Union Africaine

An Integrated, Prosperous and Peaceful Africa

CADRE STRATÉGIQUE DE L'UA EN MATIÈRE DE DONNÉES

TABLE DES MATIÈRES

AVANT-PROPOS

Les pays africains ont conscience de l'énorme potentiel d'une économie numérique solide pour créer de nouvelles opportunités commerciales, accroître l'efficacité, contribuer au développement durable et remodeler la vie des gens. L'explosion du volume de données en tant qu'atout stratégique et élément clé de l'économie et de la société contemporaines a joué un rôle central dans l'élaboration des politiques, l'innovation et la création d'emplois.

L'adoption de la Stratégie de transformation numérique (STN) pour l'Afrique 2020-2030, ainsi que la mise en œuvre de la Zone de libre-échange continentale africaine (ZLECAf), ouvrent d'immenses perspectives pour l'avènement de marchés plus interconnectés et interopérables, tout en offrant des possibilités d'épanouissement aux start-ups technologiques et aux entreprises en ligne. Dans ce contexte, la Commission a élaboré le Cadre stratégique en matière des données de l'UA, qui a été approuvé par le Conseil exécutif de l'UA en février 2022.

En outre, le Cadre stratégique en matière des données de l'UA représente une étape importante vers la création d'un environnement de données consolidé et de systèmes harmonisés de gouvernance des données numériques, afin de permettre la circulation libre et sécurisée des données sur le continent tout en préservant les droits humains, en assurant la sécurité et en garantissant un accès équitable aux avantages, tout comme le partage de celles-ci.

Ce cadre définit une vision commune, des principes, des priorités stratégiques et des recommandations clés pour guider les pays africains dans le développement de leurs systèmes de données nationaux et de leurs capacités à utiliser efficacement les données et à en tirer de la valeur.

L'adoption de ce document de politique continentale par les organes de l'Union africaine témoigne de l'engagement et de la volonté politique des dirigeants africains d'investir dans les données en renforçant la collaboration intersectorielle et en développant les infrastructures nécessaires pour héberger, gérer, traiter et utiliser les données générées par les personnes et les entreprises afin d'éclairer la formulation des politiques et les processus décisionnels. À travers ce cadre, les pays africains conviennent de mettre en place les mécanismes et les réglementations nécessaires pour permettre, de manière conjointe, la circulation des données à travers l'Afrique et ouvrir la voie à la réalisation du marché unique numérique.

Notre approche des données est inclusive, transformatrice et tournée vers l'avenir. Nous visons à exploiter le potentiel de la révolution des données pour outiller les personnes, institutions et entreprises, stimuler le commerce numérique intra-africain, contribuer aux efforts d'intégration économique, sensibiliser les citoyens aux questions de protection des données et de confidentialité, promouvoir la recherche et l'innovation, préserver la souveraineté et la propriété des États, instaurer la confiance dans l'écosystème des données et renforcer la participation de l'Afrique en tant que front uni avec une position uniforme dans les discussions multilatérales sur divers domaines liés aux données.

L'appropriation de ce cadre par les pays africains et la mise en œuvre de ses recommandations clés et des interventions politiques proposées à l'échelle nationale, régionale et continentale, ainsi que le développement des capacités humaines et institutionnelles nécessaires à la poursuite de ces objectifs, positionneront l'Afrique comme un partenaire solide et permettront à la jeunesse africaine de participer et de s'épanouir dans l'économie et la société numérique mondiale.

Dra. Amani Abou-Zeid
Commissaire à l'infrastructure et à l'énergie de l'UA

REMERCIEMENTS

Le Cadre stratégique en matière des données de l'UA a été préparé sous la direction générale de S.E. Dr. Amani Abou-Zeid, Commissaire à l'infrastructure et à l'énergie, d'un groupe de travail comprenant Moses Bayingana, Directeur adjoint de la Division « Société de l'Information » et Souhila Amazouz, Chargée de mission principale (Coordinatrice d'équipe), ainsi que grâce aux contributions et apports précieux de :

Towela Nyirenda-Jere, Tichaona Mangwende et Gideon Nimako (AUDA-NEPAD) ; Jean-Pierre Gashami et Omar Elmi Samatar (BAD) ; Miriem Slimani (UAT) ; Aretha Mare et Jan Krewer (Smart Africa) ; Tunde Fafunwa, Mactar Seck et Linda Bonyo (CEA) ; Torbjorn Fredriksson et Pilar Fajarnes Garces (CNUCED) ; Amr Farouk Safwat et May Ragab Abdelhamid (présidence du Bureau STC-CICT) ; Philip Sauerbaum (UE) ; Caroline Gaju (UIT) ; Seyni Fati (GSMA) ; Tapiwa Ronald Cheuka (CUA/ETIM) ; Marguerite Ouedraogo Bonane et Patricia Poku (Réseau africain des autorités de protection des données) ; Tania Priscilla Begazo Gomez, Marelize Gorgens et Mark Williams (BM).

Le Cadre a bénéficié du soutien financier de GIZ et du soutien technique de Research ICT Africa.

Des commentaires ont été reçus à différentes étapes de l'élaboration de ce Cadre par des experts africains des États membres de l'UA, des communautés économiques régionales et des institutions spécialisées de l'UA participant à l'atelier de validation virtuelle et au quatrième comité technique spécialisé sur la communication et les TIC.

Le Cadre stratégique en matière des données de l'UA a été approuvé par la décision EX.CL/ Déc.1144(XL) du Conseil exécutif lors de sa 40e session ordinaire qui s'est tenue les 2 et 3 février 2022.

Addis Abeba, février 2022

RÉSUMÉ ANALYTIQUE

Les données sont de plus en plus considérées comme une ressource stratégique, essentielles à l'élaboration des politiques, à l'innovation et à la gestion des performances dans les secteurs privé et public, et offrant de nouvelles opportunités entrepreneuriales pour les entreprises et les particuliers. Les nouvelles technologies, lorsqu'elles sont appliquées aux services publics, peuvent générer des quantités massives de données numériques et contribuer de manière significative au progrès social et à la croissance économique. Le rôle central des données nécessite une perspective politique stratégique de haut niveau, capable de concilier des objectifs politiques multiples, de la libération du potentiel économique et social des données à la prévention des préjudices associés à la collecte et au traitement de masse des données personnelles.

L'objectif de ce document consiste à fournir le cadre stratégique qui permettra aux pays africains de tirer le meilleur parti d'une économie axée sur les données en créant un environnement politique favorable aux investissements privés et publics nécessaires pour soutenir la création de valeur et l'innovation fondées sur les données. Cet environnement favorable implique à la fois une collaboration entre les secteurs, les institutions et les parties prenantes des pays, un alignement de leurs priorités de développement, et l'harmonisation des politiques à travers le continent d'une manière qui offre l'ampleur et la portée nécessaires pour créer des marchés compétitifs au niveau mondial.

D'un point de vue politique, l'approche adoptée est centrée sur les personnes, les positionnant par rapport au rôle des données dans l'économie et la société contemporaines en identifiant les éléments et leurs connexions dans ce que l'on peut appeler « l'écosystème des données » afin d'identifier les points exacts d'intervention politique. Cette approche permet une évaluation systémique des enjeux interdépendants issus à la fois de l'impact des développements mondiaux sur les économies de données nationales émergentes, ainsi que d'une activité économique naissante axée sur les données, comme de dotations institutionnelles inégales et du développement humain dans de nombreux pays africains. Il est ainsi possible de concevoir un cadre stratégique en matière de données, fondé sur le contexte mais tourné vers l'avenir, qui s'appuie sur la réglementation économique pour guider les décideurs politiques dans la réalisation des opportunités de création de valeur par les données. Ce cadre indique les moyens de concrétiser les opportunités et d'atténuer les risques associés en créant un environnement favorable et fiable.

La construction d'une économie des données nationale et régionale favorable nécessitera des niveaux de collaboration sans précédent entre les parties prenantes pour répondre aux pressions économiques, politiques et stratégiques déjà ressenties par l'économie mondiale des données. En vue de garantir un accès équitable et sûr aux données pour l'innovation et la concurrence, les États membres devraient établir une approche juridique unifiée, claire et sans ambiguïté, qui offre une protection et des obligations sur tout le continent. Le cas échéant, les instruments et institutions juridiques existants devront être réexaminés pour s'assurer qu'ils ne sont pas en conflit les uns avec les autres et qu'ils offrent des niveaux complémentaires de protection et d'obligations.

Une stratégique globale en matière de données inclura nécessairement l'harmonisation entre les politiques et les lois sur la concurrence, le commerce et la fiscalité, tant au niveau national que régional. Ainsi, un écosystème de données optimisé pour l'Afrique permettra d'équilibrer la mobilisation des recettes et la nécessité d'éviter les distorsions sur les marchés locaux et

le système fiscal mondial. Les lois sur la propriété intellectuelle devraient également être révisées afin de stipuler clairement qu'elles n'entravent pas, de manière générale, la circulation des données ou la protection des données. Parallèlement, les gouvernements doivent élaborer des politiques et des stratégies numériques transversales pour coordonner les activités dans l'ensemble du secteur public et entre les secteurs public et privé afin d'atteindre les objectifs nationaux.

Bien qu'il existe de multiples définitions différentes des données, toutes reconnaissent qu'il existe de nombreux types de données différents. Il existe également de nombreuses façons de classer les données, ce qui a une incidence sur le choix d'une politique et d'une réglementation appropriées pour chaque catégorie afin d'atténuer tout risque potentiel lié au traitement, au transfert ou au stockage de ces données. Une distinction essentielle est celle entre les données à caractère personnel et les données à caractère non personnel, la protection des données consistant à garantir le respect de la vie privée des personnes concernées. Les lignes directrices sur la catégorisation des données devraient être l'une des premières actions du régulateur de l'information sur les données, une institution clé pour le développement d'un système national intégré de données, qui devrait être établie en partenariat avec toutes les parties prenantes concernées. Pour créer un environnement propice à l'économie des données, il est essentiel de mettre en place l'infrastructure numérique fondamentale nécessaire et les ressources humaines requises pour faire des données un atout stratégique. Il convient d'accorder toute l'attention nécessaire à l'élaboration de systèmes d'identification numérique solides pour la fourniture de valeur publique et privée aux citoyens et aux consommateurs.

Le cadre souligne également que cet objectif ne peut être atteint qu'en instaurant une culture de la confiance dans l'écosystème des données. Cela passe par la mise en place de systèmes de données sûrs et sécurisés, fondés sur des règles et pratiques efficaces en matière de cybersécurité et de protection des données, ainsi que sur des codes de conduite éthiques pour ceux qui définissent la politique en matière de données, la mettent en œuvre et pour ceux qui utilisent les données, que ce soit dans le secteur public ou privé. Cela n'est toutefois pas suffisant. La confiance dans la gouvernance des données et dans un système national de données est établie par la légitimité. Celle-ci implique des systèmes et des normes qui garantissent la conformité des secteurs public et privé, l'adhésion par le gouvernement lui- même aux règles de protection des données personnelles et le partage des données publiques par ce dernier.

Le cadre fait ressortir l'importance des processus politiques collaboratifs et fondés sur des preuves pour l'incorporation au niveau national de la politique proposée. La gouvernance et les dispositions institutionnelles doivent attribuer des rôles clairs au gouvernement en tant que décideur politique et aux régulateurs indépendants, dynamiques et compétents pour mettre en œuvre la politique et réglementer efficacement l'économie des données afin de garantir qu'une concurrence équitable produise des résultats positifs pour le bien-être des consommateurs. La création de régulateurs en matière de données et d'information, afin de promouvoir et de sauvegarder les droits des citoyens ainsi que leur participation et leur représentation équitable dans l'économie et la société des données, devra être une priorité pour les pays qui ne les ont pas encore mis en place. La coordination avec les autres régulateurs pour y parvenir sera essentielle. L'écosystème juridique doit être harmonisé et rééquilibré.

L'accès aux données est une condition préalable à la création de valeur, à l'esprit d'entreprise et à l'innovation. Lorsque les données sont de mauvaise qualité ou ne sont pas interopérables, elles limitent la capacité des entreprises et du secteur public à s'engager dans le partage et l'analyse qui peuvent apporter une valeur économique et sociale aux données. Ces cadres de

traitement doivent s'aligner sur les principes suivants : consentement et légitimité, limitation de la collecte, spécification de la finalité, limitation de l'utilisation, qualité des données, garanties de sécurité, ouverture (qui inclut la notification des incidents, corrélation importante avec les impératifs de cybersécurité et de cybercriminalité), responsabilité et spécificité des données. Les modèles de sécurité doivent également être transversaux, et mettre l'accent sur le stockage et le traitement en nuage des données sensibles/propriétaires, la gestion des API et le soutien des marchés de données équitables.

Il convient de prêter attention à l'accès à des données de qualité, interopérables et fiables - provenant principalement de l'État, mais aussi du secteur privé et d'autres secteurs - en revigorant les principes de la gouvernance ouverte sur tout le continent. Le renforcement des capacités doit être une priorité nationale et régionale essentielle, et des ressources devront être allouées à cet égard dans les domaines de la protection des données, de la cybersécurité et de la gouvernance institutionnelle des données dans les organismes concernés. Les compétences et la compréhension de l'écosystème des données devront également être développées dans les institutions publiques, ainsi que dans d'autres secteurs et communautés.

Le cadre repose sur les grands principes de transparence, de responsabilité des institutions et des acteurs, d'inclusion des parties prenantes, d'équité entre les citoyens et de concurrence équitable entre les acteurs du marché. Les principes qui guident le cadre sont la confiance, l'accessibilité, l'interopérabilité, la sécurité, la qualité et l'intégrité, la représentativité et la non-discrimination.

Ainsi, comme il est souligné dans le cadre, la collaboration transversale doit être étayée par des mécanismes visant à stimuler la demande de données, ce qui implique d'encourager les communautés de données innovantes et, du côté de l'offre, de garantir la qualité, l'interopérabilité et la pertinence des données dans les secteurs public et privé, ainsi que dans la société civile.

De même, comme indiqué dans le cadre, il existe plusieurs processus, mécanismes et instruments régionaux qui peuvent et doivent être mis à profit dans les efforts du continent pour développer un cadre politique cohérent en matière de données. Il s'agit notamment de l'accord de la Zone de libre-échange continentale africaine (ZLECAf), qui offre une opportunité de coopération sur un certain nombre d'aspects importants de ce cadre stratégique. La collaboration entre les parties prenantes nationales et régionales est également nécessaire pour que les pays africains deviennent plus compétitifs dans les forums mondiaux d'élaboration de politiques où sont élaborées les réglementations de l'économie mondiale des données, et où les États africains ont adopté des normes élaborées principalement par d'autres acteurs mondiaux.

Il est reconnu que les États africains ont des capacités économiques, techniques et numériques différentes, et les recommandations et actions doivent être interprétées dans cette optique. Il est toutefois envisagé que les différentes exigences liées à la mise en place d'un écosystème de données soient progressivement réalisées par les pays. Par ailleurs, plusieurs domaines peuvent être pris en charge indépendamment des capacités économiques ou techniques, notamment l'établissement d'une indépendance réglementaire, la promotion d'une culture de la confiance et de l'éthique, la mise en place de cadres de collaboration pour les secteurs concernés, l'élaboration de politiques et de réglementations transparentes, fondées sur des données probantes et participatives, la participation à des

processus et mécanismes régionaux de collaboration et la ratification de la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel.

Le Cadre présente un ensemble de recommandations détaillées et de mesures connexes pour guider les États membres dans la formulation des politiques dans leur contexte national ainsi que des recommandations pour renforcer la coopération entre les pays et promouvoir les flux de données intra-africains. Les principales recommandations générales de haut niveau sont évoquées ici. Il est recommandé que les États membres:

- coopèrent pour permettre aux données de circuler dans le continent tout en préservant les droits de l'homme, la protection des données, la sécurité et le partage équitable des bénéfices ;
- coopèrent pour créer les capacités nécessaires en matière de données afin de tirer parti des avantages des technologies et des services qui dépendent des données, notamment la capacité de gouverner les données de manière qu'elles profitent aux pays et aux citoyens africains et favorisent le développement ;
- promeuvent une politique transversale des données et une réglementation souple pour appréhender l'émergence de nouveaux modèles commerciaux dynamiques basés sur les données, qui puissent favoriser le commerce numérique intra-africain et l'entrepreneuriat basé sur les données ;
- créent des cadres intergouvernementaux pour faciliter la coordination des régulateurs autonomes de la concurrence, des différents secteurs et des données afin de réglementer efficacement la société et l'économie numérique, formuler, mettre en œuvre et réviser la politique des données de manière dynamique, prospective et expérimentale ;
- élaborent des législations nationales sur la protection des données à caractère personnel et des réglementations adéquates, notamment en ce qui concerne la gouvernance des données et les plateformes numériques, afin de garantir que la confiance est préservée dans l'environnement numérique ;
- établissent ou maintiennent des autorités de protection des données (APD) indépendantes, efficaces et dotées de ressources suffisantes, renforcent la coopération avec les autorités de protection des données des membres de l'Union africaine et mettent en place des mécanismes au niveau continental pour élaborer et partager des pratiques réglementaires et soutenir le développement institutionnel afin de garantir un niveau élevé de protection des données à caractère personnel ;
- favorisent l'interopérabilité, le partage des données et la réactivité à la demande de données par la mise en place de normes de données ouvertes dans la création de données qui soient conformes aux principes généraux d'anonymat, de respect de la vie privée, de sécurité et à toute considération sectorielle relative aux données afin de faciliter l'accès des chercheurs, des innovateurs et des entrepreneurs africains aux données à caractère non personnel et à certaines catégories de données à caractère personnel ;
- favorisent la portabilité des données afin que les personnes concernées ne soient pas enfermées dans un seul fournisseur et, ainsi, encouragent la concurrence et la liberté de choix des consommateurs et permettent aux travailleurs indépendants de passer d'une plateforme à l'autre ;
- améliorent les infrastructures inégalement développées sur le continent en s'appuyant sur les actions régionales des CER afin d'accéder à une couverture efficace des réseaux à large bande, un approvisionnement énergétique fiable, ainsi que des infrastructures et des systèmes numériques (données) fondateurs (IDE) (identité numérique

(Digital ID)), des paiements interopérables fiables, une infrastructure de cloud et de données et des systèmes de partage de données ouvertes, pour le commerce numérique transfrontalier et le commerce électronique ;

- établissent un système national intégré de données pour permettre la création de valeur publique et privée basée sur les données, fonctionnant sur la base de cadres de gouvernance harmonisés qui facilitent le flux de données nécessaire à une économie de données dynamique, mais avec des garanties suffisantes pour être fiable, sûr et sécurisé ;
- administrent le système national intégré de données selon des principes d'accès, de disponibilité, d'ouverture (lorsque l'anonymat peut être préservé) d'interopérabilité, de sûreté, de sécurité, de qualité et d'intégrité ;
- intègrent des codes ou des lignes directrices sur les données propres à un secteur ou à un spécialiste dans les régimes nationaux et continentaux de gouvernance des données ;
- ratifient la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel dès que possible s'ils ne l'ont pas encore fait, afin de servir d'étape fondamentale pour l'harmonisation du traitement des données ;
- fournissent des lignes directrices pour promouvoir l'accès aux données afin de soutenir l'innovation locale, l'esprit d'entreprise et à des fins pro-concurrentielles dans les négociations à venir sur les protocoles relatifs au commerce des services et au commerce électronique, ainsi que sur les protocoles relatifs à la concurrence et à la propriété intellectuelle, dans la zone de libre-échange continentale africaine ;
- donnent la priorité aux partenariats qui respectent la neutralité politique et qui tiennent compte de la souveraineté individuelle et de la propriété nationale, afin d'éviter les interférences étrangères susceptibles de nuire à la sécurité nationale, aux intérêts économiques et aux développements numériques des États membres de l'UA ; et
- promeuvent la recherche, le développement et l'innovation dans divers domaines basés sur les données, notamment l'analyse des données massives, l'intelligence artificielle, l'informatique quantique et la technologie Blockchain.

Il est en outre recommandé à la Commission de l'Union africaine, aux CER et aux institutions régionales de :

- faciliter la collaboration entre les différentes entités qui traitent des données sur le continent par la mise en place d'un cadre de consultation pour les dialogues politiques au sein de la communauté de l'écosystème numérique afin de préserver l'intérêt de chaque acteur ;
- encourager et faciliter la circulation des données au sein des États membres de l'UA et entre eux en élaborant un mécanisme de circulation transfrontalière des données qui tienne compte des différents niveaux de préparation au numérique, de la maturité des données ainsi que des environnements juridiques et réglementaires dans les pays ;
- faciliter la circulation des données entre les secteurs et au-delà des frontières en élaborant un cadre commun de catégorisation et de partage des données qui tienne compte des grands types de données et les niveaux de confidentialité et de sécurité associés ;
- travailler en étroite collaboration avec les autorités nationales chargées de la protection des données personnelles des États membres de l'UA, avec le soutien du Réseau

africain des autorités de protection des données personnelles (RAPDP), afin de mettre en place un mécanisme et un organe de coordination qui supervisent le transfert des données personnelles au sein du continent et assurent le respect des lois et règles existantes en matière de sécurité des données et des informations au niveau national ;

- établir ou renforcer un mécanisme au sein de l'Union africaine pour centraliser et renforcer les engagements régionaux sur les normes de données ;
- établir des mécanismes et des institutions ou habiliter ceux qui existent déjà, au sein de l'Union africaine, afin de renforcer les capacités et de fournir une assistance technique aux États membres de l'UA pour l'internalisation de ce cadre politique en matière de données ;
- soutenir le développement d'une infrastructure de données régionale et continentale pour accueillir des technologies avancées axées sur les données (telles que le Big Data, l'apprentissage automatique et l'intelligence artificielle), un environnement propice et un mécanisme de partage des données nécessaires pour assurer la circulation des données à travers le continent ;
- œuvrer à la construction d'un cyberespace sûr et résilient sur le continent, qui offre de nouvelles opportunités économiques, par l'élaboration d'une stratégie de cybersécurité de l'UA et la création de centres opérationnels de cybersécurité pour atténuer les risques et les menaces liés aux cyberattaques, aux violations des données et à l'utilisation abusive d'informations sensibles ;
- permettre le partage des données et l'amélioration de l'interopérabilité entre les États membres de l'UA et d'autres mécanismes de l'UA, notamment le mécanisme de coopération policière de l'Union africaine (AFRIPOL) ;
- établir un Forum annuel d'innovation basée sur les des données pour l'Afrique afin de sensibiliser les décideurs politiques au potentiel des données en tant que moteur d'une économie et d'une société numériques et ainsi faciliter les échanges entre les pays et à permettre le partage des connaissances sur la création de valeur et l'innovation en matière de données et les implications de l'utilisation des données sur la vie privée et la sécurité des personnes ;
- renforcer les liens avec d'autres régions et coordonner les positions communes de l'Afrique sur les négociations internationales liées aux données afin de garantir l'égalité des chances dans l'économie numérique mondiale ; et
- élaborer un plan de mise en œuvre qui tienne compte de la souveraineté numérique des États ainsi que des différents niveaux de développement, de la vulnérabilité des populations et de la numérisation au sein des États membres de l'UA, notamment des aspects liés au manque d'infrastructures TIC et à l'absence de politiques et de législations en matière de cybersécurité.

