence dans le placement de produits payants dans les médias sociaux) ; • des informations appropriées et complètes (comme l'étiquetage) ; • des processus efficaces de confirmation des transactions et de paiement axés sur la transparence vis-à-vis du consommateur ; • des mesures proactives pour gérer les risques liés à la vie privée et à la sécurité ; • la sécurité des produits dans les chaînes d'approvisionnement du commerce électronique ; • des périodes de rétraction pour les consommateurs ; • Un accès concret à des mécanismes efficaces pour résoudre les litiges, pouvant inclure le règlement des litiges en ligne.
	Cryptage	Le cryptage devient important en tant que méthode permettant aux utilisateurs de se protéger contre la cybercriminalité. Il peut s'appliquer dans le cadre des communications, mais aussi dans le cadre des transactions. Toutefois, le cryptage présente un conflit intéressant : alors qu'il renforce bien sûr la sécurité des personnes en ligne, les autorités répressives se plaignent qu'il entrave leur capacité à enquêter. Deux approches clés émergent : certains pays adoptent une législation visant à obliger les entreprises de technologie et de communication à décrypter les données des clients, tandis que d'autres (Pays-Bas, Estonie) sont favorables à un cryptage fort. Certains affirment qu'avec une entité de surveillance régionale fortement habilitée, exiger des « portes dérobées » dans le cryptage au niveau du bloc régional permettrait aux organismes d''appliquer la loi tout en préservant l'intégrité des communications. Cependant, aucune méthode viable pour garantir qu'aucun défaut de conception dans un système de cryptage ne soit exploitée par de mauvais acteurs n'a encore émergé. Étant donné que nombre des acteurs mondiaux, étatiques ou non, qui menacent la sécurité des communications et des transactions numériques en Afrique australe ont des capacités technologiques supérieures à presque tous les acteurs commerciaux (et à la plupart des acteurs étatiques) dans la région, les défauts de conception rendront la région vulnérable aux mauvais acteurs - tout en décourageant les entreprises technologiquement innovantes d'opérer dans la région.
Propriété intellectuelle et droit d'auteur	**Exceptions au droit d'auteur**	Étant donné que le droit d'auteur existe automatiquement, l'établissement des exceptions aux règles générales devient le point d'intersection le plus important pour le droit. Les instruments internationaux (*Convention de Berne, 1886) ont principalement établi un critère à trois facteurs, parfois appelé critère à trois étapes, soulignant que les exceptions et les limitations aux droits exclusifs sont admissibles :* a) dans certains cas particuliers ; b) qui ne compromette pas l'exploitation normale de l'oeuvre ; c) qui ne porte pas indûment atteinte aux intérêts légitimes de l'auteur ou du titulaire des droits. Bien que le sens précis de

		chacune des étapes reste contesté, le test peut être mieux résumé et clarifié comme suit : Les exceptions et les limitations au droit d'auteur sont permises si elles (1) ne sont pas trop vagues, (2) ne privent pas les titulaires de droits de revenus tangibles dans les domaines où les titulaires de droits obtiennent normalement ces revenus du droit d'auteur et (3) ne nuisent pas aux intérêts des titulaires de droits d'une manière disproportionnée. Ces exceptions devraient s'efforcer d'intégrer des considérations d'intérêt public et, dans le contexte du numérique et du développement, cibler le rôle de l'expansion de l'éducation et de l'inclusion des citoyens pour aider à lutter contre les inégalités qui peuvent survenir dans le contexte de l'économie numérique. Les dispositions relatives à l'utilisation et au traitement équitable peuvent alors exister en tant qu'exclusions plus générales et plus flexibles, s'appliquant lorsqu'aucune autre limitation du droit d'auteur n'est disponible. Ceci permettrait une certaine flexibilité dans un monde technologique en rapide évolution. En plus des exceptions universelles, certaines exceptions spécifiques sont importantes pour l'économie numérique : • Des exceptions pour permettre l'apprentissage en ligne. • Des exceptions pour l'utilisation transfrontalière de contenu incluant du contenu utilisé dans le cadre d'une exception dans le pays d'origine. • Des exceptions pour permettre l'interopérabilité des systèmes de TIC. • Des exceptions pour permettre la réparation et la sécurisation de dispositifs qui intègrent des logiciels.
	Dispositifs connectés à Internet	Des considérations de sécurité particulières devraient être en place pour les IOTs. Par exemple, des exigences peuvent être créées pour obliger les appareils connectés à Internet à avoir un mot de passe unique à l'appareil, qui puisse être modifié par l'utilisateur. Le fournisseur d'un appareil connecté à Internet devrait également être tenu de fournir un point de contact pour la notification des problèmes de sécurité.
	IA et IP	Bien qu'il s'agisse d'un défi relativement nouveau pour les politiques, les enjeux pour les innovateurs et les entrepreneurs sont élevés. Les étapes proactives comprennent : • Établir que le droit d'auteur ne s'applique qu'aux produits créatifs des auteurs humains. • Autoriser l'utilisation d'œuvres protégées par le droit d'auteur pour permettre une analyse avancée de l'information, comme la formation d'algorithmes d'IA. • Exiger des demandeurs de brevet qu'ils divulguent l'utilisation de l'IA dans le développement d'inventions.