1. INTRODUCTION

Les données sont au cœur de la transformation numérique qui se déroule à un rythme et à une échelle sans précédent au niveau mondial. Le recours aux technologies axées sur les données pour transformer la plupart des aspects de notre vie quotidienne et de notre travail en données quantifiables pouvant être suivies, contrôlées, analysées et monétisées est devenue un phénomène si répandu que le terme de « donnéification » a été inventé pour le décrire.

Ces processus, qui se sont accélérés au cours de ce que l'on a appelé la première « pandémie des données », peuvent transformer les organisations publiques et privées en entreprises axées sur les données, améliorer les flux d'informations et l'efficacité, et créer des économies plus compétitives. Si les bonnes conditions sont réunies, l'amélioration des flux d'informations peut également réduire les asymétries d'information entre les gouvernements et les citoyens, ce qui renforce finalement la bonne gouvernance.

Ces processus ont parfois été progressifs ou perturbateurs, mais tous ont été très inégaux. L'utilisation des données est l'un des principaux facteurs permettant d'accélérer la réalisation de l'Agenda 2063 et des Objectifs de développement durable (ODD), l'absence de données de qualité étant l'un des principaux obstacles à l'évaluation des progrès accomplis dans la réalisation des objectifs sous-jacents. Plus précisément, l'amélioration des systèmes de données intégrés contribue directement à la réalisation de plusieurs objectifs, tels que l'amélioration des systèmes de santé, d'éducation et d'identité, mais sans intervention poli- tique directe, la répartition inégale actuelle des opportunités et des inconvénients découlant de la donnéification entre les pays et au sein de ceux-ci se verra exacerbée.

C'est en fonction des politiques adoptées et mises en œuvre que les États africains pourront créer les conditions permettant de tirer parti de ces processus de numérisation et de donnéification pour créer de la valeur ajoutée, accroître l'efficacité et la productivité, améliorer les services sociaux et créer de formes nouvelles de travailler. Cet état de fait requiert une réponse africaine concertée.

L'optimisation des avantages d'une économie axée sur les données et la réduction des risques dépendent fortement de l'adoption de cadres politiques et réglementaires favorables qui renforcent la légitimité et la confiance du public envers la gestion des données. L'infrastructure de données qui permet un système de données intégré constitue un atout stratégique essentiel pour les pays, mais l'ampleur, l'étendue et la rapidité des changements induits par les technologies numériques axées sur les données rendent la réglementation complexe et gourmande en ressources. À mesure que les technologies émergentes deviennent plus essentielles dans l'économie des données, la diversité des parties prenantes et la pléthore de plateformes impliquées dans sa réglementation se développent également de manière spectaculaire, ce qui rend de plus en plus difficile pour les décideurs de rester impliqués et informés (Banque africaine de développement, 2019). Les technologies avancées émergentes comme l'intelligence artificielle (IA) sont susceptibles de remettre de plus en plus en question l'efficacité des approches législatives traditionnellement disparates en matière d'élaboration des lois.

Les données sont mondialisées par nature, ce qui signifie que, d'une part, les réglementations ont des implications transfrontalières et que, d'autre part, la préséance réglementaire est le plus souvent établie par les pays développés riches en données et à forte intensité de données.

La pression du marché est également imposée par des entreprises en oligopole, notamment Google, Apple, Facebook, Amazon et Microsoft (ou GAFAM). La nature des données permet à ces entreprises qui opèrent sur les marchés numériques mondiaux axés sur les données de tirer parti de leur avantage concurrentiel en matière de données et d'algorithmes dans le monde entier. Ceci affecte à terme la concurrence locale et entrave la compétitivité mondiale des participants nationaux à l'économie des données. Par conséquent, les questions de propriété intellectuelle et d'accès aux données, de commerce équitable, de concurrence et de droits des consommateurs ont un impact sur la politique en matière de données dans un contexte mondial et soulèvent la nécessité d'une gouvernance et d'une collaboration mondiales.

En outre, ces facteurs mettent en évidence le fait qu'une grande partie du développement des réglementations, de la gestion et des marchés de données échappe au contrôle des parties prenantes africaines, qui ont été en grande partie des « suiveurs de normes » dans la gouvernance mondiale. Ils soulignent également la nécessité d'une collaboration et de partenariats dans de nombreux écosystèmes de données africains, indépendamment de la maturité numérique et des dotations économiques plus larges.

Ce cadre stratégique offre donc aux pays la possibilité de s'assurer que les lois permettent de manière proactive l'accès aux données à des fins de développement, d'innovation et de concurrence. Dans le même temps, il démontre la nécessité de les harmoniser les uns avec les autres pour créer l'ampleur et la portée sur le marché nécessaires à la création de valeur et à l'innovation axées sur les données, qui peuvent catalyser le marché numérique unique envisagé dans la Stratégie de transformation numérique de l'Union africaine.

2. MANDAT

Le rôle central des données **exige une perspective politique stratégique de haut niveau, fortement ancrée dans le contexte local** et capable d'équilibrer des objectifs politiques multiples. Les politiques nationales en matière de données et les approches interopérables au niveau international peuvent contribuer à libérer le potentiel économique et social des données tout en prévenant les préjudices et en atténuant les risques (OCDE, 2019).

Ce cadre politique en matière de données découle de la Stratégie de transformation numérique (STN) adoptée par l'Union africaine en 2020 pour transformer les sociétés et les économies africaines d'une manière qui permette au continent et à ses États membres d'exploiter les technologies numériques pour une innovation locale qui améliorera les opportunités de vie, atténuera la pauvreté et réduira les inégalités en facilitant la fourniture de biens et de services.[1] La concrétisation des objectifs de la STN est essentielle à la réalisation de l'Agenda 2063 de l'Union africaine, le cadre stratégique panafricain pour l'unité, l'autodétermination, la liberté, le progrès et la prospérité collective, et des objectifs de développement durable des Nations unies.

Le Cadre stratégique en matière de données s'appuie sur des instruments et initiatives existants tels que la Stratégie de transformation numérique pour l'Afrique 2020-2030 (STN), l'accord de la Zone de libre-échange continentale africaine (ZLECAf), l'Initiative politique et réglementaire pour l'Afrique numérique (PRIDA), le Programme de développement des infrastructures en Afrique (PIDA), la Vision Smart Africa pour transformer l'Afrique en un marché numérique unique d'ici 2030, la Libre circulation des personnes (LCP), le Marché unique du transport aérien africain (MUTAA), Le marché unique de l'électricité en Afrique, le Cadre d'interopérabilité des systèmes d'identification numérique, la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo), la Déclaration sur la gouvernance de l'Internet et le développement de l'économie numérique africaine de 2018, les Lignes directrices sur la protection des données à caractère personnel pour l'Afrique, les lois types régionales sur la protection des données et la cybersécurité et la Charte africaine des droits de l'homme et des peuples.

Ce Cadre stratégique en matière de données définit une vision commune, des principes, des priorités stratégiques et des recommandations clés pour guider les États membres de l'Union africaine dans le développement de leurs systèmes de données nationaux et de leurs capacités à tirer efficacement de la valeur des données générées par les citoyens, les entités gouvernementales et les industries. Le potentiel des solutions fondées sur les données pour surmonter la plupart des problèmes de développement de l'Afrique est rendu possible par l'adoption par les États membres d'une stratégie commune en matière de données, étayée par une approche de gouvernance cohérente. En outre, le développement de systèmes de données intégrés est essentiel pour optimiser les flux d'informations et les gains de productivité découlant de la numérisation et de la donnéification.

1 Le Conseil exécutif, lors de sa trente-sixième session ordinaire tenue les 6 et 7 février 2020, a approuvé la Stratégie de transformation numérique pour l'Afrique (2020-2030), mentionnée dans la décision [EX.CL/Dec.1074 (XXXVI)], en tant que plan directeur qui guidera l'Agenda de développement numérique du continent, les données étant l'un de ses thèmes transversaux et un élément constitutif de la mise en place de l'économie et de la société numériques africaines. Pour permettre la création d'une économie et d'une société numériques en Afrique, le Conseil exécutif, dans sa décision [EX.CL/Dec.1074 (XXXVI)], a chargé la Commission de l'UA de diriger et de coordonner l'élaboration d'un cadre continental sur la politique en matière de données et de le soumettre au STC-CICT 4 en 2021 pour examen et approbation.

Le présent Cadre stratégique en matière de données vise à renforcer et à harmoniser les cadres de gouvernance des données en Afrique et à créer ainsi un espace de données partagé et des normes qui régulent la production et l'utilisation croissantes des données sur le continent. Il s'agit de créer un environnement numérique sûr et fiable pour stimuler le développement d'une économie numérique inclusive et durable qui favorise le commerce numérique intra-africain, conformément aux initiatives d'intégration économique régionale en cours dans le cadre de la ZLECAf.

CAS D'UTILISATION DES DONNÉES POUR LA CRÉATION DE VALEUR

Dans de nombreux pays africains, la fracture numérique se traduit par des déserts en matière de données, car de nombreuses personnes n'ont pas accès aux services et aux systèmes utilisés pour générer les données nécessaires à l'entraînement des algorithmes ou à l'analyse en vue de la prise de décision. Les ensembles de données générés par les utilisateurs, tels que les mises à jour des médias sociaux et les enregistrements de données de communication (CDR), constituent une part importante de la révolution des données, à condition qu'ils soient collectés de manière responsable. Ces ensembles de données peuvent être combinés et réutilisés avec d'autres données, telles que les données anonymes des citoyens, pour refléter les expériences vécues par des millions d'individus et fournir des informations précieuses sur de nombreuses communautés vulnérables différentes qui peuvent éclairer l'élaboration des politiques, améliorer les interventions et stimuler l'activité économique dans divers cas d'utilisation. Par exemple, au Sénégal, le big data a été utilisé pour cartographier le CDR, la mobilité et l'activité économique. Au Kenya, le big data sur les transactions d'argent mobile M-Pesa a été utilisé pour créer des produits de crédit et d'épargne pour les abonnés et des profils de crédit pour les petits exploitants agricoles à des fins de prêts d'intrants et de récolte, une section de l'économie qui n'est généralement pas en mesure d'accéder aux installations bancaires formelles.[2]

2.1 VISION

Le Cadre stratégique en matière de données envisage le potentiel transformateur des données en vue d'autonomiser les pays africains, d'améliorer la vie des personnes, de sauvegarder les intérêts collectifs, de protéger les droits (numériques) et de favoriser un développement socio-économique équitable.

En pratique, le processus vise à concrétiser cette vision dans un cadre qui permettra, une fois mis en œuvre de :

Donner aux Africains les moyens d'exercer leurs droits par la promotion de systèmes de données fiables, sûrs et sécurisés, qui seront intégrés sur la base de normes et de pratiques communes ;

Créer, coordonner et donner les moyens aux institutions de gouvernance de réguler, si nécessaire, le paysage des données en constante évolution et d'accroître l'utilisation productive et innovante des données afin de fournir des solutions et de créer de nouvelles opportunités tout en atténuant les risques ;

Veiller à ce que les données puissent circuler à travers les frontières aussi librement que possible, tout en réalisant une distribution équitable des bénéfices et en traitant les risques liés aux droits de l'homme et à la sécurité nationale.

2 *https://www.developlocal.org/the-big-data-in-africa-report/*

2.2 PORTÉE ET OBJECTIFS

Compte tenu du fait que les données traversent désormais tous les aspects de notre vie quotidienne, mais dans des circonstances très différentes à travers le continent, **le Cadre fournit des orientations fondées sur des principes** aux États membres pour faciliter l'incorporation au niveau national du cadre stratégique continental en matière de données de façon adaptée à leurs conditions et propose aussi un instrument ou un mécanisme pour intégrer et coordonner les efforts continentaux. Le Cadre stratégique africain en matière de données vise à **renforcer les systèmes de données nationaux** pour une utilisation efficace des données en créant un environnement favorable qui **stimule l'innovation et l'esprit d' entreprise afin de favoriser le développement d'économies fondées sur la valeur des données** et qui facilite l'interopérabilité des systèmes et les flux de données transfrontaliers nécessaires à la réalisation du marché numérique unique africain. Une fois harmonisé sur l'ensemble des marchés africains, il permettra de garantir que les réglementations soient claires et que l'échelle et la portée soient propices aux investissements nécessaires à la création de valeur publique et privée à partir des données, accompagnés des effets distributifs et les multiplicateurs non économiques qui en découlent.

En ce qui concerne la portée du cadre, il est important de tenir compte du fait que la politique s'intéresse à la **gouvernance des données qui comprend les données à caractère personnel, non personnel, industriel et public**, et pas seulement à la protection des données à caractère personnel qui a fait l'objet d'une attention particulière au niveau international et sur le continent au cours des dernières années.

Les objectifs généraux du cadre stratégique africain en matière de données sont les suivants :

- Permettre aux États de coopérer sur les questions de gouvernance des données pour atteindre des objectifs communs liés au développement durable de leurs économies et de leurs sociétés ;
- Informer et soutenir l'internalisation de la stratégique continentale par les pays africains ;
- Veiller à ce que les données puissent circuler à travers les frontières aussi librement que possible, tout en favorisant une répartition équitable des bénéfices et en traitant les risques liés aux violations des droits de l'homme et aux autres intérêts légitimes des États, tels que la lutte contre le blanchiment d'argent, l'évasion fiscale, les jeux d'argent en ligne, la sécurité nationale ;
- Favoriser et faciliter les flux de données transfrontaliers et augmenter les opportunités commerciales tout en garantissant un niveau adéquat de données personnelles et de vie privée ;
- Établir des mécanismes de confiance collaboratifs pour permettre aux données de circuler aussi librement que possible entre les États membres, tout en préservant la souveraineté des États membres et leur capacité à réguler l'économie numérique ;
- Permettre aux États, au secteur privé, à la société civile et aux organisations intergouvernementales de coordonner leurs efforts sur les questions de données à travers le continent afin de réaliser un marché numérique unique et d'être plus compétitif dans l'économie mondiale ;
- Permettre la compétitivité dans l'économie mondiale grâce à une coopération étroite et durable des États africains, du secteur privé et de la société civile par le biais d'opportunités de restructuration pour optimiser les avantages de la donnéification de l'économie et de la société ;

- Veiller à ce que les données soient utilisées d'une manière durable qui profite à la société dans son ensemble et ne porte pas atteinte à la vie privée, à la dignité et à la sécurité des personnes ;
- Veiller à ce que les données soient largement disponibles avec les garanties appropriées pour une utilisation tant commerciale que non commerciale ; et
- faciliter des méthodes innovantes pour promouvoir les avantages publics en utilisant les données de nouvelles manières qui permettraient de tirer parti de la valeur des données en Afrique dans la prise de décision, la planification et le suivi et l'évaluation du secteur public.

Pour que le Cadre stratégique continental en matière de données atteigne ses objectifs et reflète les intérêts de toutes les parties prenantes, la formulation du **cadre stratégique s'inspire d'initiatives et de documents antérieurs**, tant en Afrique qu'à l'extérieur du continent. Le processus a inclus une consultation publique ouverte. Les contributions faites par le biais de cette consultation en ligne et d'un webinaire public ont permis d'élaborer le projet de ce Cadre stratégique.

En outre, la CUA a coordonné l'élaboration du Cadre stratégique continental en matière de données en collaboration avec des organisations panafricaines et des agences et institutions spécialisées de l'UA, à savoir : les Communautés Économiques Régionales, AUDA-NEPAD, le Secrétariat de Smart Africa, la Banque africaine de développement, l'Union africaine des télécommunications (UAT), la Commission économique des Nations unies pour l'Afrique, l'Union internationale des télécommunications (UIT), la Conférence des Nations Unies sur le commerce et le développement (CNUCED), la Banque mondiale ainsi que d'autres institutions partenaires.

Cadre réglementaire des données

Élaboration	Incorporation	Contrôle et évaluation
Détermination des enjeux stratégiques des principes généraux, ainsi que des recommandations et des mesures	Mise en œuvre des mesures (systèmes nationaux de données intégrées) Stratégies pour la réalisation progressive de conditions propices	Indicateurs Objectifs Évaluation
Initiatives continentales, mécanismes, instruments		
Gouvernance mondiale		

3. ESSOR DE L'ÉCONOMIE DES DONNÉES : NÉCESSITÉ DE REPENSER LES STRATÉGIES DE RÉGLEMENTATION

Un changement d'approche en matière de réglementation des données est nécessaire pour que les pays puissent bénéficier comme il se doit de l'émergence de l'économie mondiale des données. Ce changement est à l'origine du présent cadre. Les éléments clés de cette approche intégrée de la formulation de stratégies en matière de données sont présentés ci-dessous.

3.1. ES DONNÉES EN TANT QUE BASE D'UN NOUVEAU CONTRAT SOCIAL ET D'UNE ÉCONOMIE DE L'INNOVATION

Les données en elles-mêmes ont généralement peu de valeur. Ce n'est que par le traitement, la transmission, le stockage et la combinaison que la valeur est ajoutée. En termes économiques, les données peuvent être considérées comme un bien public dans la mesure où elles sont intrinsèquement non rivales, (au sens technique, elles sont utilisables à l'infini sans que cela n'affecte la capacité d'une autre personne à les utiliser). Elles sont naturellement non exclusives, ce qui signifie qu'il n'y a pas d'obstacles naturels à l'utilisation simultanée des mêmes données par plusieurs personnes. Bien qu'il existe des tentatives pour rendre les données excluables par des moyens technologiques et parfois juridiques, il ne s'agit pas de caractéristiques intrinsèques des données. Les tentatives de limiter l'accès, que ce soit à des fins de commercialisation ou de sécurité, peuvent être réglementées de manière à rendre les données non exclusives. Par exemple, les données ouvertes en vertu d'une licence internationalement reconnue ou de statistiques publiques peuvent être réglementées afin d'être accessibles comme la radiodiffusion publique en clair, en tant que bien public classique.

Les données ne génèrent pas non plus automatiquement de la valeur. Au contraire, il existe différentes utilisations des données et différentes méthodes permettant de mesurer la valeur économique et sociale des données et des flux de données (OCDE, 2019). Au sens économique, c'est ce que les entreprises font qui conduit à la création de valeur à la fois en interne au sein de l'entreprise et en externe à travers le réseau étendu de données. Théoriquement, cette valeur peut être quantifiée en attribuant une valeur monétaire prenant en considération plusieurs variables de coûts et de revenus, comme la manière dont les organisations facturent les données générées par les utilisateurs, ou le rapprochement des coûts de gestion des données tels que la collecte, la maintenance et la publication des données. La valorisation des données du point de vue des avantages socio-économiques - ou de la valeur des données non marchandes - intervient lorsqu'il existe des conditions fondamentales ou des catalyseurs qui permettent aux gouvernements de fournir des services publics plus efficaces, d'offrir une gestion efficace de l'environnement, et lorsque les citoyens vivent en meilleure santé et en sécurité économique grâce à l'exploitation des données (Banque mondiale, 2021). Un exemple de création de valeur des données publiques est l'utilisation des données pour informer les besoins d'allocation des ressources afin d'améliorer la prestation de services.

Ces caractéristiques des données ont été présentées ailleurs comme le **potentiel des données à fournir la base d'un nouveau contrat social** (Banque mondiale, 2021). Les orientations politiques qui découlent de cette approche mettent l'accent sur la nécessité de disposer

de données ouvertes, de normes d'interopérabilité et d'initiatives de partage des données pour exploiter le potentiel des données en vue de stimuler le développement, d'assurer une meilleure répartition des avantages liés aux données, d'encourager la confiance grâce à des garanties qui protègent les personnes contre les dommages liés à une utilisation abusive des données, de créer et de maintenir un système de données national intégré qui permette le flux de données entre un large éventail d'utilisateurs d'une manière qui facilite l'utilisation et la réutilisation sûres des données.

La confiance est essentielle pour un environnement de données robuste et florissant. Dans le contexte de la gouvernance numérique, la confiance est souvent assimilée à la sécurité technique et à la confiance dans le système technique nécessaire au fonctionnement du commerce électronique. Si la sécurité technique peut être une condition nécessaire à la confiance, elle n'est cependant pas suffisante. La confiance doit au contraire imprégner l'ensemble de l'écosystème des données, depuis la formulation centrée sur l'individu de politiques et de réglementations préservant les droits jusqu'à la garantie d'accès et d'utilisation des données afin de permettre une inclusion plus équitable dans l'économie des données.

Bien que les préjudices liés à la concentration des données et des informations et aux asymétries de pouvoir soient universels, leurs impacts sont inégaux, tant entre les pays qu'au sein de ceux-ci. La mise en place de politiques qui atténuent le risque différentiel pour différentes catégories de personnes, comme les enfants, ou pour des catégories de données dans différents secteurs, comme les données sur la santé, ou encore la garantie que la centralité croissante des données ne perpétue pas les injustices historiques et les inégalités structurelles, nécessiteront une réglementation beaucoup plus granulaire et adaptative. Si un cadre politique de préservation des droits en matière de données est essentiel, les notions individualisées de vie privée, de liberté d'expression et d'accès à l'information (droits de première génération) dans les cadres normatifs actuels de protection des données ne suffiront pas à garantir des résultats plus équitables et plus justes. Les droits sociaux et économiques de deuxième génération sont également pertinents pour plusieurs domaines de la gouvernance des données en ce qui concerne la disponibilité, l'accessibilité, la facilité d'utilisation et l'intégrité des données qui nécessitent une gouvernance des données pour avoir un impact sur l'inclusion équitable. Cela met en évidence la nécessité d'aller au-delà d'une réglementation de conformité négative et de passer à une réglementation positive qui créera un environnement permettant aux États et aux citoyens africains de participer efficacement à l'économie numérique. La création des conditions permettant l'accès nécessaire aux données tout en préservant les droits nécessitera le renforcement des capacités institutionnelles au sein de l'État et des capacités à réglementer de manière agile afin d'exploiter le potentiel des données visant à résoudre certains des problèmes les plus insolubles du continent.

Pour y parvenir, **les décideurs politiques doivent équilibrer certaines des tensions liées à la valorisation des données** afin de les optimiser à ces fins. La transformation des données en informations utiles pour guider la prise de décision s'articule autour de la chaîne de valeur des données, où les entreprises et certaines entités publiques disposent de cadres adéquats pour soutenir un écosystème de données cohérent. La création de valeur à partir des données peut renforcer les intérêts privés, comme l'amélioration de l'efficacité opérationnelle des entreprises, l'augmentation de leur clientèle et la création de produits et services innovants qui profitent aux activités commerciales et aux personnes concernées. Pour les gouvernements, la valeur publique des données est réalisée en s'assurant que les avantages socio-économiques des données permettent d'atteindre des objectifs socio-économiques plus larges. Bien que l'évaluation des données publiques et privées ait des intentions et des résultats différents, elles ne s'excluent pas mutuellement. De fait, la valeur marchande et la valeur non marchande

ne devraient pas être corrélées au secteur privé et au secteur public. La valeur non marchande pourrait également être reliée à la recherche ou à la société civile. Le secteur public peut également créer une valeur marchande en ouvrant certains ensembles de données et en établissant des sources de revenus nouvelles. Il existe également des interactions innovantes entre les acteurs publics et privés qui peuvent améliorer l'écosystème global des données pour répondre aux besoins de développement socio-économique et améliorer le bien-être.

Compte tenu de la complexité et de l'adaptabilité croissante du système mondial de communication, les formes de gouvernance, aussi bien les nouvelles formes que les formes traditionnelles, se révèlent incapables de fournir des outils adéquats pour la gouvernance de biens publics mondiaux tels que les données. D'un point de vue politique, on distingue de plus en plus la création de valeur à partir des données et les caractéristiques d'extraction de valeur des modèles industriels et des modèles d'affaires existants axés sur les plateformes et les données (Mazzucato et al., 2020). Il y a eu peu de retenue de la part des régulateurs de la concurrence ou des données sur la multiplication des plateformes mondiales monopolistiques produisant et extrayant des quantités massives de données privées, qui ont été transformées en marchandises avec apparemment peu de considération pour les implications sociales et négatives pour les personnes concernées (Zuboff, 2019). Cela peut nécessiter des réponses réglementaires spécifiques, et transversales, afin de préserver les obligations positives sur la gouvernance des données.

3.2 NÉCESSITÉ D'UNE GOUVERNANCE DES DONNÉES - CRÉER DE LA VALEUR, PRÉVENIR LES PRÉJUDICES

La gouvernance des données à un niveau macroéconomique apparaît comme une opportunité d'utiliser des normes, des règles, des standards et des principes **en tant que mécanismes permettant à la fois d'atténuer les risques et préjudices identifiés liés aux données, tout en faisant progresser le développement de l'économie des données et les dividendes numériques.**

La politique en matière de gouvernance des données comporte ainsi certains mécanismes d'intérêt pratique :

- Aligner les principes pour souligner que la gouvernance des données est une fonction normative ;
- Attribuer des rôles et des responsabilités pour la mise en œuvre de la politique à des niveaux macro et micro ;
- Identifier et assurer la clarté juridique et politique des mécanismes de mise en œuvre de la gouvernance des données ;
- Identifier et encourager la collaboration entre les groupes de parties prenantes verticales et horizontales ;
- Tenir compte de la nécessité que les données circulent pour améliorer la création de valeur tout en créant des incitations économiques pour investir dans les infrastructures et les services de données ; et
- Établir des mécanismes de confiance pour favoriser le partage des données selon les modalités convenues par toutes les parties sur les règles d'utilisation des données et les questions de responsabilité (exactitude des données, par exemple).

De plus, cette simplification de la politique de gouvernance des données doit ensuite être c ontextualisée par rapport aux défis et opportunités décrits ci-dessous.

Ainsi, les priorités en matière de gouvernance deviennent les suivantes :

Définition des données - Fournir des spécificités et des détails sur les types de données à réglementer, et dans quelle mesure, afin de garantir que les différents acteurs bénéficient au maximum de la mise en œuvre de la politique en matière de données. Cela devrait être fait en tenant compte de la valeur et de la nature des données.

Coordination continentale - Fournir des mécanismes et des priorités pour la coordination sur le continent afin de renforcer la position de l'Afrique au sein de la gouvernance mondiale et fournir un soutien à l'incorporation au niveau régional.

Capacité institutionnelle nationale - Assigner des obligations, des responsabilités et des compétences aux acteurs institutionnels au niveau national pouvant aider à créer un environnement national cohérent pour les communautés de données (publiques et privées) afin d'instituer des activités liées aux données.

Collaboration nationale - Assurer l'alignement des politiques, identifier les participants multipartites et promouvoir des mécanismes pour une internalisation réussie.

Soutien aux politiques - Fournir des normes et des solutions applicables qui mettent l'accent sur la qualité, le contrôle, l'accès, l'interopérabilité, le traitement et la protection des données et la sécurité des données nationales comme moyen de faire croître l'économie des données.

Clarté - Garantir la clarté, qui facilite la conformité, n'entraîne pas de restrictions involontaires, mais peut également servir de fondement à la coordination transfrontalière (et entre les silos).

4. CONTEXTE

4.1. VUE D'ENSEMBLE DES TENDANCES EN MATIÈRE DE POLITIQUE ET DE LÉGISLATION RÉGIONALES INTERNATIONALES

De nombreuses juridictions dans le monde n'ont pas de politique en matière de données, et environ un tiers d'entre elles n'ont pas de législation en la matière. La CNUCED a constaté en 2020 que 66 % des pays du monde disposent d'une législation quelconque, que 10 % ont un projet de législation, que 19 % n'ont aucune législation et que 5 % n'ont aucune données (CNUCED, 2020).

À l'échelle mondiale, un certain nombre d'instruments ont vu le jour dans ce contexte, tel que le RGPD 2016/679 de l'UE. Parmi les autres instruments régionaux figurent le cadre de protection des données à caractère personnel de l'APEC et l'accord de partenariat transpacifique (PPT). Ces accords adoptent des approches légèrement différentes de la protection des données et peuvent servir de points de référence pour les efforts concertés de l'Afrique en matière de protection des données.

Le RGPD 2016/6 de l'UE a une grande envergure avec une définition étendue de ce que constituent les données à caractère personnel. Sa vaste portée territoriale s'applique à l'intérieur et à l'extérieur de l'UE, prévoit de graves sanctions en cas de subversion du règlement, exige une ouverture et une transparence considérables et, surtout, accorde aux individus des droits substantiels qui peuvent être appliqués aux entreprises. Cette approche de la protection des données s'articule autour d'un programme de défense des droits de l'homme dans l'écosystème numérique.

Le cadre de protection des données à caractère personnel de l'APEC, qui a été mis en œuvre par les États membres de l'APEC depuis 2005, se compose d'un ensemble de principes visant à garantir la libre circulation des informations à l'appui du développement économique. Le cadre de l'APEC adopte une approche différente de la protection des données en alignant le mandat du cadre sur la promotion du commerce et de l'investissement. L'un des points forts du cadre réside dans le fait qu'il souligne que les réglementations en matière de protection de la vie privée doivent prendre en considération l'importance des intérêts commerciaux et des entreprises, ainsi que les cultures et autres diversités des économies des États membres.

Le Partenariat transpacifique global et progressiste (PTPGP) met l'accent sur l'ouverture du commerce et l'intégration régionale entre les États membres. L'accord autorise le transfert transfrontalier de renseignements par voie électronique, y compris de renseignements personnels, lorsque cette activité est nécessaire à la « conduite des affaires », mais les pays peuvent exiger la protection des données transférées.

En dehors de ces accords multilatéraux, les objectifs publics de la protection des données sont généralement articulés autour de la protection de la vie privée des personnes et des communautés, de la protection des données précieuses contre les fuites, les pertes et les vols, et du maintien et de l'augmentation de la confiance du public, des investisseurs et des clients. Dans le but d'atteindre ces objectifs, de nombreux pays ont inclus dans leur législation nationale des obstacles potentiels à la circulation des données, tels que des exigences de localisation des données et, dans certains cas, des exigences plus strictes en matière de traitement et de

collecte des données. Ces obstacles peuvent, par inadvertance, retarder ou contrecarrer les objectifs de cadres stratégiques régionaux de plus grande envergure.

Dans l'évolution des politiques nationales en matière d'économie numérique, plusieurs stratégies se sont cristallisées au niveau mondial, telles que l'approche gouvernementale (préconisée par l'UE), l'approche du secteur privé (promue par les États-Unis), l'approche politique descendante (illustrée par Singapour) et l'approche ascendante (comme à Hong Kong ou en Chine). Ces approches ont des effets complémentaires variables sur la mise en œuvre, le déploiement, l'impact, l'innovation, l'agilité et la stabilité des politiques.

4.2 CONTEXTE POLITIQUE ET LÉGISLATIF AFRICAIN

Conformément aux précédents internationaux, la plupart des efforts en matière de réglementation des données sur le continent se sont concentrés sur la protection des données, l'objectif principal étant de respecter et de protéger les droits à la vie privée des utilisateurs d'Internet. Bien que l'utilisation et le traitement des données soient une préoccupation transversale, qui a un impact sur un éventail de domaines politiques traditionnellement cloisonnés, il n'existe pas d'exemples de lois générales qui réglementent tous les aspects des données. Au lieu de cela, les données ont été réglementées par cinq branches du droit : la léglisation sur la protection des données, la législation sur la concurrence, la législation sur la cybersécurité, la législation sur les communications et les transactions électroniques et la législation sur la propriété intellectuelle, qui peuvent entrer en conflit dans certains cas et laisser des lacunes dans d'autres[3].

On estime que 32 des 55 pays d'Afrique ont adopté ou repris à leur compte une forme de réglementation dont l'objectif principal consiste à protéger les données à caractère personnel. Au niveau régional, des outils législatifs tels que le cadre de la Communauté d'Afrique de l'Est relatif aux cyberlois de 2008, l'Acte Additionnel relatif à la protection des données à caractère personnel dans l'espace de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) de 2010 et la loi type de la Communauté de développement d'Afrique australe de 2013 harmonisant les politiques pour le marché des TIC en Afrique subsaharienne ont été élaborés. Sur le plan continental, l'Union africaine a élaboré le premier cadre panafricain grâce à la Convention de l'Union africaine sur le cyber sécurité et la protection des données à caractère personnel (Convention de Malabo) en 2014, qui n'est pas entrée en vigueur mais est en cours de ratification.

Les lois et protocoles régionaux sur la concurrence dans les communautés économiques régionales (CER) établies s'appliquent aux entreprises qui traitent des données, bien qu'elles ne fassent généralement pas explicitement référence aux données. Il s'agit notamment des règlements et des règles de concurrence du COMESA (2004), de la loi sur la concurrence de la CAE (2006), du protocole du marché commun de la CAE et du protocole relatif à la création d'une union douanière de la CAE, de l'Acte additionnel de la CEDEAO relatif à « l'adoption des règles de concurrence communautaires et aux modalités de leur application dans l'espace de la CEDEAO », du Protocole de la SADC sur le commerce (2006) et de la Déclaration de la SADC sur la coopération régionale en matière de politique de concurrence et de consommation (2009). Ils abordent les pratiques anticoncurrentielles, y compris l'abus de position dominante, ainsi que la structure du marché par la réglementation des fusions et acquisitions. Toutefois, les détails et les approches sont différents, ce qui pose des problèmes aux entreprises opérant dans plusieurs régions.

3 Les dimensions continentales de ces défis sont abordées par le biais de la collaboration numérique continentale.

AUTRES INITIATIVES MAJEURES SUR LE CONTINENT CONCERNANT LA POLITIQUE DES DONNÉES

L'initiative politique et réglementaire pour l'Afrique numérique (PRIDA[4]) : Dans le cadre de la mise en œuvre de ce projet, la Commission de l'Union africaine a mis en place un groupe de travail d'experts qui a contribué à l'identification des indicateurs clés d'harmonisation et au développement d'un modèle et d'un outil de suivi et d'évaluation (S&E) sur la protection des données et la localisation qui sont prêts à être utilisés par les États membres de l'UA et les organisations régionales pour évaluer le degré d'harmonisation et d'alignement des lois et réglementations nationales.

Smart Africa soutient la création d'un cadre harmonisé pour la législation en matière de protection des données en Afrique et la mise en place de mécanismes de collaboration et de confiance intercontinentaux, par le biais du groupe de travail sur la protection des données de Smart Africa. Le groupe de travail produira une cartographie des cadres juridiques, des directives de mise en œuvre pour les États membres de Smart Africa et des recommandations sur l'harmonisation et les mécanismes de collaboration entre les autorités de protection des données (APD).

4.3 ANALYSE DE LA SITUATION DE L'ÉCONOMIE DES DONNÉES EN AFRIQUE

Entreprendre une analyse situationnelle de l'ensemble du continent avec ses divers systèmes juridiques, réglementaires et politiques et considérer l'inégalité du développement économique et de la préparation au numérique des pays est intrinsèquement limité et trop généralisé. L'objectif de l'analyse SWOT de haut niveau est d'identifier les points forts et les points faibles des pays au niveau régional et d'identifier les possibilités potentielles et les risques connus associés aux processus mondiaux de numérisation et d'intégration des données qui caractérisent le développement de l'économie des données pour tous les pays, et ce que cela signifie spécifiquement pour les pays africains, dans leur contexte de développement plus large.

4 PRIDA est une initiative conjointe de l'Union africaine (UA), de l'Union européenne (UE) et de l'Union internationale des télécommunications (UIT) qui vise à permettre au continent africain de récolter les fruits de la numérisation, en abordant les différentes dimensions de la demande et de l'offre de large bande en Afrique et en renforçant les capacités des parties prenantes africaines dans l'espace de gouvernance de l'internet.

POINTS FORTS	POINTS FAIBLES
• Des Instruments régionaux fondamentaux de gouvernance des données. • Les Communautés économiques régionales (CER) pour soutenir économiquement des initiatives de politique de données. • Des tribunaux régionaux et continentaux pour permettre une résolution harmonisée des conflits. • De nouveau pôles d'innovation dans la région pour démontrer les meilleures pratiques entre les juridictions. • Des Lois sur la concurrence, les données et la propriété intellectuelle sur les données moins nombreuses et moins développées, ce qui peut accroitre le potentiel d'harmonisation continentale rapide des lois permettant ainsi le commerce transfrontalier.	• Connectivité et utilisation des données non optimales. • Régime de gouvernance des données non harmonisé. • Incohérences dans le traitement des données en matière de protection des données, de concurrence et de propriété intellectuelle au sein des pays. • Règles de localisation qui limitent le flux transfrontalier d'informations nécessaires à la création de valeur locale et à l'établissement du marché unique. • Manque de ressources dans l'évolution et la mise en œuvre des cadres de gouvernance des données. • Infrastructure de données inadéquate. • Données publiques ouvertes insuffisantes pour répondre à la demande en matière de données. • Fourniture ou accès inadéquats à des données de qualité. • Différents niveau de développement des normes de données. • Faible pénétration de l'identification numérique. • Nombre limité d'autorités nationales de protection des données (APD) dont beaucoup ne disposent pas de ressources suffisantes et/ou de pleins pouvoirs). • Besoin de capacité de cybersécurité.

POSSIBILITÉS	RISQUES
• Si les conditions préalables sont réunies et les environnements favorables • sont créés, la création de valeur basée sur les données peut opérer à la fois dans le secteur public et privé grâce à une amélioration des flux d'informations et a une meilleure efficacité. • Utilisation des données pour améliorer la planification et la prestation de services dans le secteur public ainsi que la coordination entre les secteurs public et privé. • Avec des données ouvertes et des normes interopérables qui forment les fondations d'un système de données national intégré, les barrières à l'entrée sur le marché peuvent être réduites • et les possibilités de développement entrepreneurial et l'innovation sont améliorées. • Efforts mondiaux pour développer et harmoniser les politiques de données et les cadres de gouvernance. • Des efforts mondiaux pour coordonner la taxation des services numériques • et des services basés sur les données qui n'ont pas encore contribué aux efforts nationaux de mobilisation des ressources. • Nouvelles opportunités de travail pour les jeunes épris de technologie, afin d'améliorer l'entrepreneuriat local, le développement de contenu local et l'innovation.	• Incapacité de certains pays à surmonter les défis liés à la création • d'environnements propices nécessaires pour concrétiser les opportunités. • Manque d'harmonisation des cadres politiques et réglementaires pour favoriser les économies d'échelle et de gamme pour la création de valeur des données et pour que tous les pays bénéficient des avantages d'un marché numérique commun. • Risques en constante évolution en matière de protection des données et de confidentialité. • Risque de prise de décision automatisée discriminatoire (basée sur des algorithmes) résultant de l'invisibilité, de la sous-représentation des catégories de personnes dans les ensembles de données et des lacunes de la modélisation des algorithmes. • Concentration sur les marchés mondiaux des données, empêchant ainsi une concurrence loyale sur les marchés locaux. • Niveaux insuffisants de coopération internationale pour traiter les problèmes mondiaux en matière de données notamment en ce qui concerne : l'accès, l'intégrité, la sécurité, l'équité, les droits et l'éthique.

4.4. LES DÉFIS STRATÉGIQUES QUI SE POSENT EN MATIÈRE DE CONCRÉTISATION DES OPPORTUNITÉS ET D'ATTÉNUATION DES RISQUES

La répartition inégale des opportunités et des risques associés au développement de l'économie des données est largement corrélée aux niveaux de développement humain et économique des pays, ainsi qu'aux inégalités entre et au sein des pays. Ceux-ci se reflètent dans les points forts et les points faibles soulignés ci-dessus. La capacité des pays et des régions d'Afrique à contrer ces tendances dépend de leur **capacité à créer un environnement favorable à une valorisation des données qui soit inclusive et équitable**. L'objectif du Cadre stratégique en matière de données est de fournir un cadre permettant aux pays de surmonter certains des défis liés à la formulation de politiques dans ce domaine dynamique et en évolution rapide grâce à un objectif commun et une action collective. Grâce à la création d'un environnement harmonisé, les forces des pays peuvent être exploitées et les faiblesses atténuées en vue du développement d'une économie de données continentale intégrée bien plus puissante que ses parties individuelles.

Il ne faut pas sous-estimer les défis politiques à relever pour créer un environnement favorable à la réalisation des opportunités offertes par les processus mondialisés de numérisation et de donnéification et pour atténuer efficacement les risques identifiés pour les pays du monde entier. Ceux-ci font actuellement l'objet de plusieurs rapports d'organisations multilatérales (CNUCED 2021, Banque mondiale 2021). Si certains des défis sont liés à la création de conditions propices à une valorisation des données au niveau national, qui sont mis en évidence dans l'analyse situationnelle ci-dessus et examinés ci-après, la nature internationale et transfrontalière des données en tant que biens publics mondiaux exige plus que jamais une **coopération régionale et mondiale** pour qu'elles puissent être réalisées au niveau national et pour atténuer les risques associés qui peuvent découler de l'utilisation des données au-delà des frontières nationales. Si le cadre stratégique en matière de données fournit un cadre de haut niveau permettant aux pays d'élaborer des politiques nationales, celles-ci doivent être fondées sur des processus consultatifs nationaux qui tiennent compte du contexte local, des besoins et des dotations institutionnelles des pays.

Pour créer cet environnement favorable dans les États membres de l'Union africaine et dans la région, les considérations suivantes découlant de l'analyse de la situation et susceptibles d'avoir un impact sur la capacité des pays à répondre aux besoins d'une nouvelle économie des données sont mises en évidence.

La numérisation et la « donnéification » touchent les secteurs public et privé, l'économie formelle et informelle, ainsi que les sphères sociales et culturelles, et nécessitent un changement par rapport aux politiques sectorielles traditionnelles. La politique en faveur de l'économie du numérique et des données dont la société a besoin doit être transversale afin de coordonner les activités dans l'ensemble du secteur public et entre les secteurs public et privé pour atteindre les objectifs nationaux et régionaux. Il est en même temps important de tenir compte des **politiques sectorielles spécifiques en matière de données** afin d'optimiser et de préserver les diverses utilisations de différents types de données (par ex., les données relatives à la santé ou au climat). Au-delà de la constatation de ce principe, l'élaboration réelle des différentes politiques sectorielles qui devront être développées dépasse les attributions de ce cadre de haut niveau. **Une réglementation efficace des marchés mondialisés, de plus en plus complexes, est essentielle** pour que la dorsale omniprésente et les services continus nécessaires au déploiement des services et applications de données puissent répondre aux divers besoins économiques et sociaux, améliorer la concurrence et favoriser l'innovation africaine. Comme dans tous

les pays du monde, les décideurs politiques devront revoir et renouveler les arrangements institutionnels pour la gouvernance de l'économie des données. Des régulateurs spécialisés, tels que les régulateurs des données ou de l'information, sont nécessaires pour traiter les nouvelles questions de gouvernance des données, et les régulateurs nouveaux comme ceux déjà établis devront s'engager dans des niveaux élevés de coordination nationale et régionale. Pour que le marché unique africain devienne opérationnel, l'harmonisation réglementaire est également essentielle à l'intégration des marchés, de même que des systèmes communs de paiement électronique, la facilitation du commerce transfrontalier et la normalisation de la fiscalité et des droits transfrontaliers. Les États africains devront se regrouper et élaborer des positions communes pour obtenir des résultats plus favorables dans les forums de gouvernance mondiale afin de mieux servir les intérêts africains.

Une politique numérique et de données transversales peut gérer l'interaction importante entre la concurrence, le commerce et la fiscalité dans une économie de données. Les États africains ont ainsi l'occasion de coordonner leurs politiques sectorielles afin de soutenir une économie des données florissante. Pour de nombreux pays africains, un risque qui doit être atténué dès le début est la tendance à la concentration du marché et à la création de richesses inégales en raison des effets de réseau indirects associés aux économies d'échelle et d'envergure. Les marchés numériques axés sur les données sont enclins aux résultats de type « les gagnants emportent tout ». Entre autres facteurs, l'hyper mondialisation et l'interdépendance numérique contribuent à la monopolisation. Cette situation affecte finalement la concurrence locale et entrave la compétitivité mondiale des écosystèmes de données nationaux. Les défis posés par la concentration des marchés, l'interdépendance numérique et la répartition inégale des richesses, notamment en raison de l'érosion des bases et du transfert des bénéfices, ouvrent la voie à des mesures incitatives qui encouragent une plus grande intégration entre les priorités mutuelles renforçant les stratégies politiques habituellement cloisonnées en matière de concurrence, de commerce et de fiscalité. En raison de l'importance croissante de la gouvernance régionale et mondiale, les communautés économiques régionales ont un rôle important à jouer pour la mise en œuvre de la politique régionale en matière de données, par le biais de lois types et en soutenant le renforcement des capacités institutionnelles et humaines.

SMART AFRICA - IDENTITÉ NUMÉRIQUE

En 2020, le Bénin a défendu un projet phare de Smart Africa visant à élaborer le plan directeur pour l'identité numérique qui a été adopté par le conseil d'administration de Smart Arica, composé de ses 32 États membres, de l'UA et de l'UIT, avec le soutien de plusieurs autres organisations multilatérales et de donateurs. Le plan directeur propose SATA comme plateforme pour faciliter la reconnaissance fiable des identités numériques entre une série d'acteurs par le biais de mécanismes de certification fédérés. Des projets pilotes de SATA devraient être mis en œuvre au Bénin, au Rwanda, en Tunisie et dans d'autres États membres de Smart Africa. SATA servira de solution souple et adaptable pour permettre l'interopérabilité entre divers systèmes d'identité publics et privés sur le continent.