	Responsabilité du fournisseur de services	Les fournisseurs de services devraient se voir accorder des limites de responsabilité. Pour les fournisseurs de services qui hébergent du contenu, la responsabilité limitée devrait être condition d'un avis de conformité et d'une exigence d'avis dans laquelle les plaintes sont adressées au fournisseur de services qui, à son tour, informe la personne qui a mis en ligne le contenu. Si la personne qui a mis en ligne le contenu accepte la plainte ou ne répond pas, le fournisseur de services peut alors supprimer le contenu. Si la personne qui a mis en ligne le contenu conteste la plainte, le fournisseur de services communique au plaignant ses coordonnées et ceux de sa défense. Le plaignant peut alors s'adresser à un tribunal ou à un autre organisme de règlement des litiges pour la résolution de la plainte.
	Mécanismes d'application	Indépendamment de la façon dont les exceptions sont formulées, il est essentiel de permettre aux créateurs d'exercer leur droit de profiter de leur travail. L'harmonisation demeure importante, tout comme l'éducation aux droits et les mécanismes d'accès à la justice (questions qui peuvent être abordées au moyen d'une réglementation guidée).

Annexures

Annexure 1: Relevant African Regional Instruments

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

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

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

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

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

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

Annexure 2: SADC Constitutional Mapping

Annexure 2A: Right to Privacy

Country	Privacy		
	Section	Text	Note
Angola	Article 32	**Article 32. Right to identity and privacy** 1. The right to personal identity, civil capacity, nationality, a good name and reputation, likeness, free speech, and privacy in personal and family life shall be recognised for all. 2. The law shall establish effective guarantees against the procurement and use of information relating to individuals and families in a manner, which is abusive or offends against human dignity.	Some reference to information privacy in the context of dignity.
Botswana	Article 9	**Article 9. Protection of privacy of home and other property** 1. Except with his or her own consent, no person shall be subjected to the search of his or her person or his or her property or the entry by others on his or her premises. 2. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision…[limitations provided].	Reference to privacy of the home and property, not in relation to information.
Comoros	Preamble (domicile)	**Preamble** The Comorian people solemnly affirm their will… They proclaim: … • the inviolability of the domicile in the conditions defined by law; … This Preamble shall be considered an integral part of the Constitution.	Reference to privacy of the home and property, not in relation to information.
Democratic Republic of Congo	Article 31	**Article 31.** All persons have the right to the respect of their private life and to the secrecy of their correspondence, of telecommunications and of any other form of communication. This right may only be infringed in the cases specified by the law.	Reference to personal and communication privacy.
Lesotho	Article 4, 11, 14	**Article 4. Fundamental human rights and freedoms** 1. Whereas every person in Lesotho is entitled, whatever his race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status to fundamental human rights and freedoms, that is to say, to each and all of the following-- … b. the right to personal liberty; … 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—	Reference to personal and communications privacy.

		a. searches of his or her person, home or property; b. the seizure of private possessions; or c. interference with private communications, including mail and all forms of telecommunications.	
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;	Congolese Patent and Trademark Office

					Directorate of Industrial 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	Regional Integration and International Trade (Ministry of Foreign Affairs)	Industrial Property Office (IPO)

				(Topographies) of Integrated Circuits Act, 2002		
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,	Intellectual Property Office (Ministry of Commerce Industry and Trade)	

				1918 (1918); Copyright Act, 1912 (1912)		
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);	Zimbabwe Intellectual Property Office (ZIPO) (Ministry of Justice, Legal and Parliamentary Affairs)	

				Patents Act (Chapter 26:03, as amended up to Act No. 14/2002) (2002); Industrial Designs Act (Chapter 26:02, as amended up to Act No. 25 of 2001) (2001), Integrated Circuit Layout Designs Act (Chapter 26:07) (2001); Merchandise Marks Act (Chapter 14:13) (2001); Intellectual Property Policy and Implementation Strategy [2018-2022]		