Compte tenu du contexte africain spécifique et de la lenteur des efforts d'harmonisation, l'approche fédérée de SATA devrait permettre la reconnaissance unilatérale de cadres juridiques adéquats par les États africains, avec le soutien d'une autorité de certification centrale et fiable. À cette fin, les États doivent renforcer leurs capacités d'application, en particulier les capacités des autorités de protection des données dans le contrôle et l'approbation des transferts transfrontaliers de données. Le cadre proposé englobera les technologies de pointe et sera respectueux des législations et réglementations des pays. Les gouvernements ne devraient pas être obligés d'utiliser des technologies spécifiques. L'utilisation de normes et de standards ouverts devrait garantir une grande diversité de choix technologiques pour les États.

Dans le contexte de l'écosystème africain des données, **l'alignement des objectifs de politique publique concernant la fiscalité et la politique des données, en particulier dans le contexte de l'activation du marché numérique unique, a été un défi politique majeur**. Les récentes mesures législatives et politiques introduites par certains pays africains, dans le contexte de plusieurs efforts multilatéraux et unilatéraux visant à taxer l'économie numérique, peuvent ne pas être propices à la création d'un marché unique ou à l'accès aux ressources internationales pour réaliser les biens publics mondiaux et remplir certaines des conditions préalables à une économie de données compétitive sur le continent. En coordonnant les positions africaines sur les réformes en cours du régime fiscal international, qui s'attaque aux défis de la taxation des services numériques et des services de données sans présence physique dans les pays dont ils génèrent des revenus. L'exploitation de nouvelles sources de recettes fiscales pourrait permettre aux pays africains de supprimer les droits d'accises sur les réseaux sociaux et les services de données, ce qui réduirait les distorsions tant sur le marché local que dans le système fiscal mondial. L'harmonisation du régime fiscal pour les biens et services numériques au niveau régional et son alignement au niveau mondial atténueraient les risques liés à la difficulté des petites économies de données de générer une valeur significative et d'être compétitives sur les marchés mondiaux pour contribuer à l'échelle et à la portée nécessaires à la création de valeur axée sur les données et à des bases fiscales globalement limitées.

La clarté et la sécurité juridiques à cet égard sont particulièrement importantes pour mettre en place une transformation numérique fiable et durable. Un défi mondial réside dans le fait que la nature des flux de données et de l'infrastructure numérique menace la souveraineté nationale en matière de données. Pour exercer un contrôle sur les données afin de sauvegarder la souveraineté, il faut à la fois des infrastructures et des lois, mais aussi la capacité technique de le faire d'une manière qui permette d'instaurer la confiance. Les politiques transversales permettent d'obtenir des certitudes sur des questions telles que la propriété ou la garde des données et les droits qui y sont associés, tout en établissant un système complet de contrôle de l'accès et de l'acquisition, ainsi que de l'analyse, du stockage et de la diffusion des données personnelles et non personnelles. Garantir la protection des consommateurs tout en permettant l'innovation est également essentiel au développement économique et à l'inclusion. En outre, étant donné que les différentes approches juridiques sectorielles servent des intérêts différents, les pays ont la possibilité de réinventer un système juridique harmonisé qui équilibre de manière adéquate les intérêts des entreprises et les droits numériques pertinents.

La création de systèmes de données nationaux intégrés et interopérables en réponse aux défis émergents améliore l'efficacité et permet une plus grande transparence et responsabilité. Un défi commun à tous les pays est que lorsque **les données sont de mauvaise qualité ou ne sont pas interopérables**, cela limite la capacité des entreprises et du secteur public à s'engager dans le partage et l'analyse qui peuvent apporter une valeur économique et sociale aux données. Des voies d'accès insuffisantes et un engagement limité en faveur de l'ouverture des données publiques, entre autres, font également obstacle à un environnement propice à une économie des données solide. La fourniture de données de qualité nécessite de créer une demande de données dans tous les sites institutionnels (c'est-à-dire le secteur public, les institutions et les entreprises, etc.). L'extraction de la valeur des données nécessite non seulement un contrôle, mais aussi le développement de capacités analytiques et techniques dans les secteurs public, privé et autres.

Bien que plusieurs pays aient introduit des systèmes d'identification numérique, **l'omniprésence et l'interopérabilité de ces systèmes restent un défi social et économique majeur sur le continent**. Les systèmes d'identification numérique permettent l'identification dans le but d'effectuer des transactions et d'interagir dans un écosystème de données de con-

fiance. L'identification fondamentale et fonctionnelle facilite les services numériques, mais la couverture complète de l'identité fondamentale, en particulier, reste un défi à la fois social et économique. Les cadres régionaux émergents sur l'identité numérique commencent à se pencher directement sur cette question. Il est possible d'intégrer l'identité fonctionnelle décentralisée dans les cadres de protection des données. Ceux-ci peuvent fournir une identité fonctionnelle tout en réduisant les risques associés aux données personnelles.

Un autre grand défi à relever en la matière est le manque d'homogénéité des données économiques et sociales, et notamment des indicateurs numériques, dans de nombreux pays, afin d'étayer la formulation de politiques fondées sur des données probantes et de fournir une image précise aux bases de données publiques mondiales telles que celles du système statistique des Nations unies. La valeur stratégique des données étant reconnue, la priorité doit être accordée à la collecte et au stockage de données de qualité afin de réaliser la valeur publique et de réduire les asymétries d'information et de pouvoir existantes au sein du secteur public, entre le secteur public et le secteur privé, et entre les secteurs public et privé et les citoyens et consommateurs.

Les pays africains sont confrontés à plusieurs défis bien documentés et interdépendants en ce qui concerne leur niveau de préparation à l'ère numérique. Il s'agit notamment des défis liés à l'élaboration en vase clos des politiques et de la législation, à l'harmonisation régionale des politiques, au manque de capacités réglementaires et administratives, à l'absence de concurrence entre les prestataires de services dans de nombreux pays, à la couverture et la qualité de la connectivité Internet, et à l'accessibilité financière, qui est liée à la fois au coût élevé des appareils numériques et au coût des données (Gillwald & Mothobi, 2019 ; Hawthorne, 2020).

En dépit de l'adoption de chartes continentales, de conventions et de lois types des communautés économiques régionales visant à harmoniser **la réponse de l'Afrique aux défis posés par la numérisation et l'intégration des données, leur ratification et leur mise en œuvre ont été variables**. Une adoption plus large des fondements numériques des initiatives continentales, telles que la ZLECAf, sera essentielle pour obtenir les avantages d'une plus grande coopération économique. La normalisation des règles relatives aux flux transfrontaliers est une condition préalable à la concrétisation des avantages attendus de la ZLECAf. Cela peut se faire en utilisant l'opérationnalisation de l'accord pour faciliter une meilleure interopérabilité transfrontalière des données et fournir une approche continentale harmonisée de l'économie numérique fondée sur les données. Ceci d'une manière qui soutienne les avantages socio-économiques du commerce numérique et du commerce électronique, tout en garantissant que les informations sensibles restent sécurisées et que les réglementations pertinentes sur la protection des données à caractère personnel sont respectées.

En réponse aux précédentes vagues d'innovation technologique, économique, réglementaire et sociale, **les pays africains ont eu tendance à suivre les normes plutôt qu'à les créer**. Les organisations multilatérales, allant de l'OCDE à l'Organisation mondiale de la propriété intellectuelle et à l'Organisation mondiale du commerce, réagissent aux défis de la gouvernance mondiale des données. Bien que l'Afrique et les pays africains n'aient pas, à quelques exceptions près, joué un rôle moteur dans les politiques numériques mondiales, il est possible de changer cette situation. Les pressions commerciales multilatérales, plurilatérales et bilatérales visant à permettre la circulation des données avec peu de restrictions s'accompagnent de pressions pour concéder des droits de propriété intellectuelle sur les données, de sorte que les pays africains sont confrontés à la perspective d'une exploitation et d'une appropriation des données. En l'absence d'une politique commune et d'un engagement en faveur de normes communes sur tout le continent, il est difficile pour la plupart des pays africains d'échapper aux courants

de la dynamique mondiale en évolution rapide. Par conséquent, une action coordonnée par et pour l'Afrique est nécessaire pour libérer collectivement l'énorme potentiel de transformation des données afin de développer une économie numérique et une société moderne inclusive et durable en Afrique.

EXEMPLES D'INNOVATION DANS LES COMMUNAUTÉS DE DONNÉES

Les exemples typiquement cités de succès dans l'innovation en matière de données ouvertes sont l'émergence de pôles d'innovation particuliers dans la région, principalement dans les zones urbaines. Les pôles d'innovation, comme préconisé ailleurs, peuvent certainement être un site pour les succès sociaux et économiques des données ouvertes ; pourtant, il existe des exemples d'innovation en matière de données ouvertes qui peuvent se produire de manière plus organique simplement par la mise à disposition de données publiques ouvertes de qualité. Ces innovations peuvent être motivées par les besoins de secteurs spécifiques. Ainsi, dans le domaine de l'agriculture, iCow est une application lancée par un entrepreneur kenyan qui a permis d'améliorer de 100 % le rendement obtenu sur l'élevage bovin pour les agriculteurs individuels. D'autres innovations dans le domaine de l'agriculture, impliquant de manière plus centrale les données ouvertes, comprennent, au Ghana, Farmerline et Esoko. Des entreprises innovantes peuvent naître des données ouvertes, comme les exemples d'OpenUp (Cape Town) et d'Open Cities Lab (Durban) en Afrique du Sud, qui sont des entreprises à vocation sociale, toutes deux fondées sur les données ouvertes. Ushahidi est une organisation (et une société de logiciels en tant que service) articulée autour d'une plateforme de source ouverte, qui intègre des données ouvertes provenant de la foule et les cartographies, et qui a été utilisée avec un effet social et de gouvernance incroyable dans la surveillance des élections et la réponse aux crises dans toute la région. Les données ouvertes peuvent permettre de réaliser des économies directes sur les coûts publics grâce aux innovations qui émergent des initiatives en matière de données, créant ainsi un cercle vertueux : dans le cadre d'un partenariat précoce entre OpenUp (alors Code for South Africa) et le Programme d'Afrique australe pour l'accès aux médicaments et aux diagnostics, un outil développé à partir de données ouvertes sur les prix des médicaments a démontré au gouvernement namibien les différences de prix qu'il recevait pour le médicament Nifedipine, ce qui, après renégociation, lui a permis de réaliser une économie directe d'un milliard de dollars américains par an.

5. CADRE STRATÉGIQUE EN MATIÈRE DE DONNÉES

Les données sont de plus en plus reconnues comme un atout stratégique, faisant partie intégrante de l'élaboration des politiques, de l'innovation et de la gestion des performances dans les secteurs privé et public, et créant de nouvelles opportunités entrepreneuriales pour les entreprises et les particuliers. Lorsqu'elles sont appliquées aux services publics, les technologies émergentes peuvent générer des quantités massives de données numériques et contribuer de manière significative au progrès social et à la croissance économique. Le rôle central des données exige une perspective politique stratégique de haut niveau, qui soit capable de concilier des objectifs politiques multiples. Pour libérer le potentiel économique et social des données tout en protégeant efficacement la vie privée, la propriété intellectuelle et d'autres objectifs politiques, les stratégies nationales en matière de données doivent être formulées dans le contexte du renforcement de l'interopérabilité internationale.

L'élaboration d'un Cadre stratégique continental en matière de données est nécessaire pour concrétiser la vision partagée et l'approche commune d'un écosystème de données africain intégré. Cet écosystème de données devrait soutenir la mise en place d'un marché unique numérique africain (MUN), favoriser le commerce numérique intra-africain et stimuler le développement d'un entrepreneuriat et d'entreprises inclusifs axés sur les données. C'est ce qu'envisagent la stratégie de transformation numérique de l'UA (STN) et les prochaines négociations de la phase II et de la phase III de la ZLECAf, où des lignes directrices sur le commerce des services et le protocole sur le commerce électronique devraient être établies.

Le Cadre fournit des orientations de haut niveau fondées sur des principes aux États membres pour les aider à élaborer une politique en matière de données adaptée à leur situation. Il recense les principes clés d'une gouvernance efficace des données et les stratégies à mettre en œuvre aux niveaux national, continental et international. Cela inclut des orientations sur les procédures et garanties institutionnelles, administratives et techniques appropriées qui doivent être mises en œuvre. L'objectif est de s'assurer que les écosystèmes de données nationaux et sous-régionaux sont construits sur une infrastructure et des processus numériques fiables et interopérables qui fassent progresser un système de données continental harmonisé permettant d'assurer une croissance économique et un développement équitables et durables pour tous les peuples d'Afrique.

Le Cadre réaffirme l'importance de l'engagement de l'UA en faveur de cadres réglementaires stables, harmonisés et prévisibles et de politiques adaptées au contexte pour favoriser :

- des incitations à investir efficacement dans les infrastructures de données numériques fondamentales et les systèmes numériques fondamentaux ;
- des dispositions institutionnelles favorisant l'interaction optimale entre l'État, les marchés et les institutions de régulation pour permettre la création de valeur publique et privée ;
- le renforcement des capacités numériques humaines et institutionnelles ;
- la création de valeur à partir d'une utilisation responsable des données, la promotion d'une croissance équitable durable et le renforcement de la prospérité commune grâce à l'économie des données ;
- une meilleure répartition des possibilités tant pour l'utilisation des services de données que pour la création de valeur axée sur les données au sein des pays et entre eux ; et

- des environnements efficacement réglementés qui favorisent une concurrence équitable et une allocation des ressources efficace qui produisent des résultats positifs pour le bien-être des consommateurs.

5.1. PRINCIPES DIRECTEURS DU CADRE

Le Cadre stratégique en matière de données doit s'aligner sur les valeurs de l'UA et le droit international afin de parvenir à une plus grande unité et solidarité entre les pays africains et leurs populations, en assurant un développement économique équilibré et inclusif, y compris la promotion et la protection des droits des peuples à travers la Charte africaine des droits de l'homme et des peuples et d'autres instruments pertinents.

Dans l'esprit de favoriser la prospérité régionale, la croissance économique et le développement, le progrès social et de coordonner les efforts continentaux, les principes de haut niveau suivants guident le cadre.

Coopération : les États membres de l'Union africaine coopèrent en matière d'échange de données, reconnaissant les données comme un apport central de l'économie mondiale et l'importance de l'interopérabilité des systèmes de données pour un marché unique numérique africain florissant ;

Intégration : Le cadre favorise les flux de données intra-africains, supprime les obstacles juridiques à la circulation des données, en tenant compte uniquement de la sécurité, des droits de l'homme et de la protection des données nécessaires ;

Équité et inclusivité : les États membres doivent veiller à ce que le cadre, dans sa mise en œuvre, soit inclusif et équitable, qu'il offre des opportunités et des avantages à tous les Africains et, ce faisant, qu'il cherche à redresser les inégalités nationales et mondiales en tenant compte des voix de ceux qui sont marginalisés par les développements technologiques ;

Confiance, sécurité et responsabilité : les États membres encouragent la mise en place d'environnements de données fiables, sûrs et sécurisés, responsables vis-à-vis des personnes concernées, et conformes à l'éthique et à la sécurité dès la conception ;

Souveraineté : les États membres, la CUA, les CER, les institutions africaines et les organisations internationales coopèrent pour créer des capacités permettant aux pays africains de gérer eux-mêmes leurs données, de tirer parti des flux de données et de gérer les données de manière appropriée ;

Complet et tourné vers l'avenir : le cadre permet la création d'un environnement qui encourage l'investissement et l'innovation par le développement des infrastructures, des capacités humaines et l'harmonisation des réglementations et de la législation ;

Intégrité et justice : les États membres veillent à ce que la collecte, le traitement et l'utilisation des données soient justes et légaux, et à ce que les données ne soient pas utilisées pour exercer une discrimination injuste ou porter atteinte aux droits des personnes.

5.2 DÉFINITION ET CATÉGORISATION DES DONNÉES

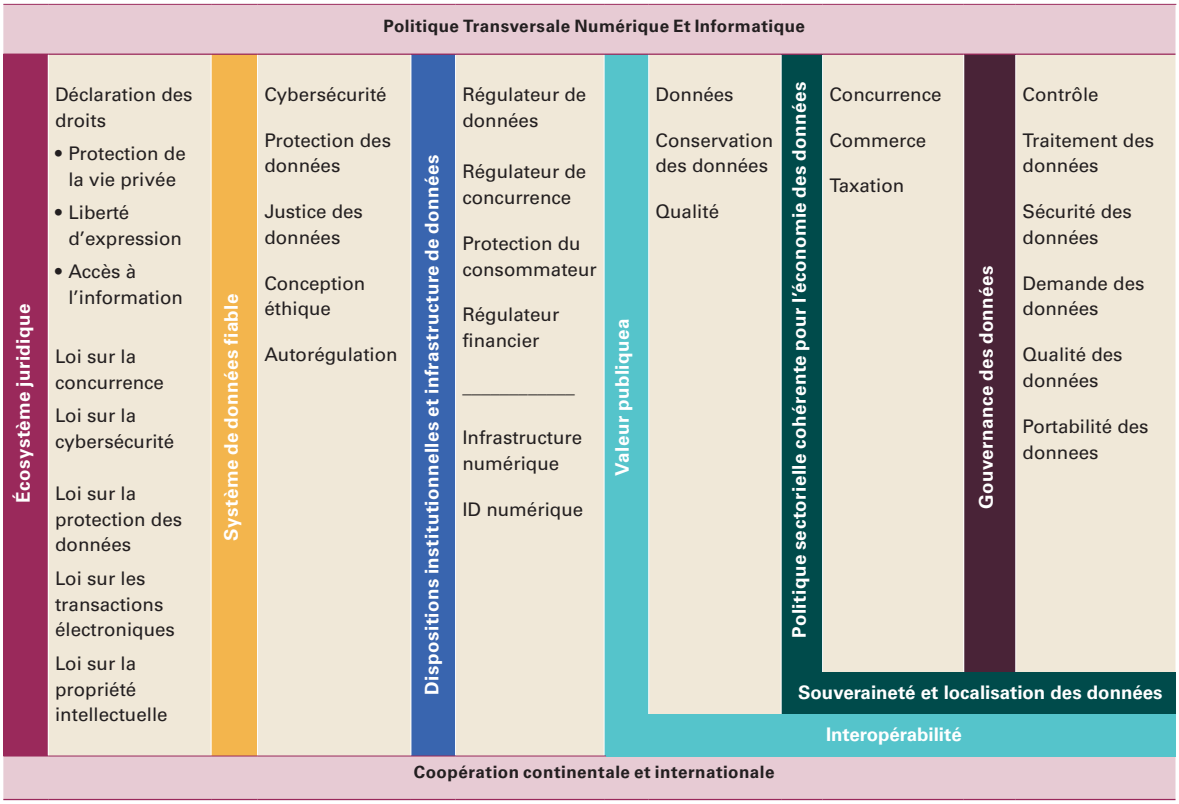
Il n'existe pas d'accord sur la définition des données, probablement en raison des très nombreux types de données qui sont collectés et utilisés, et de leurs objectifs et valeurs variables. Si les gouvernements ne reconnaissent pas ces différents types de données et les divers rôles qu'elles peuvent jouer, ils ne seront pas en mesure d'aborder efficacement des questions telles que la protection des données à caractère personnel ou la concurrence. Une meilleure mesure des données et des flux de données, ainsi que de leur rôle dans les chaînes de production et de valeur, contribuera également à soutenir l'élaboration des politiques.

5.2.1 DONNÉES À CARACTÈRE PERSONNEL ET NON PERSONNEL

Bien que les données, d'un point de vue conceptuel, aient des significations différentes selon les communautés et le contexte, un concept important, qui est au cœur du règlement sur la protection des données, est celui des données à caractère personnel. Le fait de définir des types spécifiques de données comme étant personnelles peut aider les organismes chargées de la protection des données à protéger plus efficacement les droits des sujets de données mais cette approche a ses limites.

Il existe de nombreuses façons de catégoriser les données qui affectent la politique et la réglementation de chaque catégorie, parmi les dimensions les plus importantes figurent l'intention publique ou privée et les méthodes de collecte traditionnelles ou nouvelles (CNUCED, 2021 ; Banque mondiale, 2021).

Cadre Réglementaire Favorable



Lorsque les organismes chargés de la protection des données commenceront à mettre en œuvre la législation sur la protection des données à caractère personnel, elles devront fournir à l'industrie des définitions claires sur la manière de différencier les données à caractère personnel et non personnel, afin de permettre la collecte, le stockage et le traitement des données par des entreprises conformes à la réglementation sur la protection des données. Cela permettra également de réduire le risque de non-conformité lors de la collecte, du stockage et du traitement des données. Il est important que les politiques et les réglementations en matière de données partagent les mêmes catégories de données afin de garantir la cohésion des politiques et de permettre la conformité.

5.3 FACTEURS PERMETTANT DE CRÉER DE LA VALEUR DANS L'ÉCONOMIE DES DONNÉES

Pour tirer profit des données, il est indispensable de mettre en place des cadres réglementaires et politiques qui facilitent l'obtention de données utiles, d'améliorer les capacités humaines, institutionnelles et techniques pour créer de la valeur à partir des données, d'encourager le partage des données et l'interopérabilité, et d'accroître la légitimité et la confiance du public à l'égard de l'État pour gérer les données des citoyens de manière responsable. En outre, l'infrastructure de données qui permet la mise en place d'un système de données intégré est un atout stratégique essentiel pour les pays. L'environnement créé par l'interaction des éléments de l'écosystème de données et la nature des relations et des processus non linéaires entre eux et en leur sein, déterminent les interventions visant à créer des incitations aux investissements technologiques qui sont nécessaires pour stimuler la croissance de l'économie des données. Ces conditions sont façonnées par la structure du marché, la compétitivité des services qui en découlent et l'efficacité de la régulation du marché.

L'économie numérique imprègne diverses industries et activités sociales, et la politique en matière de données doit être située dans le contexte de l'écosystème numérique complexe et adaptatif plus large. Comme nous l'avons vu, cela a des implications pour d'autres domaines politiques, notamment le commerce, les échanges et la fiscalité. Les États devraient investir dans des capacités de données et des actifs complémentaires pour soutenir l'élaboration des politiques. Les investissements dans l'innovation et la recherche et développement (R&D) liées aux données, ainsi que dans les capacités d'harmonisation des normes, des compétences et des infrastructures, peuvent permettre aux gouvernements d'élaborer de meilleures politiques liées aux données dans tous les domaines. Les questions de confiance et d'éthique sont tout aussi importantes, tandis que les réglementations fondées sur les faits et la consultation doivent être privilégiées.

RECOMMANDATIONS

- Les États membres de l'Union africaine devraient promouvoir la recherche, le développement et l'innovation dans divers domaines liés aux données, notamment l'analyse des données massives, l'intelligence artificielle, l'informatique quantique et la technologie blockchain.
- Tous les groupes de parties prenantes, y compris les gouvernements, devraient renforcer leurs capacités d'analyse et de gestion des données afin de faciliter l'utilisation de données de qualité et de systèmes interopérables fiables. Cependant, il est important de se rappeler que dans de nombreux pays, le plus grand producteur et collecteur commun de données est l'État. Par conséquent, bon nombre des observations incluses dans la discussion sur la gouvernance des données ci-dessous ont une incidence particulière sur les actions des gouvernements.

5.3.1 INFRASTRUCTURE DE DONNÉES FONDAMENTALE

5.3.1.1 ACCÈS ET UTILISATION DU HAUT DÉBIT ET DES DONNÉES

Définition des problématiques.

Il existe des obstacles à l'accès aux infrastructures à large bande qui empêchent les personnes de rejoindre l'économie des données, même en tant qu'utilisateurs. Selon le rapport de la Commission de l'UIT « Connecting Africa Through Broadband »":[5] « Près de 1,1 milliard de nouveaux utilisateurs uniques doivent être connectés pour parvenir à un accès Internet à haut débit universel, abordable et de bonne qualité d'ici 2030, et on estime que 100 milliards de dollars supplémentaires seraient nécessaires pour atteindre cet objectif au cours de la prochaine décennie. »

En dépit de cela, et d'une myriade de contraintes contextuelles, l'Afrique a une position avantageuse pour développer un écosystème de données innovant, étant moins entravée par les infrastructures de données existantes, et ayant une utilisation du spectre et des niveaux de congestion relativement plus faibles. Alors que la pénétration du haut débit fixe dans la région est inférieure à un pour cent, l'internet mobile est plus omniprésent et son coût d'adoption est plus faible[6]. Par conséquent, l'évolution de l'écosystème des données en Afrique sera principalement rendue possible par les réseaux mobiles à large bande.

RECOMMANDATION

Pour accélérer l'internalisation du cadre, il convient de mettre en place une infrastructure numérique robuste et massive dans tous les pays membres de l'UA, ainsi que les capacités suffisantes. Les États membres devraient donner la priorité à l'obtention d'une connectivité significative et d'un accès Internet abordable, afin d'intégrer davantage d'utilisateurs et de stimuler la demande de services d'infrastructure. Pour une adoption et une utilisation plus efficaces des données dans la région, il convient de remédier aux déficits d'infrastructures complémentaires qui limitent l'utilité des données.

→ ACTIONS

Les États membres devront faire évoluer les politiques qui :

- proscrivent les frais prohibitifs de « droit de passage » des câbles à large bande et soutiennent le partage des infrastructures ;
- préviennent les pratiques anticoncurrentielles découlant d'une domination sur les marchés des infrastructures ;
- investissent dans le Wi-Fi public et les technologies complémentaires ;
- adoptent des techniques innovantes d'utilisation du spectre, telles que l'attribution et l'accès dynamiques au spectre, et l'exploitation du dividende numérique (bandes de spectre accélérées par la migration de la radiodiffusion analogique vers le numérique) pour étendre l'accès au haut débit pour les zones rurales mal desservies ;
- promeuvent la transition et l'adoption de l'IPv6[7], à mesure que les ressources de l'IPv4 s'épuisent au niveau mondial ;

5 *https://broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf*
6 Département des données et des statistiques sur les TIC, Bureau de développement des télécommunications, "Faits et chiffres sur les TIC pour 2016", Union internationale des télécommunications, Genève, Rapport, 2016.
7 Le protocole Internet version 6 est la version la plus récente du protocole Internet qui fournit un système d'identification et de localisation des appareils sur les réseaux et achemine le trafic sur Internet.

- investissent dans des infrastructures nationales de dorsale et de connectivité transfrontalière, telles que les points d'interconnexion Internet (IXP), aux niveaux national et régional, afin de tirer parti de la bande passante internationale disponible, de réduire le coût d'accès à Internet et d'améliorer les vitesses d'accès aux données dans la région ;
- tirent parti de modèles innovants pour le financement des infrastructures de données.

5.3.1.2 INFRASTRUCTURE DES DONNÉES

Définition des problématiques

L'infrastructure de données fondamentale qui facilite les systèmes de données et permet le partage, la collecte et le stockage de données volumineuses ou la manipulation des sources de données existantes aura un impact sur la façon dont les gouvernements répondront aux défis liés à la disponibilité, à la qualité et à l'interopérabilité des données et aborderont les considérations liées à la légitimité et à la confiance du public.

L'infrastructure de données fondamentale fait référence à un large éventail de technologies qui facilitent l'utilisation intensive de données de qualité, y compris l'infrastructure matérielle et immatérielle[8] qui doit combler les déficits actuels de l'infrastructure TIC « traditionnelle » en parallèle à la création d'une architecture destinée à soutenir l'intensification de la donnéification. Cela inclut également des ressources d'infrastructure telles que l'identification numérique pour permettre des transactions et une présence en ligne sécurisées. Le présent cadre se concentre sur trois aspects de l'infrastructure des données qui nécessitent des considérations politiques se renforçant mutuellement et qui influencent également la gouvernance des données : les services en nuage, le big data et la plateformisation.

Le développement de la valeur des données publiques à partir de l'infrastructure informatique en nuage et des logiciels qui complètent le traitement et l'analyse des big data devra s'appuyer sur des modèles de sécurité et de confiance bien développés pour le stockage et le traitement en nuage des données sensibles ou exclusives, pour la gestion des API et pour le soutien des marchés équitables des écosystèmes de données. Au-delà des insuffisances de l'infrastructure numérique dans de nombreux gouvernements - y compris les faibles facilitateurs pour accueillir un environnement pour l'offre et la consommation de services en nuage - les pays africains sont confrontés à une multitude de défis pour répondre aux besoins d'infrastructure, car cette infrastructure est souvent fournie par et achetée auprès de fournisseurs de services privés étrangers.

Cela implique que pour tirer parti des opportunités associées à la transformation numérique, d'autres enjeux tels que les responsabilités des intermédiaires, les frontières juridictionnelles, l'interopérabilité et les questions de souveraineté, pour n'en citer que quelques-uns, devront être pris en compte. Ces enjeux soulignent la nécessité d'une collaboration et de partenariats dans de nombreux écosystèmes de données africains afin de renforcer les catalyseurs fondamentaux de marchés d'activités performants basés sur les données à différents points de la chaîne de valeur des données, indépendamment de la maturité et des dotations numériques nationales.

Les réglementations et législations en vigueur sur les plans technologique, organisationnel, juridique et commercial auront une incidence sur l'efficacité de l'infrastructure partagée qui facilitera l'accès des différents acteurs du marché des données. Les écosystèmes de données

8 Voir Annexe pour une définition plus complète.

devraient pouvoir soutenir divers domaines d'application et permettre l'échange et l'intégration de données aux différentes étapes du cycle de valeur des données, tout en préservant la provenance et l'intégrité des données.

SERVICES EN NUAGE

Il est utile, à des fins politiques, de faire la distinction entre « services en nuage » et « services basés sur le nuage ». Le principal avantage offert par les services en nuage est la réduction des coûts grâce à une meilleure efficacité des systèmes. Par exemple, les petites, moyennes et micro-entreprises (PMME) et le secteur public, dont les ressources sont limitées, peuvent réduire les dépenses d'investissement dans les équipements informatiques, notamment les serveurs internes, les équipements de réseau, les ressources de stockage et les logiciels, en adoptant un modèle de services en nuage basé sur les services publics.

L'interopérabilité de la fourniture de services en nuage est un facteur essentiel, car elle offre une certaine souplesse et permet aux utilisateurs de passer d'un fournisseur de services en nuage à un autre. Parmi les autres avantages de l'informatique en nuage, citons la réduction des dépenses liées à la consommation d'énergie ainsi que la diminution de la demande de gestion et de maintenance des systèmes en confiant la gestion des ressources informatiques à des tiers. En conséquence, les fonds peuvent être réaffectés à des activités orientées vers les clients et à une meilleure prestation des services publics. Toutefois, comme certains facteurs favorisent un environnement propice aux services en nuage, il faut prendre des dispositions pour adopter les nouvelles technologies tout en s'attaquant aux problèmes structurels de la fracture numérique (capital humain, infrastructure, etc.). Ces processus doivent se renforcer mutuellement et être adaptés aux réalités économiques des États membres. Le développement de la valeur des données grâce à l'infrastructure informatique en nuage et aux logiciels qui complètent le traitement et l'analyse des big data devra être fondé sur des modèles de sécurité et de confiance bien développés pour le stockage en nuage et le traitement des données sensibles/propriétaires, la gestion des API, et pour soutenir des marchés de données équitables.

BIG DATA

Des quantités massives de données sont produites - y compris en tant que sous-produits d'autres activités (comme par les plateformes de réseaux sociaux lorsqu'elles créent des profils de leurs utilisateurs pour les annonceurs) - et utilisées pour le développement de produits, de services et de formes d'entreprises entièrement nouvelles, avec le potentiel de générer des gains d'efficacité et de productivité substantiels. Cela présente également un potentiel pour le secteur public, qui dispose de grandes quantités de données qui pourraient être utilisées pour l'analyse des big data en améliorant la prise de décision, les prévisions et en permettant une meilleure segmentation et un meilleur ciblage des consommateurs. Les avantages d'échelle et de portée liés aux effets de réseau ont donné lieu à des positions de quasi-monopole, qui ont encore été renforcées par les fusions de nouveaux fournisseurs de services plus petits qui, à première vue, ne semblent pas être sur le même marché, comme Facebook et WhatsApp. Il est ainsi quasiment impossible pour les acteurs locaux de faire face à la concurrence (Arntz et al., 2016).

PLATEFORMISATION

L'informatisation des données a également donné naissance à des modèles commerciaux et des modes de création et d'extraction de valeur entièrement nouveaux. L'un d'entre eux est la « plateformisation », qui facilite les transactions et la mise en réseau ainsi que l'échange d'informations, en regroupant plusieurs vendeurs et acheteurs sur une seule plateforme.

Le commerce numérique et les plateformes de commerce électronique étant de plus en plus à la base de l'activité mondiale et transfrontalière, l'intégration de domaines traditionnellement distincts de la réglementation et des priorités politiques est devenue de plus en plus importante et entrelacée au-delà des frontières géographiques. Toutefois, des politiques telles que la localisation des données ne seront pas plausibles sans les exigences structurelles et institutionnelles nécessaires à leur évolution et à leur mise en œuvre efficaces, en particulier en ce qui concerne les capacités numériques (Andreoni & Tregenna, 2020).

RECOMMANDATIONS

- L'utilisation des données comme outil de promotion des intérêts publics exigera des États qu'ils renforcent leurs infrastructures de données nationales et nécessitera un engagement solide des parties prenantes aux niveaux national, régional et mondial. L'élaboration de cadres politiques complets pour les données devrait s'accompagner de stratégies de mise en œuvre dans les délais impartis pour les différents mandats nationaux afin de garantir la responsabilité et la transparence.
- Les États membres devraient hiérarchiser les ressources afin de s'assurer qu'il existe des incitations à accroître les investissements dans l'infrastructure numérique, les plateformes de données et les capacités logicielles pour exploiter le big data. Les investissements dans les infrastructures de données doivent soutenir le contrat social numérique. Les efforts des États pour améliorer l'interopérabilité, la qualité et l'administration publique des données doivent également compléter et améliorer les systèmes numériques publics tels que les identifications numériques, les paiements numériques et les flux de données ouvertes, dans la mesure du possible. L'infrastructure appropriée est également une condition indispensable à tout système de partage de données interopérable et intégré. En outre, la réutilisation des données nécessite généralement des systèmes de données performants qui facilitent la circulation des données dans des formats lisibles par les machines permettant leur utilisation par un grand nombre.

→ ACTIONS

- Au lieu de se concentrer sur un investissement initial important pour remplacer les équipements TIC hérités qui se déprécient, les États membres devraient tirer parti des économies d'échelle et de gamme pour adopter des infrastructures qui soutiennent les avantages facilitateurs offerts par les services en nuage et d'autres nouvelles technologies qui soutiennent la création de valeur des données.
- Les politiques fiscales, commerciales (y compris en matière d'investissement et d'innovation) et de concurrence doivent être cohérentes, complémentaires et adaptées à l'économie numérique axée sur les données, notamment pour informer les stratégies de développement des infrastructures.
- Les États membres doivent veiller à ce que les entreprises locales participent aux chaînes de valeur des fournisseurs étrangers de logiciels en tant que service (SaaS), d'infrastructures en tant que service (IaaS) et de plateformes en tant que service (PaaS) pour les marchés publics et créer des incitations pour avoir des PMI locales dans les

chaînes de valeur des données au sein des industries. Cela peut se faire en veillant à ce que les politiques fiscales, commerciales (y compris l'investissement et l'innovation) et de concurrence soient cohérentes, complémentaires et adaptées à l'économie numérique axée sur les données.

- Adopter des modèles de production d'électricité plus durables, au niveau national et dans toute la région, afin de garantir que l'infrastructure numérique fondamentale soutienne des activités de données nationales et transfrontalières durables ayant moins d'impacts extractifs sur l'environnement naturel.

GOUVERNANCE DES DONNÉES

- Créer des droits de portabilité des données - y compris pour les données non personnelles, afin que les clients des services en nuage puissent plus facilement changer de fournisseur.
- Développer des normes contractuelles pour les organisations publiques (qui peuvent être utilisées par les PME également), qui protègent leurs droits d'accès, de récupération, de suppression, etc. des données (y compris les données non personnelles, encore une fois) qui sont traitées par les fournisseurs de cloud computing.
- Développer des obligations de licences équitables, raisonnables et non discriminatoires (FRAND) pour les plateformes et les fournisseurs de cloud computing qui ont accès à des ensembles de données qui deviennent une ressource vitale pour entrer sur un marché.

5.3.1.3 ID NUMÉRIQUE

Définition des problématiques

Alors que le continent africain abrite le plus fort pourcentage de personnes sans identité légale, qui ne peuvent donc pas être enregistrées à l'état civil et se voient refuser les services sociaux essentiels offerts par les États, tels que les soins de santé, l'éducation de base ou les services alimentaires[9], l'économie numérique offre des possibilités de corriger les inégalités telles que les exclusions socio-économiques et structurelles dont souffrent les groupes minoritaires sur le continent.

L'identité numérique en tant que forme d'expression des données personnelles, doit être construite et mise en œuvre de manière cohérente, conformément aux cadres généraux de gouvernance des données. L'identité numérique facilite la réalisation des objectifs des secteurs privé et public dans le cadre d'une économie des données, mais elle exige un cadre solide fondé sur la confiance afin d'atténuer les dommages potentiels, tels que l'abus de données personnelles, l'exclusion ou la discrimination fondée sur une représentation inexacte (ou injuste) des données, qui peuvent accompagner de telles initiatives. En outre, bien que les partenariats public-privé aient le potentiel d'étendre la prestation de services publics et de stimuler l'innovation socio-entrepreneuriale, ces collaborations peuvent potentiellement exacerber les inégalités (par l'utilisation abusive des données) en plus des préjudices mentionnés ci-dessus. Les cadres adoptés par les autorités/agences nationales d'identité existantes devraient donc être révisés pour refléter ces opportunités, risques et inconvénients.

9 Voir *https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity*

RECOMMANDATIONS

La mise en place d'un système d'identification numérique équitable et fiable est une condition préalable essentielle pour combiner et réutiliser les données administratives publiques avec d'autres types de données dans divers cas d'utilisation. Les activités régionales en matière de politique des données devraient s'aligner sur celles qui se déroulent dans le cadre d'activités identité numérique simultanées. Les initiatives d'identité numérique du secteur public doivent rester guidées par des cadres de gouvernance des données, qu'ils soient fondamentaux ou fonctionnels[10].

5.3.2 CRÉER DES SYSTÈMES DE DONNÉES LÉGITIMES ET DIGNES DE CONFIANCE

Définition des problématiques

Pour créer un environnement de données fiable, les utilisateurs doivent faire confiance à l'ensemble du système politique et économique qui sous-tend l'économie des données. Parmi les aspects fondamentaux de ce système, citons la sauvegarde des droits de l'homme fondamentaux par le biais de l'État de droit, des dispositions institutionnelles et des réglementations établies par des processus consultatifs et transparents, et l'obligation pour les institutions chargées de superviser l'utilisation des données, ainsi que pour les producteurs de données publics et privés, de rendre compte de l'utilisation des données publiques et à caractère personnel. L'inclusion et la diversité des personnes qui gèrent et supervisent les environnements de données, par exemple par le biais d'équipes mixtes, sont des critères importants pour instaurer la confiance. Plusieurs pays africains disposent déjà d'un grand nombre de ces aspects, le défi continental étant de s'assurer que tous les pays disposent de tous les aspects nécessaires et que ceux-ci sont adaptés de manière appropriée aux défis technologiques et économiques des données qui évoluent rapidement. Le cadre définit toutes les composantes essentielles des systèmes de données légitimes et dignes de confiance afin de permettre aux pays de déterminer s'ils ont certains ou tous les composants entièrement en place.

La confiance dans les transactions de données, les données statistiques et la prise de décision fondée sur les données doit donc être soutenue par un cadre juridique et réglementaire transparent et solide qui, à la fois, protège contre les préjudices liés aux données et soutient les outils facilitant l'accès aux données, leur partage et leur modification de manière responsable. Un cadre de confiance solide, et la capacité institutionnelle à soutenir ce cadre, permettront aux gouvernements de créer de la valeur à partir des données, de minimiser les asymétries de données entre le public et le privé, et de freiner les comportements non compétitifs sur les écosystèmes de données (Macmillan, 2020).

Dans ce contexte de construction d'un écosystème numérique de confiance, trois domaines clés interdépendants doivent faire l'objet d'une attention particulière : la cybersécurité, la cybercriminalité et la protection des données. Le rôle de la conception éthique et de la réglementation positive pour garantir des résultats justes mérite également d'être souligné.

10 La Commission de l'Union africaine élabore actuellement un cadre d'interopérabilité pour l'identification numérique qui fournira un ensemble détaillé de recommandations aux États membres sur l'introduction et la protection des systèmes d'identification numérique

5.3.2.1 CYBERSÉCURITÉ

L'évolution de la technologie et l'adoption de technologies de rupture créent de nouvelles menaces et des risques indésirables. Cela a un impact non seulement sur les biens, les infrastructures et les réseaux, mais aussi sur les économies, les sociétés et les personnes, les plus vulnérables étant les plus touchées. De ce fait, l'utilisation que les acteurs font des technologies perturbatrices et les normes, règles et pratiques des secteurs public et privé pour régir la sécurité, peuvent avoir un impact sur les droits fondamentaux des personnes en matière d'équité, de dignité et de sécurité.

Si les politiques, les lois et les réglementations peuvent être des outils utilisés pour repousser les menaces et protéger les personnes des risques, elles peuvent également servir à normaliser ou à légitimer les systèmes d'oppression et de répression. Par conséquent, toute réponse cybernétique visant à renforcer la sécurité des données devrait considérer les éléments de proportionnalité (y compris la légalité, le but légitime, la nécessité et l'adéquation) comme l'exigence la plus importante devant être satisfaite dans toute forme de limitation des droits de l'homme en ligne.

5.3.2.2 CYBERCRIMINALITÉ

L'écosystème des données met en évidence les opportunités et les risques d'un vaste réseau de systèmes publics et privés interconnectés. En raison de la nature transnationale de la cybercriminalité et des cyber opérations, la politique de sécurité des données est principalement élaborée dans des forums multilatéraux mondiaux ou régionaux. Si la participation africaine à ces forums s'est accrue, celle des acteurs africains non étatiques reste limitée. En outre, un nouveau défi politique consiste à évaluer les capacités nécessaires au niveau national pour mettre en œuvre les conventions régionales et mondiales sur la cybercriminalité, ainsi que les cyber normes volontaires et non contraignantes.[11]

5.3.2.3 LA PROTECTION DES DONNÉES

Les risques liés à la possession illégale de données traitées sont principalement supportés par les personnes concernées elles-mêmes, et non par l'entité qui en extrait la valeur. De ce fait, les mécanismes et principes d'atténuation des risques liés à la vie privée doivent être au cœur de tout cadre politique national et régional visant à exploiter le potentiel des économies de données.

Pour cela, il convient de mettre en place des institutions et des lois solides en matière de gouvernance des données, mais ces lois doivent également être adaptées aux contextes particuliers dans lesquels elles sont mises en œuvre. Il s'agit notamment de tenir compte des réalités socio-économiques et technologiques et des capacités du public. Autrement dit, un cadre politique en matière de données doit élaborer une politique et une réglementation capables de reconnaître les réalités des capacités et des fonctionnalités d'un citoyen, ainsi que les risques qui accompagnent les développements numériques et conduisent à une répartition inégale des avantages et des inconvénients (Sven, 2001 ; Van der Spuy, 2021).

11 La capacité de mise en œuvre est insuffisante dans cinq domaines : politique et stratégie de cybersécurité ; cyberculture et société ; éducation, formation et compétences en matière de cybersécurité ; cadres juridiques et réglementaires ; normes, organisations et technologies.

Par exemple, étant donné qu'un nombre important de personnes ne savent pas utiliser les outils numériques ou sont analphabètes en Afrique, le fait de s'appuyer sur des mécanismes numériques de consentement éclairé ne peut pas être suffisant pour protéger les droits des personnes. Il existe un risque que, pour de nombreuses personnes, les moyens numériques couramment utilisés pour obtenir le consentement, tels que la cliquer sur un bouton relié à un long ensemble de conditions juridiques, n'équivalent pas réellement à un consentement éclairé, car l'action censée constituer le consentement peut ne pas être un acte éclairé ou ne pas être comprise du tout par la personne qui l'effectue. D'autres moyens de gestion des données, tels que les fiducies de données, qui émergent à l'échelle mondiale et qui garantissent le respect des droits des personnes sur leurs données, sont examinés ci-dessous. De même, le cadre dominant de la gouvernance des données est généralement assimilé à la protection des données et la protection des données est assimilée au respect de la vie privée. Elle est largement comprise comme un droit individuel et un défi individuel. Toutefois, il existe des questions de droits communautaires et collectifs qui peuvent être importantes à mettre en avant dans le traitement des questions d'intérêt public.

5.3.2.4 LA JUSTICE EN MATIÈRE DE DONNÉES

Le concept de justice en matière de données promeut une vision plus large que la protection des données. Alors qu'un cadre de politique des données préservant les droits sera essentiel pour protéger les droits des personnes, les notions individualisées de la vie privée dans les cadres normatifs actuels de la protection des données peuvent ne pas être suffisantes pour assurer une inclusion plus équitable dans une économie des données digne de confiance. La justice en matière de données est un concept qui a gagné en popularité en réponse à l'adoption exponentielle de technologies axées sur les données dans le monde entier, en particulier l'intelligence artificielle (GPAI, 2021[12] ; Taylor, 2019). La justice en matière de données vise à garantir que le recours croissant aux données, notamment pour la prise de décision automatisée, ne perpétue pas les injustices historiques et les inégalités structurelles. Elle aborde la question de l'équité en réponse à la mesure dans laquelle les personnes sont visibles, représentées ou sous-représentées et discriminées en raison de leur production de données numériques.

La justice en matière de données s'étend également au-delà des notions de droits politiques et de justice, aux droits sociaux et économiques et à la réglementation nécessaire pour corriger les inégalités et permettre aux personnes d'exercer leurs droits. Il existe de nombreux autres domaines de la gouvernance des données en relation avec la disponibilité, l'accessibilité, la facilité d'utilisation et l'intégrité des données qui ont un impact sur l'inclusion équitable. Si ces derniers sont réglementés dans l'intérêt public, ils pourraient contribuer à une meilleure répartition des opportunités non seulement pour la consommation de services de données mais aussi pour la production de services.

12 Le Partenariat mondial sur l'intelligence artificielle a développé un projet qui vise à combler les lacunes de la recherche et de la pratique en matière de justice des données, en fournissant un cadre pour aider les praticiens et les utilisateurs à aller au-delà de la compréhension de la gouvernance des données étroitement comme une question de conformité de la vie privée individualisée ou de la conception éthique. Le projet cherche à inclure des considérations d'équité et de justice en termes d'accès et de visibilité et de représentation dans les données utilisées dans le développement des systèmes d'IA/ML. https://gpai.ai/projects/data-governance/data-justice/

RECOMMANDATIONS

Les États membres devraient s'efforcer d'établir un environnement de données digne de confiance par le biais de la cybersécurité, de la protection des données à caractère personnel, de l'État de droit et d'institutions compétentes, réactives et responsables. Ils devraient établir la confiance dans la gouvernance des données et dans un système national de données par la légitimité. Cela inclut des systèmes et des normes qui garantissent la conformité des secteurs public et privé, le respect par le gouvernement lui-même des règles de protection des données à caractère personnel et le partage des données publiques par le gouvernement.

→ ACTIONS

- Protéger les droits de l'homme fondamentaux dans l'environnement numérique grâce à l'État de droit
- Veiller à ce que les dispositions institutionnelles et les réglementations ne soient établies que par des processus inclusifs, consultatifs et transparents ;
- Veiller à ce que les institutions chargées de superviser l'utilisation des données, ainsi que les producteurs de données publics et privés, soient responsables de l'utilisation des données publiques et personnelles.
- Renforcer la coopération avec les autres APD pour assurer une sauvegarde suffisante, une protection réciproque des données personnelles ainsi que des droits numériques individuels et collectifs sur tout le continent.
- Renforcer les accords d'assistance mutuelle légaux et les activités entre les États pour les enquêtes et les poursuites en matière de cybercriminalité.
- Veiller à ce que les institutions chargées de superviser l'utilisation des données personnelles soient habilitées à disposer de pouvoirs d'entrée et d'inspection aux fins de l'application des lois et règlements sur la protection de la vie privée et des données.
- S'assurer en outre que l'institution responsable de la surveillance de l'utilisation des données personnelles dispose des pouvoirs de correction suivants en ce qui concerne la correction de la violation des aspects de l'utilisation abusive et de l'abus des données personnelles :
    - Avertir un responsable du traitement ou un sous-traitant des données que les opérations de traitement prévues sont susceptibles d'enfreindre les dispositions des lois et réglementations applicables en matière de protection des données.
    - Réprimander un responsable du traitement ou un sous-traitant lorsque les opérations de traitement enfreignent les dispositions des lois et réglementations applicables en matière de protection des données.
    - Ordonner à un responsable du traitement de communiquer une violation de données personnelles aux personnes concernées.
    - Imposer une limitation temporaire ou définitive incluant une interdiction de traitement des données personnelles.
    - Ordonner la suspension des flux de données vers un destinataire dans un pays tiers ou vers une organisation internationale qui n'assure pas une protection adéquate similaire à celle du pays exportateur de données.

- Les institutions chargées de surveiller l'utilisation des données personnelles devraient être habilitées soit à assister, soit à demander l'indulgence d'un tribunal pour aider une personne ayant subi un préjudice matériel à la suite d'une violation de ses données personnelles à recevoir une indemnisation d'un responsable du traitement ou d'un sous-traitant pour le dommage subi.

5.3.2.5 ÉTHIQUE DES DONNÉES

Un moyen important de réduire les risques et d'atténuer les préjudices liés à l'application des nouvelles technologies basées sur les données consiste à adopter une éthique des données adaptée au contexte. Des codes d'éthique devraient être élaborés par tous les groupes de parties prenantes travaillant dans le domaine des données, notamment les chercheurs, les associations industrielles et les experts en données. Ces codes d'éthique sont précieux pour guider l'utilisation des données et les processus de conception et de mise en œuvre des systèmes de données, y compris leur intégration dans le code informatique dans le cas du développement d'algorithmes.

Toutefois, les codes d'éthique ont été critiqués car ils représentent les points de vue de groupes démographiques limités, principalement ceux des entreprises et des technologues. Les codes d'éthique peuvent également dispenser les entreprises de leur responsabilité réglementaire lorsqu'ils sont utilisés comme une forme d'autorégulation, et peuvent être insuffisants pour permettre le respect des droits fondamentaux des personnes lorsqu'elles utilisent la technologie.

Les codes d'éthique, associés à la loi, permettent aux systèmes de données d'être fiables, car ils fournissent le type de détails pratiques et techniques qui sous-tendent les lois, qui sont souvent d'application plus générale que les codes d'éthique spécifiques, mais qui s'adaptent aussi parfois moins rapidement aux nouvelles technologies. L'éthique fonctionne de manière prospective, ce qui permet une conception éthique, tandis que les lois sont généralement promulguées et fonctionnent de manière rétrospective. Les codes de conduite éthiques devraient incarner les droits numériques et favoriser le respect du droit international et national.

L'UA soutient les efforts visant à rendre les codes éthiques plus inclusifs grâce à des processus qui prennent en compte les voix des citoyens, des consommateurs, des personnes marginalisées sous-représentées. Pourtant, les mécanismes permettant d'assurer l'adhésion aux codes éthiques et leur mise à jour sont sous-développés.

Les traités relatifs aux droits de l'homme - en tant que produits de processus consensuels entre les représentants légitimes des citoyens - jouissent d'une plus grande légitimité que les codes d'éthique et sont juridiquement applicables lorsqu'ils sont promulgués au niveau national et par le biais de décisions régionales. Si ces traités n'ont parfois pas la spécificité nécessaire pour les écosystèmes de données, les droits numériques, qui ont été formulés de diverses manières par la société civile entre autres et qui s'appuient sur le cadre des droits de l'homme, fournissent le type de spécificité dont on peut s'inspirer. Bien que les organismes de défense des droits de l'homme et les organes juridictionnels existants aient la capacité requise pour développer des droits en réponse aux questions liées aux données, leurs mandats juridiques ne leur donnent peut-être pas suffisamment de pouvoir pour le faire.

RECOMMANDATIONS

- Les États membres devraient encourager l'élaboration et l'adhésion à des codes d'éthique adaptés au contexte africain, qui favorisent les droits numériques et les droits de l'homme. Cela signifie que les personnes qui travaillent dans le domaine des données, quel que soit le secteur dans lequel elles travaillent, doivent respecter les droits et adhérer à ces normes éthiques. Ces codes doivent tenir compte des considérations de genre dans le contexte africain, en veillant à réduire les préjudices et l'exclusion des femmes et des filles. Il n'est pas possible pour les États membres de légiférer pour que toutes les technologies et tous les fournisseurs de technologies traitant des données adhèrent à des codes éthiques particuliers, car beaucoup de ces technologies sont conçues, construites et exploitées dans d'autres territoires. Les États membres devraient toutefois encourager l'adoption de ces codes d'éthique en n'utilisant eux-mêmes que des technologies et des fournisseurs de technologies qui adhèrent à des codes d'éthique approuvés.
- Outre les recours juridiques réglementaires ou judiciaires disponibles dans un pays, il est également possible d'envisager d'habiliter les mécanismes des droits de l'homme existants au niveau national, régional et continental à statuer sur les utilisations des données.

→ ACTIONS

- L'industrie des données et les communautés de recherche utilisant des données doivent formuler des codes de pratique, y compris les principes de responsabilité et d'éthique dès la conception, par le biais de processus incluant les personnes dont les données sont concernées ;
- Les États membres doivent exiger des cadres éthiques conformes aux droits dans les processus de passation de marchés publics ;
- Les États membres doivent inclure l'évaluation des codes d'éthique en matière de données dans les mandats des organismes de défense des droits de l'homme existants, tels que les commissions des droits de l'homme.

5.3.3 DISPOSITIONS INSTITUTIONNELLES POUR LA RÉGLEMENTATION DES SYSTÈMES ADAPTATIFS COMPLEXES

Les points suivants sont des considérations essentielles pour aligner le contexte réglementaire dans un pays qui dispose des exigences d'une économie de données. La réglementation dans les économies de données exige des décisions réglementaires flexibles orientées vers l'avenir en cas d'incertitude. Ainsi, les régulateurs ont besoin à la fois du mandat et de la confiance pour réglementer de manière proactive. Si les principes traditionnels d'indépendance, de transparence et de redevabilité continuent de guider la réglementation et la gouvernance des données, les décideurs politiques et les régulateurs doivent néanmoins développer de nouvelles capacités pour relever de nouveaux défis.

5.3.3.1 RENFORCER LES CAPACITÉS DES ORGANISMES DE RÉGLEMENTATION

Les processus de numérisation et de donnéification qui s'intensifient rapidement présentent de nouveaux défis réglementaires dans les domaines traditionnels de la concurrence et de la protection des consommateurs, ainsi que des domaines de réglementation entièrement nouveaux, notamment la protection des données à caractère personnel et la gouvernance algorithmique afin de garantir que les personnes ne soient pas victimes de discrimination. Si les principes traditionnels d'indépendance, de transparence et de responsabilité continuent de guider la réglementation et la gouvernance efficaces des données, les décideurs politiques et les régulateurs doivent développer de nouvelles capacités pour relever ces défis.

5.3.3.2 VERS LA FIN DES SILOS RÉGLEMENTAIRES

Les différentes dotations institutionnelles détermineront si les régulateurs existants ont les capacités de gérer de nouveaux domaines de gouvernance, toutefois il est indéniable qu'il faudra passer d'une réglementation cloisonnée au sein des secteurs traditionnels à une action réglementaire intégrée ou, à tout le moins, coordonnée. Cela est rendu possible par l'élaboration de stratégies et de politiques numériques transversales qui reconnaissent la nature transversale de la numérisation et de la donnéification. Cette démarche est essentielle pour créer la coordination nécessaire entre les différents secteurs des services publics concernés par l'économie des données, tout en répondant aux besoins sectoriels en matière de gouvernance des données.

Domaine de régulation	Points de collaboration potentielle avec l'autorité de régulation des données
Télécommunications	La disponibilité et la qualité de l'infrastructure fondamentale pour permettre les services basés sur les données
Concurrence	La concentration, les fusions et les acquisitions, les pratiques anticoncurrentielles sur les marchés du numérique et des données, mais aussi l'effet de la tarification et de la structure du marché sur la sécurité
Protection du consommateur	Les dispositifs et services numériques, le commerce électronique
Commerce et industrie	La fiscalité numérique, le commerce électronique, les services numériques, les services financiers numériques
Finance	Le blockchain financier, la cybersécurité, l'inclusion financière, les services financiers mobiles, la confidentialité
Éducation	La protection des enfants en ligne, la connectivité des écoles, la disponibilité des données pour l'acquisition de compétences en matière de données

Source : adapté de TGM 2020 dans UIT Banque mondiale 2020.

LE RÉSEAU AFRICAIN DES RÉGULATEURS DE L'INFORMATION

est un exemple de collaboration régionale visant à mettre en place des régulateurs de données nationaux, à sensibiliser aux nouvelles informations et à la gouvernance des données, à assurer la gouvernance des flux de données transfrontaliers et à coopérer avec les régulateurs au niveau international. Il s'agit d'aligner la gouvernance, notamment en ce qui concerne la réponse proportionnelle et normalisée aux violations de données et aux violations des droits.

Les régulateurs et les décideurs nationaux ont un rôle à jouer sur la scène internationale. Il s'agit d'intensifier la coopération internationale sur les flux de données transfrontaliers afin de s'assurer que les exigences de localisation des données et les autres restrictions sur les flux de données transfrontaliers n'interfèrent pas indûment avec les communications transfrontalières et les avantages économiques et sociétaux que les réseaux mondiaux de données rendent possibles et qu'elles restreignent le moins possible les échanges, tout en favorisant la confiance.

La coopération régionale et internationale sur les initiatives en matière de confidentialité des données et de cybersécurité doit également être encouragée afin de rationaliser les règles et pratiques disparates en matière de confidentialité des données et de cybersécurité dans des normes et des lois régionales ou mondiales communes et permettre la libre circulation des données et le commerce numérique (UIT, 2021).

5.3.3.3 RÉGULATEUR DE DONNÉES

La capacité des régulateurs sectoriels à être efficaces est déterminée, au moins dans une certaine mesure, par les dispositions institutionnelles et l'autonomie des régulateurs pour mettre en œuvre la politique. Les niveaux d'efficacité et d'innovation qui permettent l'évolution de l'écosystème dépendent de la disponibilité des aptitudes et des compétences des personnes et des institutions à chaque nœud de l'écosystème pour exploiter les avantages associés aux réseaux intégrés pour le développement économique et l'engagement social ou politique (Gillwald, Moyo et Stork, 2012). La mise en place d'un système de données intégré au niveau national et régional dépend aussi fortement de cadres réglementaires et politiques favorables qui facilitent l'obtention de données utiles, le renforcement des capacités humaines et techniques pour créer de la valeur à partir des données, l'incitation au partage des données et à l'interopérabilité, et l'augmentation de la légitimité et de la confiance du public au sein de l'État pour gérer les données des citoyens de manière responsable. Pour créer les conditions qui permettent l'accès nécessaire aux données tout en préservant les droits, il faudra renforcer les capacités et les compétences institutionnelles afin d'optimiser le potentiel des données, et développer des mécanismes d'application.

5.3.3.4 CONCURRENCE

Alors que les régulateurs africains s'efforcent d'introduire et d'appliquer la réglementation traditionnelle en matière de concurrence, il existe un risque que la réglementation statique de la concurrence pour régir des systèmes dynamiques et adaptatifs inhibe l'innovation et endommage la technologie sous-jacente permettant l'innovation. Par exemple, une réglementation axée sur la limitation de la domination de la seule couche applicative de l'internet pourrait avoir un impact négatif, voire nuire à l'ensemble de l'internet et de son infrastructure. Les régulateurs doivent faire attention à ne pas appliquer de manière instrumentale des règles de concurrence de marché unilatérales basées sur des modèles d'efficacité statique aux nouvelles plateformes de données et aux nouveaux produits basés sur l'efficacité dynamique qui peuvent produire des produits complémentaires innovants

(comme Whatsapp) qui améliorent le bien-être et le choix des consommateurs ou même les possibilités de concurrence locale sur leurs plateformes tout en étant dominants sur le marché mondial sous-jacent (comme Facebook).

Les plateformes se distinguent des opérateurs traditionnels sur les marchés, car elles sont constituées de nombreux marchés pertinents qui ont de multiples « côtés », chacun ayant une dynamique de concurrence spécifique. De même, les produits et services OTT (Over the Top) peuvent sembler verticalement intégrés alors qu'en réalité ils sont complémentaires et renforcent la concurrence. Ces types de défis exigent des régulateurs tout aussi adaptables, capables de gérer leur complexité dans l'intérêt du public.

5.3.3.5 PROTECTION DES CONSOMMATEURS

Les organismes de protection des consommateurs n'étant pas responsables d'un secteur spécifique, ils se sont généralement appuyés, dans l'exercice de leurs fonctions, sur d'autres régulateurs sectoriels. Des règles claires, solides et applicables en matière de gouvernance des données peuvent constituer une défense adéquate pour la protection des consommateurs numériques tout en créant un cadre prévisible et structuré pour les activités numériques. Des protocoles et des mécanismes réglementaires agiles, capables de s'adapter à des technologies et des conditions en évolution rapide, peuvent grandement contribuer à renforcer la confiance dans l'écosystème numérique. Il s'agit notamment de se conformer aux exigences liées à l'accès aux données à caractère non personnel conservées par les plateformes numériques, à la transparence de certains algorithmes essentiels utilisés par les services numériques, à la portabilité des données essentielles des plateformes structurantes, ainsi qu'à l'interopérabilité et à la maintenance des API (UIT, 2020).

Un moyen d'accroître la transparence sur l'utilisation des données des consommateurs est la création d'un portail de transparence, mais cela dépend du fait que l'autorité de réglementation des données dispose des ressources nécessaires pour établir, surveiller et faire respecter les violations. Cela permet aux personnes d'avoir un accès sécurisé à un portail où elles peuvent obtenir l'inventaire de quand et avec qui leurs données personnelles ont été partagées, ce qui leur permet de contester les données partagées ou utilisées sans leur consentement. Cette disposition peut ne pas s'appliquer à certaines catégories de données d'intérêt public, le partage des données s'effectuant par pseudonymisation ou anonymisation des données.

RECOMMANDATIONS

Les États membres de l'UA doivent disposer de réglementations adéquates, notamment en matière de gouvernance des données et de plateformes numériques, afin de garantir que la confiance est préservée dans l'environnement numérique. Les régulateurs des données devraient disposer des pouvoirs nécessaires pour faire respecter les réglementations en matière de données, tels que les pouvoirs d'émettre des avertissements, de sanctionner les violations, d'accorder des compensations aux victimes de données, et de coopérer avec d'autres organismes, y compris les organismes d'exécution.

→ **ACTIONS**

- Les Membres disposant de régulateurs de données devraient évaluer si les pouvoirs d'application existants sont suffisants.
- Les membres créant des régulateurs de données devraient envisager un éventail de pouvoirs d'application, et en tenant compte des contraintes de ressources, de la manière dont les régulateurs de données pourraient potentiellement s'appuyer sur d'autres organismes pour l'application.

5.3.4 RÉÉQUILIBRER L'ÉCOSYSTÈME JURIDIQUE

Définition des problématiques

Un certain nombre de branches du droit, différentes mais qui se chevauchent, telles que la législation en matière de protection des données, le droit de la concurrence, la législation en matière de cybersécurité, la législation en matière de communications et transactions électroniques, et les différentes catégories de droit de la propriété intellectuelle, abordent la question des données. Toutefois, elles peuvent entrer en conflit ou se contredire. Contrairement à la protection des données qui ne s'applique qu'aux données pouvant être reliées à un individu, la réglementation de la concurrence s'applique aux données lorsque le contrôle des données a un effet anticoncurrentiel. La concentration du contrôle des données, y compris des flux de données et de l'analyse des données, implique non seulement des obstacles à l'entrée sur le marché, mais aussi l'intérêt public. La concentration des données, des flux de données et des systèmes de données augmente considérablement la probabilité et le préjudice qui peuvent être causés par des cyberattaques et des violations de données, car elle conduit à un seul ou à quelques points de défaillance qui peuvent avoir des conséquences à grande échelle. Ces préoccupations ne sont pas du ressort de nombreuses autorités de la concurrence, mais devraient l'être puisqu'il s'agit de questions d'intérêt public. Les autorités de la concurrence peuvent être mandatées pour éviter la centralisation structurelle des entreprises de données qui augmente les risques de cyber-attaques ou de violations massives des données à l'échelle de la société. L'accès aux données est généralement favorable à la concurrence, mais peut entrer en conflit avec d'autres lois telles que les droits de propriété intellectuelle sur les données et les bases de données, ainsi que la protection de la vie privée et des données.

S'il est généralement admis que les données brutes ne sont protégées par aucun droit de propriété reconnu, des revendications ont été formulées sur les données en fonction des différents types de propriété intellectuelle : droits d'auteur, protection sui generis des bases de données, secrets commerciaux et brevets. Aucun de ces droits ne confère la propriété des données en tant que telles. La protection sui generis des bases de données est un droit propre à l'Union européenne, limité à l'Europe. Dans quelques pays de Common Law, le droit d'auteur a été étendu aux bases de données et aux compilations de données, mais même ces pays ont des règles différentes, certains tribunaux étendant le droit d'auteur simplement pour l'effort de compilation, tandis que d'autres exigent un critère de créativité. Le droit d'auteur est destiné à récompenser les auteurs humains et son application aux bases de données compilées par des ordinateurs est indéterminée. Les litiges entre concurrents sur l'utilisation des bases de données standard de l'industrie chevauchent le droit d'auteur et le droit de la concurrence. Un jugement du tribunal (Discovery Ltd and Others c. Liberty Group Ltd ZAGPJHC 67, 2000) offre une solution qui respecte à la fois la protection des données et la concurrence : dans ces litiges, si les données sont de nature personnelle, elles sont la « propriété » de la

personne concernée et les concurrents ne peuvent pas empêcher les autres d'accéder à ces informations. Alors que l'application des lois sur la propriété intellectuelle aux données est toujours en cours de résolution, les droits des personnes sur leurs données personnelles devraient être considérés comme plus forts que toute revendication de propriété intellectuelle sur ces données, étant donné l'importance de la protection des données pour la construction d'économies de données.

Les secrets commerciaux peuvent également s'appliquer aux données dans certaines circonstances, mais ces circonstances ne sont pas clairement définies.

L'application des lois sur la propriété intellectuelle est à la fois compliquée et indéterminée, mais il est au moins clair que les revendications sur les données fondées sur la propriété intellectuelle, même si elles sont contestées, compromettent potentiellement les flux bénéfiques de données et la protection des données.

Les lois sur la cybercriminalité interdisent l'accès, l'utilisation ou la modification non autorisés des données à caractère personnel ou des systèmes d'identification. Comme cela a été rappelé tout au long du cadre stratégique, la sûreté et la sécurité sont essentielles à la mise en œuvre effective de la politique et constituent une condition préalable, mais non suffisante, à la mise en place d'un système fiable. Les lois sur la cybercriminalité, en déterminant les modes d'accès, d'utilisation et de distribution des données, ont le potentiel d'élever les barrières d'entrée dans l'économie des données. La Convention de Malabo, adoptée par l'Union africaine qui a été spécialement conçue pour la région, traite à la fois de la cybercriminalité et de la protection des données. Toutefois, elle n'est pas encore en vigueur car elle doit être ratifiée.

Les États membres disposent d'une opportunité de réinventer un système juridique harmonisé qui équilibre de manière adéquate les intérêts divergents.

RECOMMANDATIONS

En vue de garantir un accès équitable et sûr aux données pour l'innovation et la concurrence, les États membres doivent établir une approche juridique unifiée, claire et sans ambiguïté, qui offre une protection et des obligations sur tout le continent. Lorsque nécessaire, les instruments juridiques existants doivent être réexaminés régulièrement pour s'assurer qu'ils ne sont pas en conflit les uns avec les autres et qu'ils offrent des niveaux complémentaires de protection et d'obligations aux États membres. Les États membres devraient soutenir la rationalisation de ces politiques au niveau infranational pour faciliter une mise en œuvre adéquate à tous les niveaux économiques. Les lois sur la propriété intellectuelle devraient être révisées pour préciser qu'elles n'entravent généralement pas la circulation des données ou leur protection.

→ **ACTIONS**

- Les ontrats qui visent à renoncer aux droits numériques, à la protection des données à caractère personnel et qui entravent la concurrence devraient, en règle générale, être inapplicables. Cela peut être formulé dans la réglementation relative à la protection des données et à la concurrence, qui peut également déterminer au cas par cas si les effets pro-concurrentiels de ces contrats l'emportent sur les effets anticoncurrentiels ;
- Les commissions nationales de réforme du droit ou des institutions juridiques expertes similaires devraient étudier et examiner comment harmoniser les différentes branches du droit, les régimes réglementaires et les organismes de contrôle qui traitent des données ;

- Les États membres devraient soutenir la mise à jour ou l'adoption de cadres et de réglementations en matière de droit de la concurrence qui prennent en compte les défis liés à l'analyse des questions de concurrence, à la conception de solutions et à l'application de leurs pouvoirs pour préserver la concurrence sur les marchés axés sur les données, ainsi que le renforcement de la capacité des régulateurs de la concurrence à mettre en œuvre ces règles ;
- Les lois sur la propriété intellectuelle devraient être modifiées pour prévoir :
  - que le droit d'auteur ne s'applique qu'aux bases de données et aux compilations de données d'auteurs humains qui font preuve d'originalité/créativité et que le droit d'auteur ne s'étend qu'à la sélection et à la disposition originales des données dans une base de données et non aux données elles-mêmes ;
  - que tout droit d'auteur ou autre droit de propriété intellectuelle, y compris les secrets commerciaux, qui permet le contrôle des données ne s'applique pas aux données à caractère personnel ;
  - que tout droit d'auteur ou autre droit de propriété intellectuelle, y compris les secrets commerciaux, qui permet le contrôle des données soit limité par les dispositions de la réglementation en matière de concurrence et des droits alternatifs qui offrent une protection aux innovations locales non envisagées dans les cadres actuels ; et
  - une adaptation des régimes de DPI existants pour tirer parti des technologies de pointe, par exemple en permettant à l'IA d'utiliser des données.

5.3.4.1 COLLABORATION AVEC LES PROCESSUS DE GOUVERNANCE RÉGIONAUX ET MONDIAUX

La réglementation de l'économie numérique et de l'économie des données dépasse de plus en plus le cadre des autorités réglementaires nationales (ARN). Pour être efficaces, les régulateurs doivent collaborer avec les régulateurs de leurs régions et du monde entier afin de garantir la réalisation de l'internet en tant que bien public, ainsi que son utilisation productive d'après les droits dans l'économie numérique.

La réglementation formelle doit laisser une place suffisante à l'autorégulation, aux modèles de réglementation hybrides et collaboratifs et aux mécanismes de contrôle de l'application de la loi. Les régulateurs disposent d'un large éventail d'outils et de solutions à explorer, allant des incitations et des récompenses aux obligations ciblées, en passant par l'abstention. Les instruments réglementaires se sont étendus pour couvrir les bacs à sable réglementaires, les cadres éthiques, les feuilles de route technologiques, les évaluations d'impact réglementaire, la recherche multivariée et la simulation de big data pour déterminer la réponse réglementaire la plus équilibrée, proportionnée et équitable. L'IA, l'IdO et la désinformation en ligne sont quelques-unes des questions complexes qui attendent d'être traitées (UIT, 2020).

5.3.4.2 UNE RÉGLEMENTATION CONSULTATIVE ET FONDÉE SUR DES PREUVES

En vue d'exploiter l'expertise des parties prenantes, les réglementations devraient également être le résultat de processus consultatifs multipartites axés sur l'intérêt public. Elles devraient également être fondées sur des preuves et contextuelles. Des données administratives améliorées grâce à une meilleure collecte et analyse, et sur lesquelles les régulateurs peuvent prendre des décisions, amélioreraient considérablement la prise de décision au sein

des organismes. Cela leur permettrait également d'offrir une plus grande certitude aux parties prenantes dans un cadre souple et adaptable, renforçant ainsi leur crédibilité (Banque mondiale & UIT, 2020).

RECOMMANDATIONS

- Lors de la création des dispositions institutionnelles, les États membres devraient clairement distinguer les rôles de l'État en tant que décideur politique et du régulateur, qui devrait être suffisamment indépendant de l'État et de l'industrie, afin de mettre en œuvre la politique dans l'intérêt du public et des fournisseurs de services et opérateurs de plateformes.
- Les institutions de régulation doivent être établies sur la base des principes d'autonomie, de transparence et de responsabilité afin d'éviter l'emprise de l'État et des organismes de régulation. Les régulateurs devraient entreprendre des études d'impact réglementaire à un stade précoce de la réglementation afin de mettre en œuvre les meilleures approches qui concilient réglementation et croissance économique. Les régulateurs doivent publier les résultats de leurs efforts politiques et réglementaires afin d'améliorer les stratégies réglementaires dans tous les États, y compris les rapports sur la participation du public aux nouvelles réglementations. Les régulateurs doivent également être autofinancés ou financés par des crédits parlementaires afin de garantir leur indépendance financière. Les décisions réglementaires doivent être fondées sur des données fiables et exploiter les connaissances du secteur privé et de la société civile par le biais de consultations publiques. Les organismes de réglementation de la concurrence et sectoriels doivent éviter une réglementation instrumentale de la concurrence, via l'adoption de modèles d'efficacité dynamiques plutôt que statiques.

→ ACTIONS

- Faire une distinction claire entre les rôles de l'État en tant que décideur politique et du régulateur, qui doit être suffisamment indépendant de l'État et de l'industrie, afin de mettre en œuvre la politique dans l'intérêt public ;
- Créer ou maintenir des organismes de concurrence pour faire face à la dominance sur le marché et à la concentration par le biais de fusions et d'acquisitions ;
- Mettre en œuvre des procédures claires de coresponsabilité entre les organismes sectoriels et les organismes de concurrence afin de garantir une réglementation coordonnée du secteur des infrastructures et des services numériques et d'éviter le « forum shopping » qui consiste à chercher l'instance la plus favorable ;
- Les régulateurs de données devraient collaborer au niveau régional et continental pour harmoniser leurs cadres, notamment à l'appui de la ZLECAf ; et
- Les personnes soumises aux décisions des organismes de réglementation devraient disposer de mécanismes clairs d'appel et de recours entendus par un organisme différent de l'organisme de réglementation, rendant les décisions conformes aux règles de justice naturelle et d'action administrative équitable.

5.3.5 CRÉATION DE VALEUR PUBLIQUE

Définition des problématiques

Disposer de données sans capacité humaine, sans contrôle suffisant ou sans incitation à la valeur ajoutée revient à ne pas en avoir. Ces contraintes s'appliquent à de nombreux pays africains. Il est également difficile de favoriser un secteur public axé sur les données. La valorisation des données dépend fortement des cadres réglementaires et politiques habilitants qui facilitent l'obtention de données utiles, le renforcement des capacités humaines, institutionnelles et techniques pour créer de la valeur à partir des données, l'incitation au partage des données et à l'interopérabilité, et le renforcement de la légitimité et de la confiance du public au sein de l'État pour gérer les données des citoyens de manière responsable. En outre, l'infrastructure de données qui permet la mise en place d'un système de données intégré est un atout stratégique essentiel pour les pays. Le climat créé par l'interaction des éléments de l'écosystème des données et la nature des relations et des processus non linéaires entre eux et en leur sein, déterminent les interventions visant à créer des incitations pour les investissements technologiques qui sont nécessaires pour stimuler la croissance de l'économie des données. Ces conditions sont façonnées par la structure du marché, la compétitivité des services qui en découlent et l'efficacité de la réglementation du marché.

5.3.5.1 CAPACITÉ DU SECTEUR PUBLIC

Les capacités du secteur public en matière numérique et de données sont un facteur déterminant de la prestation de services dans de nombreux domaines prioritaires. Créer les conditions pour que les données soient optimisées dans le secteur public afin de répondre plus efficacement aux besoins des citoyens sont des conditions nécessaires à l'inclusion sociale et économique. Toutefois, il existe des inégalités multidimensionnelles et des inefficacités politiques superposées qui limitent les capacités humaines et institutionnelles pour renforcer une culture de l'entrepreneuriat numérique, favoriser des communautés d'innovation numérique inclusives et promouvoir des écosystèmes de données justes et équitables, où tous les Africains, quelques soient leurs compétences, puissent travailler avec des technologies numériques de pointe et contribuer au cycle de valeur des données ou participer aux chaînes de valeur des données de manière plus inclusive.

Pour qu'un secteur public axé sur les données se matérialise, la fonction publique doit être réorganisée avec un leadership et une volonté politique pour s'assurer que les fonctionnaires à tous les niveaux sont équipés d'une compréhension de base de la façon dont les données peuvent être utilisées pour améliorer la prestation de services et la mise en œuvre des politiques. En outre, un secteur public alimenté par les données nécessite une approche commune et un modèle architectural d'infrastructure de données capable de prendre en charge l'intégration et l'échange potentiels de données et d'applications pilotées par les données entre les secteurs, les applications et les plateformes.

5.3.5.2 CONSERVATION DES DONNÉES PUBLIQUES

Le secteur public est mandaté pour gérer les données clés du développement économique. Il s'agit notamment de données statistiques et d'indicateurs économiques utilisés pour l'établissement de rapports avec les institutions multilatérales, ainsi que de données

administratives, telles que les identités numériques. Ces données sont souvent anonymisées et combinées avec d'autres données dans divers cas d'utilisation allant de l'hyperpersonnalisation commerciale, comme la solvabilité, à l'intérêt public pour les subventions sociales et la gestion des catastrophes.

Pour que la création de valeur à partir des données soit efficace dans le secteur public, une approche transversale cohérente est nécessaire afin de comprendre quels sont les besoins en matière de données et la manière dont celles-ci peuvent être utilisées pour améliorer les efforts en termes socio-économiques et dans la prestation de services publics. L'absence de consensus général concernant les cadres de gouvernance des données, ainsi que le manque de bonnes pratiques sectorielles pertinentes (en fonction du cas d'utilisation), peuvent constituer une menace importante pour l'interopérabilité et les efforts de partage des données ouvertes, et limiter la mesure dans laquelle les gouvernements peuvent adopter des pratiques permettant de créer de la valeur à partir des données dans le secteur public. Faciliter l'interopérabilité est une question essentielle. Les systèmes de données ouvertes nécessitent une approche commune et des modèles d'infrastructure de données qui puissent prendre en compte l'intégration et l'échange potentiels de données lisibles par machine et d'applications basées sur les données entre les secteurs, les applications et les plateformes. Le partage des données et l'interopérabilité ne dépendent pas seulement des systèmes de données, des protocoles techniques, de l'infrastructure ou de la gouvernance. Ils nécessitent également un leadership et une volonté politique pour un consensus autour d'une approche de l'interopérabilité qui soit soutenue et adoptée dans le cadre de divers mandats du secteur public.

Dans le secteur public, les données sont souvent utilisées pour améliorer le contrat social et atténuer les asymétries d'information dans l'élaboration des politiques, ainsi que pour le suivi de l'impact des interventions et la prestation de services, notamment pour décider de l'affectation des ressources publiques. Les données publiques anonymisées peuvent être combinées avec d'autres ensembles de données à des fins commerciales pour réduire les coûts d'entrée sur le marché, perturber les industries, améliorer l'efficacité et faciliter le développement d'innovations, de produits, d'informations et d'opportunités qui peuvent être disponibles en ligne, sans limites des frontières géographiques et physiques. Toutefois, les institutions qui conservent les données publiques sont confrontées à divers défis qui sont examinés ci-dessous.

5.3.5.3 GARANTIR LA QUALITÉ ET LA PERTINENCE DES DONNÉES DU SECTEUR PUBLIC

Il existe plusieurs théories ou modèles pour étudier les défis liés à la qualité des données. La définition des déterminants de la qualité et de la pertinence des données d'un point de vue technique dépend donc d'un large éventail de scénarios d'application, tels que la disponibilité des données, le type de données, les caractéristiques du domaine et la manière dont les données sont utilisées et/ou collectées, entre autres (Wook et al., 2021 ; Wang et al., 1996). Par exemple, dans la recherche sur la santé, un cadre d'évaluation de la qualité des données comprendrait 30 indicateurs de qualité des données ou plus (Schmidt et al., 2021), tandis que pour la qualité des données de capteurs collectées à partir de dispositifs IdO, seules deux dimensions peuvent être prises en compte (Teh et al., 2020 ; Karkouch et al., 2016). En outre, l'avènement de l'analyse des big data, y compris l'apprentissage automatique (ou Machine Learning) et les capacités techniques au-delà de la science des données, telles que l'ingénierie et la gestion des données, permet de traiter les données (les nettoyer) et peuvent améliorer la qualité des données collectées, ce qui les rend disponibles pour une grande variété de cas d'utilisation (Wook et al., 2021 ; Svolba, 2019).

Les systèmes éducatifs ne sont pas adaptés à la réalité numérique et, par conséquent, les compétences dans les domaines STIM et les TIC et le numérique, ainsi que les talents existants sont limités pour exploiter pleinement les techniques d'analyse des big data et la science des données afin de créer de la valeur à partir des données accumulées ou produites. Les insuffisance dans la conservation et le partage des données dans le secteur public entravent le développement de systèmes des données intégrés et les avantages qui en découlent.

RECOMMANDATIONS

- Compte tenu du rythme accéléré de la numérisation, en tant que principal gardien des données des citoyens, le secteur public doit disposer de ressources adéquates pour exploiter les données afin de renforcer les intérêts publics, d'une manière qui protège les citoyens. L'un des moyens d'y parvenir est de mettre en place des formations ciblées et des initiatives de cocréation de connaissances avec d'autres organismes internationaux - les institutions manquant de ressources qui conservent les données publiques et abritent déjà des professions analytiques (statistiques, économie quantitative, recherche opérationnelle et recherche sociale, etc.). Ces ressources existantes peuvent être mises à niveau et utilisées pour améliorer la création de valeur des données dans le contexte du secteur public.

- Les États membres doivent s'engager à adopter une approche gouvernementale globale pour utiliser les données dans le cadre de diverses priorités politiques, les entités publiques qui conservent divers types des données doivent recevoir des mandats clairs et être dotées de capacités techniques, institutionnelles et humaines. Cela peut contribuer à garantir qu'ils sont des gardiens responsables de données de qualité qui peuvent être partagées et réutilisées de manière responsable pour de multiples cas d'utilisation.

- En vue de favoriser la confiance dans l'intendance des données publiques, les organismes de réglementation du secteur et les responsables des données publiques doivent collaborer avec les parties prenantes de l'industrie. Dans la mesure où les évaluations de la qualité des données du secteur privé échappent souvent au contrôle du secteur public, les efforts de gouvernance des données de l'industrie sont plus adaptés à l'élaboration de lois et de règlements encourageant l'utilisation des données de haute qualité. Cela est nécessaire pour tenir compte des différents cas d'utilisation qui nécessitent différents indicateurs d'évaluation de la qualité des données. Ces lignes directrices en matière d'évaluation devraient être élaborées dans le cadre d'efforts multipartites - la gouvernance des données doit être envisagée dans le contexte des réalités opérationnelles des différents cas d'utilisation des données, dans tous les secteurs.

→ ACTIONS

- Les organismes de réglementation du secteur et les responsables des données publiques doivent opérer dans le cadre de lignes directrices spécifiques concernant la manière dont les évaluations de la qualité des données doivent être réalisées, en fonction des cas d'utilisation communs, des algorithmes et du type de données utilisées. Ces lignes directrices peuvent s'inspirer des meilleures pratiques mondiales (notamment la gouvernance des données et de l'IA), mais doivent être adaptées au

contexte des cas d'utilisation des données africaines. L'échange, les combinaisons, le stockage stratégique et la réutilisation sont nécessaires pour créer de la valeur à partir des données. Pour qu'une stratégie puisse garantir la qualité des données dans l'ensemble du secteur public, celle-ci doit prendre en compte les réalités techniques/pratiques/opérationnelles et définir les rôles, les responsabilités et les mandats des différentes organismes publics dans la collecte et la conservation de données de haute qualité dans le respect de la protection des citoyens.

- Les États membres doivent participer aux efforts visant à définir et adopter un cadre normatif pour des normes et des systèmes des données harmonisés visant à établir une interopérabilité nationale, régionale et internationale. Il peut s'agir d'interventions ciblées en matière de formation humaine, technique et institutionnelle, de projets d'infrastructure sous-régionaux et de bacs à sable réglementaires des CER.
- Une approche continentale facilite les économies d'échelle pour inciter les investissements privés dans les infrastructures numériques fondamentales, notamment dans les technologies basées sur le cloud. L'harmonisation régionale des réglementations relatives à la gouvernance des données pourrait minimiser davantage les coûts de mise en conformité et réduire l'incertitude et le risque opérationnel pour les investissements majeurs dans les infrastructures liées aux TIC.
- Les institutions publiques qui conservent les données devraient disposer de ressources adéquates pour contribuer aux forums multilatéraux sur les données et être les gardiens d'un accès inclusif et d'une utilisation responsable des données, guidés par des normes techniques et réglementaires, des standards et des meilleures pratiques appropriés qui sous-tendent les caractéristiques informationnelles et économiques des données dans les secteurs prioritaires.

5.3.6 DES POLITIQUES SECTORIELLES COHÉRENTES POUR VALORISER LES DONNÉES

Définition des problématiques

Les politiques en matière de concurrence, de commerce et de fiscalité sont étroitement liées aux données. Des économies de données locales compétitives, par exemple, peuvent accroître les services fondés sur les données et l'ouverture commerciale peut stimuler le commerce numérique international et les investissements directs étrangers (IDE) sur les économies de données nationales. Toutefois, cela peut également renforcer la domination des oligopoles mondiaux sur les écosystèmes de données nationaux, créant ainsi des tensions commerciales liées aux flux de données transfrontaliers. Simultanément, les modèles commerciaux numériques axés sur les données peuvent miner la concurrence nationale et renforcer la concentration du marché, car les autorités fiscales ont du mal à quantifier, évaluer, établir et suivre les chaînes de valeur numériques en raison de caractéristiques telles que les vendeurs tiers et l'absence de présence physique comme base pour établir la responsabilité fiscale des entreprises dans le secteur des données.

Pour les États membres, une action collective par le biais d'une approche unifiée permettra plus probablement d'obtenir de meilleurs résultats tenant compte des contextes africains lorsqu'il s'agit de relever les défis en matière de concurrence, de commerce et de fiscalité sur les marchés des données.

5.3.6.1 POLITIQUE DE CONCURRENCE

Définition des problématiques

Les caractéristiques dynamiques des modèles d'entreprise axés sur les données créent des défis en matière de mise en œuvre des outils traditionnels de la politique de concurrence, d'application effective de la concurrence, de recours et de réglementation des concentrations sur les marchés numériques. Pour relever ces défis, il faut des interventions préventives sur le marché et une collaboration continue avec des politiques complémentaires telles que la protection des consommateurs, le commerce, l'industrialisation et l'investissement.

La politique de concurrence doit tenir compte non seulement des effets économiques des structures du marché des données, mais aussi des effets sur la sécurité et la vie privée, notamment en évitant la concentration des courtiers ou des plateformes de données, car cela pourrait générer une défaillance du marché en un point unique. Ainsi, l'application de la réglementation de la concurrence et la conception de la réglementation et de la politique ex ante doivent être adaptées aux économies de données.

5.3.6.2 POLITIQUE COMMERCIALE

Définition des problématiques

L'activité des systèmes numériques n'est plus encadrée par des juridictions nationales clairement définies. Une réforme de la politique commerciale est nécessaire pour faire face à l'augmentation du commerce numérique et du commerce électronique. Les différentes influences géopolitiques, les dotations et les capacités institutionnelles et humaines sur le continent peuvent affecter les approches unilatérales du commerce numérique et les efforts d'harmonisation régionale. La stratégie transfrontalière en matière de données adoptée au niveau national devra s'appuyer sur des capacités institutionnelles différentes et ne pourra être efficace que sur la base des dotations de l'écosystème de données mis en place. Celle-ci influencera la manière dont la valeur des données sera créée ou extraite au sein des pays africains et entre eux, et déterminera qui bénéficiera le plus du cycle de valeur des données au niveau national et régional. En outre, les facteurs « hors ligne » tels que l'infrastructure routière physique, la fiabilité postale, l'efficacité de la logistique et de la chaîne d'approvisionnement, entre autres, sont des catalyseurs cruciaux qui facilitent à la fois le commerce numérique et le commerce électronique.

COMMERCE DES SERVICES, FLUX DE DONNÉES TRANSFRONTALIERS ET LOCALISATION

Pour que le commerce numérique puisse avoir lieu, les données doivent être déplacées au- delà des frontières. Si l'accumulation de données peut être un moyen sûr et sécurisé de gérer les données, la thésaurisation des données sans possibilité d'utilisation, d'échange ou de réaffectation en toute sécurité peut également créer des risques de sous-utilisation, ce qui peut diminuer l'efficacité et amoindrir les autres avantages du commerce numérique. La protection des données et les réglementations nationales n'ont pas seulement un impact sur les opportunités commerciales locales, elles affectent également le commerce intrarégional et la participation à l'économie numérique mondiale axée sur les données.

Si les données à caractère non personnel sont utilisées et échangées au-delà des frontières, l'importance des données générées par les utilisateurs et des services numériques en tant qu'intrants dans diverses activités industrielles offrira d'énormes possibilités d'accroître les exportations de services numériques. Les services sont également des intrants dans de nombreux produits manufacturés et dans différentes chaînes de valeur des données. C'est la raison pour laquelle trois régimes stylisés généraux communs de gouvernance des données pour les flux transfrontaliers de données à caractère personnel sont apparus. Ceux-ci varient en termes d'ouverture, d'intervention requise et d'acteurs responsables. Il existe également des variations de ces trois modèles stylisés en fonction du type de données et du cas d'utilisation. Souvent, les données sensibles telles que les données à caractère personnel sont soumises à des exigences transfrontalières plus strictes que les données à caractère non personnel. Les règles et les normes de protection des données peuvent également être intégrées aux réglementations sectorielles dans des secteurs très réglementés comme la santé et la finance, qui exigent des évaluations de qualité et des considérations éthiques plus rigoureuses.

Le choix d'un régime stylisé de protection des données transfrontalières plutôt qu'un autre doit permettre de trouver un équilibre entre la promotion d'un développement économique équitable et la fourniture de garanties adéquates en matière de données. Les États membres doivent comprendre les effets économiques des différents régimes de gouvernance des données transfrontalières, en fonction de leurs réalités économiques et de leurs priorités de développement.

En outre, étant donné les déficiences de l'infrastructure de données de nombreux pays africains lorsqu'il s'agit de stocker et d'accéder à des quantités massives de données, si les services de données en nuage constituent une alternative plus rentable que la mise en place et l'exploitation d'un centre de données physique, certaines conditions permettant de créer un environnement propice à la fourniture et à la consommation de services en nuage doivent être favorisées. Enfin, les dispositions transfrontalières pour les services d'informatique en nuage et les centres de données, telles que la confidentialité des données, la sécurité et les restrictions sur le lieu d'hébergement des données (exigences de localisation), doivent être décidées en tenant compte des priorités de développement économique plus larges.

Les tableaux ci-dessous résument les principaux avantages et inconvénients de chaque régime de gouvernance des données, afin d'aider les décideurs politiques à décider de la meilleure approche à suivre dans le contexte de leurs priorités de développement.

Trois approches différenciées pour régir les flux de données transfrontaliers

Régime de gouvernance des données transfrontalières	Description	Avantages	Inconvénients	Hypothèses
Régime de transferts ouverts	Des dispositions d'homologation obligatoires a priori relativement faibles et des normes industrielles volontaires du secteur privé qui permettent la libre circulation des données (par exemple, aux États-Unis et dans l'APEC)	La charge réglementaire minimale permet une plus grande flexibilité dans le mouvement des données Plus adapté au commerce des services numériques et à la création de valeur des données La protection de la vie privée est un droit des consommateurs	isque de prolifération des normes entre les entreprises et les juridictions, sans garantie d'une norme minimale pour la protection des données personnelles Requiert des capacités techniques, humaines et institutionnelles Droits limités des sujets de données - absence de consentement pour l'utilisation des données personnelles	Des systèmes et infrastructures de données interopérables Une capacité humaine, technique et institutionnelle pour créer de la valeur à partir des données Des conditions préalables solides (facilitateurs) pour tirer parti de l'économie numérique basée sur les données Des sujets de données disposant de la capacité de donner leur consentement
Régime de transfert conditionnel	Une base de consensus, des garanties réglementaires établies en matière de données et des directives réglementaires générales émanant des autorités chargées de la protection des données ou d'accords internationaux (par exemple, le RGPD)	Offre un meilleur équilibre entre la protection des données et le besoin d'ouverture des transferts de données pour la création de valeur Favorise la création d'une autorité nationale de traitement des données Des lignes directrices claires et des garanties réglementaires obligatoires qui, une fois respectées, permettent la libre circulation des données transfrontalières	Est basé sur des droits forts des sujets de données Certaines conditions doivent être remplies ex ante Risque de perpétuer les charges de conformité et les goulets d'étranglement du commerce numérique	Comme ci-dessus Collaboration internationale et influence géopolitique pour faire respecter les conditions ex ante
Modèle de transferts limités	Les flux de données transfrontaliers sont conditionnés par l'approbation du gouvernement et les exigences de localisation pour le stockage ou le traitement national des données (par exemple, en Chine et en Russie).	Est basé sur des impératifs forts de sécurité nationale et de contrôle des données publiques	Une approbation réglementaire stricte pour les transferts internationaux de données qui peut exiger la localisation explicite ou implicite des données et leur stockage obligatoire	Comme ci-dessus

Source : Interprétation résumée des auteur à partir de Ferracane et Van der Marel (2021), WDR (2021).

COMMERCE ÉLECTRONIQUE

Les plateformes de commerce électronique permettent aux consommateurs de bénéficier d'une plus grande variété de choix à des prix plus compétitifs. Les stratégies visant à améliorer le commerce électronique ne peuvent pas être formulées isolément, car le commerce électronique est lié à une multitude d'autres questions, notamment l'identification numérique, la gouvernance des données, les droits de douane, les flux de données transfrontaliers, la cybersécurité, l'interopérabilité des systèmes de paiement, la protection des consommateurs[13], la concurrence, la fiscalité et les normes, pour n'en citer que quelques-unes. En outre, pour améliorer l'adoption du commerce électronique, il faut tenir compte de facteurs tels que la pénétration de l'internet, la fiabilité des services postaux, l'utilisation des services de paiement (comptes bancaires ou argent mobile) et la sécurité des serveurs internet[14]. Pour les États membres, une action collective par le biais d'une approche unifiée aura plus de chances de fournir de meilleurs résultats qui tiennent compte des contextes africains lorsqu'il s'agit de relever des défis qui se chevauchent et qui affectent différents mandats gouvernementaux sur les marchés de données dans les forums multilatéraux.

Les accords commerciaux ne constituent pas à eux seuls des instruments appropriés de gouvernance des données transfrontalières. L'approche commune actuelle consistant à utiliser les accords commerciaux pour régir les flux de données transfrontaliers n'a pas conduit à des règles contraignantes, universelles ou interopérables régissant l'utilisation des données entre les pays. Toutefois, dans le contexte de la ZLECAf, une approche harmonisée et coordonnée visant à relever les défis liés à l'intégration des données au niveau national contribuera à un meilleur alignement sur les divers efforts de coordination du commerce numérique et du commerce électronique intra régionaux qui se chevauchent, au-delà des futurs protocoles sur le commerce électronique[15] et les services[16] prévus par la stratégie.

RECOMMANDATIONS

- Pour favoriser des marchés de données compétitifs, sûrs, dignes de confiance et accessibles, les responsables de la concurrence doivent trouver des moyens coordonnés et efficaces de réglementer la concentration des marchés de données tout en préservant les avantages qu'ils offrent dans le contexte des différents besoins de développement sur le continent. Cela inclut une réglementation ex ante des problèmes de concurrence avant qu'ils ne s'aggravent sur le marché.
- Les décideurs politiques en matière de fiscalité, de concurrence et de commerce devront renforcer les capacités humaines et techniques pour traiter les questions émergentes au-delà du mandat sectoriel traditionnel qui peuvent affecter les marchés de données.
- Les États membres doivent promouvoir la prévisibilité et la convergence des régimes dans les domaines d'action complémentaires, de manière à ce qu'ils se renforcent mutuellement. Cela doit être fait pour naviguer de nouveaux modèles commerciaux

13 Protection des consommateurs en ligne et retours de produits, sécurité des consommateurs et responsabilité des fournisseurs.

14 *https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d12_en.pdf*

15 Le protocole sur le commerce électronique de la ZLECAf est un outil important pour préserver le marché africain consolidé dans la sphère numérique, et éliminer toute autre disposition qui pourrait potentiellement compromettre le programme de libéralisation et d'intégration. Les lignes directrices devraient être finalisées au cours de la phase III des négociations de la ZLECAf.

16 La phase II de la ZLECAf devrait porter sur le commerce des services, les droits de propriété intellectuelle, l'investissement et la politique de concurrence.

dynamiques axés sur les données qui peuvent favoriser le commerce numérique intra-africain et l'entrepreneuriat axé sur les données. Dans le même temps, les décideurs politiques devraient tenir compte des liens bidirectionnels entre les résultats économiques et la gouvernance des données et peser soigneusement les compromis.

- Les États membres devraient favoriser une approche régionale coordonnée, globale et harmonisée des défis de gouvernance mondiale associés à l'économie numérique mondiale axée sur les données, en favorisant notamment :
  - la collaboration transfrontalière pour la mise en œuvre d'instruments de politique de la concurrence visant à lutter contre les comportements anticoncurrentiels sur les marchés numériques axés sur les données ;
  - la portabilité des données par la réglementation et d'autres activités habilitantes ;
  - les efforts de l'Organisation de coopération et de développement économiques (OCDE) pour prévenir l'évasion fiscale en ce qui concerne les entreprises axées sur les données[17] ;
  - les accords de l'Organisation mondiale du commerce (OMC) sur les services fondés sur les données et le commerce électronique ;
  - la mise en place d'une infrastructure régionale coordonnée de données de base et d'initiatives de développement de systèmes de données numériques ;
  - le renforcement des capacités humaines, techniques et institutionnelles pour soutenir l'interopérabilité des données, la création de valeur et la participation équitable aux marchés des données ; et,
  - la contribution à l'harmonisation internationale des normes techniques en matière d'éthique, de gouvernance et meilleures pratiques concernant les données, d'analyse du big data et d'intelligence artificielle.

→ ACTIONS

- Les États membres devraient encourager une réforme et une expérimentation dynamiques des politiques et des réglementations (par exemple, des bacs à sable réglementaires au niveau de l'industrie et des CER) ;
- Les décideurs politiques doivent tenir compte des liens bidirectionnels entre les résultats économiques et la gouvernance des données et peser soigneusement les compromis. Les différentes entités étatiques doivent s'efforcer d'établir des cadres de partage de données sûrs et responsables qui répondent à la demande de données, facilitent l'interopérabilité des données, les flux de données transfrontaliers et les chaînes de valeur des données, ainsi que des normes et systèmes de données ouverts dans les secteurs prioritaires clés définis par la STN. Lorsque des mesures correctives sont imposées, elles doivent être fondées sur une analyse économique tenant compte des impacts à long terme sur les incitations à l'investissement et à l'innovation ;
- Pour que l'utilisation des données soit efficace, inclusive et innovante, il faudra une collaboration entre les institutions de régulation à travers différents mandats et une régulation coordonnée du marché (dans des domaines politiques interdépendants tels

17 *https://www.oecd.org/tax/beps/*

que les télécommunications, les finances, la concurrence, le commerce, la fiscalité et la réglementation des données) ;

- Les autorités de la concurrence ou les institutions connexes devront renforcer leurs capacités humaines et techniques pour traiter les problèmes de concurrence émergents, au-delà de la concentration du marché, qui peuvent affecter les marchés axés sur les données ;
- Les outils traditionnels de la concurrence, tels que les lignes directrices sur la définition des marchés, l'évaluation de la position dominante, les pratiques anticoncurrentielles (par exemple, l'abus de position dominante, les pratiques coordonnées et l'abus de puissance d'achat), les lignes directrices sur l'évaluation des fusions, ainsi que les théories du préjudice et la conception des solutions, devront être adaptés pour intégrer le dynamisme des données et les caractéristiques des entreprises axées sur les données;
- Les signataires de la ZLECAf devront déterminer la manière dont le protocole sur le commerce électronique fonctionnera parallèlement aux lois et politiques existantes, et devra rendre compte et soutenir les objectifs des autres protocoles tels que la politique d'investissement, de propriété intellectuelle et de concurrence (à négocier en phase II) ; et
- Développer et renforcer les mécanismes de dialogue public-privé pour améliorer l'élaboration des politiques liées au commerce électronique.

5.3.6.3 POLITIQUE FISCALE

Définition des problématiques

Une incohérence existe entre la taxation actuelle des bénéfices des plateformes mondiales et la manière dont la valeur est créée à partir des données dans le secteur de l'économie numérique. En Afrique, la plupart des pays représentent principalement des marchés de données pour les plateformes mondiales, les utilisateurs contribuant de manière appréciable à la génération de profits des plateformes sans qu'un mécanisme plausible de capture de la valeur ne soit mis en place. Actuellement, le trafic de données en Afrique augmente à un taux annuel de 41% (CNUCED, 2019), ce qui implique une plus grande utilisation et adoption des services fournis par les plateformes numériques mondiales dans la région. Bien que les institutions multilatérales se soient engagées, principalement sous l'impulsion du Cadre inclusif de l'OCDE sur L'érosion de la base d'imposition et le transfert de bénéfices (BEPS) (bien qu'il ne soit pas totalement inclusif pour l'Afrique puisque seuls 23 pays y participent), un consensus mondial n'a pas été atteint pour les différentes options proposées (Piliers 1 et 2) en matière de fiscalité numérique.

Plusieurs pays africains, réticents à retarder la taxation des services numériques ou non conscients des avantages pour leur pays des réformes internationales, mettent déjà en œuvre des mécanismes unilatéraux. Il s'agit notamment de taxes sur les services numériques et de prélèvements de péréquation fondés sur des données économiques significatives afin de saisir une partie de la valeur des données en taxant certaines parties de l'économie numérique au sein de leurs juridictions. Ces mécanismes comprennent également l'extension de la taxation sectorielle sur l'industrie des télécommunications et la taxation des transactions d'argent mobile et de l'utilisation de certaines applications de communication over-the-top (OTT) dans la région, telles que WhatsApp, Facebook, Twitter, Skype et Instagram. Si ces taxes visent à augmenter les recettes publiques, leur impact négatif sur les consommateurs a ralenti l'accès et l'inclusion numériques (en raison du déplacement des coûts pour les consommateurs) et

a restreint le droit à la liberté d'expression des citoyens. Du côté de l'offre, l'augmentation des taxes sur le secteur des télécommunications a un impact négatif sur les bénéfices des opérateurs du secteur résident (avec des conséquences négatives pour les investissements en infrastructures dont le besoin est crucial au sein de la région aux ressources limitées), tandis que les OTT fondés sur les données sont largement non taxés localement (CTO, 2020 ; ICTD, 2020 ; RIA, 2021).

Du point de vue de la souveraineté et des avantages fiscaux, chaque pays a le droit d'imposer les bénéfices des plateformes numériques mondiales dès lors qu'elles ont une interaction économique avec ses citoyens et ses résidents (en grande partie via la vente de leurs données à caractère personnel). Toutefois, bien que des millions de leurs citoyens et résidents utilisent des applications de données gérées par des plateformes numériques mondiales, les pays africains, dans le cadre du régime actuel de fiscalité internationale, n'ont pas le nexus requis pour imposer les bénéfices de ces entités. Bien que certaines des plateformes aient une forme de présence locale dans les pays africains, ces filiales ne sont que des services de soutien administratif et ne possèdent pas légalement les actifs de ces plateformes (qui sont en grande partie intangibles et actuellement non inclus dans les propositions de la plupart des formules de répartition), et ne reçoivent ainsi aucun revenu cumulable sur les actifs.

En outre, les différentes propositions fiscales relatives à l'économie numérique - qui comprennent des formules de répartition, l'application de la notion de présence économique significative (SEP) et l'utilisation de mécanismes indirects tels que la taxe sur la valeur ajoutée (TVA) et plus directement la retenue à la source - nécessitent toutes l'accès aux données relatives aux transactions, que les plateformes numériques mondiales ne sont actuellement pas disposées à partager (en particulier sur les marchés non-résidents). Même dans les cas où certaines de ces données sont accessibles, elles devront être vérifiées et validées.

Les récentes mesures législatives et politiques introduites par certains pays africains dans le contexte de plusieurs efforts multilatéraux et unilatéraux visant à taxer l'économie numérique peuvent ne pas être propices à la création d'un marché unique ou à l'accès aux ressources internationales pour réaliser des biens publics mondiaux et remplir certaines des conditions préalables à une économie de données compétitive sur le continent. L'exploitation de nouvelles sources de recettes fiscales pourrait permettre aux pays africains de supprimer les droits d'accises sur les réseaux sociaux et les services de données, ce qui réduirait les distorsions tant sur le marché local que dans le système fiscal mondial.

RECOMMANDATIONS

Les gouvernements africains doivent accroître les activités économiques au sein de leurs juridictions qui tirent parti des mécanismes de numérisation et de donnéification, car une productivité accrue dans ce domaine amplifiera les capacités de recettes fiscales plus élevées. Ce processus nécessitera le développement d'un plus grand nombre d'entreprises locales fondées sur les données dans le cadre de la politique industrielle de la région. Cette voie peut aider à atténuer les risques de conformité fiscale qui sont amplifiés dans la situation actuelle où une partie importante des données publiques dans la région est capturée et contrôlée par des sociétés des données étrangères (Khan & Roy, 2019).

→ **ACTIONS**

- Les États membres doivent soutenir l'harmonisation du régime fiscal des biens et services numériques au niveau régional, et l'alignement au niveau mondial, qui atténueraient les risques liés au fait que les petits marchés des économies de données ne sont pas en mesure de générer une valeur significative et d'être compétitifs sur les marchés mondiaux pour contribuer à l'échelle et à la portée nécessaires à la création de valeur axée sur les données et à des bases fiscales généralement limitées.
- De manière complémentaire, un fonds de données publiques coalisé par les pays membres de l'UA pourrait être mis en place en collaboration avec le secteur privé pour construire l'infrastructure nécessaire à l'extraction de ces données de transaction, où les données peuvent être conservées dans le cadre d'un fonds commun de données régionales au-delà du seul domaine de la fiscalité.
- La mise à disposition d'un fonds de données publiques exigera des pays africains qu'ils numérisent leurs systèmes d'administration fiscale pour permettre une évaluation et un recouvrement plus efficaces des taxes des plateformes numériques. Un système administratif fiscal numérique renforcera la capacité d'enregistrement des impôts, le partage des données de transaction avec les autorités fiscales nationales et l'échange d'informations sur les obligations fiscales auprès des plateformes numériques à des fins de conformité, tout en réduisant les coûts opérationnels.
- Les États membres devraient saisir l'occasion de la coordination de la taxation des services numériques pour un marché numérique unique pour exploiter de nouvelles sources de recettes fiscales qui pourraient leur permettre de supprimer les droits d'accises régressifs et fiscalement contre-productifs sur les réseaux sociaux et les services de données et, de réduire les distorsions tant sur le marché local que dans le système fiscal mondial.

5.4 GOUVERNANCE DES DONNÉES

Pour qu'une politique de gouvernance des données soit efficace, elle doit encourager un écosystème dans lequel de multiples parties prenantes s'efforcent d'améliorer l'accès aux données et leur utilisation. Elle doit également encourager la réutilisation et la combinaison des données de manière à limiter les dommages et les risques associés aux processus de donnéification tout en garantissant qu'une grande variété de données sera utilisée à son plus grand potentiel économique et social. Certaines de ces politiques impliquent la mise à disposition des données tandis que d'autres, au contraire, restreignent le flux de données (Macmillan, 2020).

5.4.1 CONTRÔLE DES DONNÉES

Le fait de faciliter le contrôle des données pour les entreprises et le gouvernement constitue un mécanisme important pour extraire la valeur des données (Carrière-Swallow & Haksar, 2019 ; Couldry & Mejias, 2018 ; Savona, 2019). La politique contribue à la fois à limiter la manière dont le contrôle peut être exercé, mais aussi à encourager les mécanismes de contrôle qui s'alignent sur les objectifs stratégiques d'une politique de données. Un rôle important de la politique est d'aider à assurer la clarté en termes de contrôle pour l'attribution des obligations et des responsabilités (Carrière-Swallow & Haksar, 2019 ; Zuboff, 2018).

5.4.1.1 SOUVERAINETÉ DES DONNÉES

Le contrôle des données peut également être compris au niveau national en relation avec la souveraineté des données (Ballell, 2019). La souveraineté des données s'appuie sur le concept d'État-nation souverain et renvoie à l'idée que les données générées dans l'infrastructure Internet nationale ou transitant par celle-ci doivent être protégées et contrôlées par cet État (Razzano et al., 2020). Dans le contexte numérique, elle peut être comprise au sens d'un sous-ensemble de la cyber souveraineté définie comme l'assujettissement du domaine cybernétique (mondial par définition) à des juridictions locales (Polatin-Reuben & Wright, 2014). Il existe deux approches de la souveraineté des données, une souveraineté faible et une souveraineté forte. La souveraineté faible des données fait référence aux initiatives de protection des données menées par le secteur privé, qui met l'accent sur les aspects de la souveraineté des données liés aux droits numériques. La souveraineté forte en matière de données favorise en revanche une approche dirigée par l'État qui met l'accent sur la sauvegarde de la sécurité nationale (Polatin-Reuben & Wright, 2014).

En général, le transfert de données à caractère personnel vers un autre pays n'est autorisé que sous certaines conditions, par exemple lorsqu'un autre pays dispose d'une loi qui exige des garanties suffisantes (notamment en matière de confidentialité et de sécurité) pour le traitement des données à caractère personnel. Les États exercent souvent leur souveraineté en matière de données pour protéger les droits de leurs citoyens, notamment par le biais de régimes de protection des données qui réglementent les flux transfrontaliers des données afin de protéger les droits des personnes concernées, souvent par le biais d'accords fixant des normes de protection des données et la protection réciproque des données échangées. Si des normes juridiques suffisantes sont nécessaires à la réciprocité, il en va de même de la capacité pratique des États à appliquer les normes convenues d'un commun accord. La mise en place de bonnes pratiques de gouvernance des données est une étape fondamentale pour la réalisation de la souveraineté des données.

5.4.1.2 LOCALISATION DES DONNÉES

Définition des problématiques

Alors que la localisation des données est souvent considérée comme une expression de la souveraineté des États, en tant qu'option politique possible, la localisation des données doit être évaluée sur une base coût-bénéfice. Ce choix politique peut présenter un défi pratique. Si la localisation des données est parfois motivée par la nécessité de protéger les personnes concernées, elle peut être appliquée à des données à caractère non personnel. C'est pourquoi il est essentiel que la localisation des données soit lue dans le contexte du contrôle, afin de souligner sur le plan politique l'importance des mécanismes de soutien qui peuvent faciliter l'acte de souveraineté.

La localisation des données implique l'érection artificielle de barrières législatives aux flux de données, notamment par le biais d'exigences de résidence des données et de stockage local obligatoire des données (Cory, 2017). Des règles strictes de localisation des données exigeant le stockage de toutes les données localement, et pas uniquement d'en faire une copie, rendent ces données sensibles aux menaces de sécurité, notamment aux cyberattaques et à la surveillance étrangère.

Certains pays africains sont confrontés à de graves contraintes de capacité technologique, de sorte que les demandes de capacité de localisation peuvent largement dépasser la capacité des centres de données nationaux. Parallèlement, les exigences de duplication des données peuvent imposer des obligations financières excessives aux entreprises locales.

RECOMMANDATIONS

- Les États membres doivent privilégier les partenariats politiquement neutres qui tiennent compte de leur souveraineté individuelle et de la propriété nationale afin d'éviter les ingérences étrangères susceptibles d'affecter négativement la sécurité nationale, les intérêts économiques et les développements numériques des États membres de l'UA.
- Les États membres de l'UA ont le droit de formuler des règles relatives au numérique et aux données en fonction de leurs priorités et de leurs intérêts notamment pour protéger la sécurité des informations de l'État et de ses citoyens, et pour empêcher des tiers d'exploiter injustement les ressources et les marchés locaux.
- Des accords bilatéraux et multilatéraux doivent être établis pour exercer la souveraineté et le contrôle nationaux, et des voies de recours en cas d'infraction sont nécessaires.
- La localisation doit être évaluée au regard des préjudices potentiels pour les droits de l'homme.
- Les exigences en matière de localisation des données nécessitent une spécificité des données. Les solutions de localisation des données ont été fortement articulées au sein de silos de données sectoriels (verticaux) dans différentes juridictions; par exemple, le Nigeria a institué certaines formes de localisation des données financières, l'Australie a prescrit des formes de localisation des données de santé, etc. Il s'agit d'un domaine dans lequel la spécificité est fortement requise, à la fois pour faciliter des flux plus larges dans la mesure où ils répondent à des impératifs politiques tels que la mise en place de la zone de libre-échange africaine, mais aussi pour la clarté qui peut aider à minimiser les coûts pour les entreprises et les innovateurs locaux et réduire les risques de conséquences involontaires.
- La politique en matière de données doit être claire, non seulement par sa spécificité, mais aussi par rapport à la catégorisation des données, de façon à permettre aux États membres d'exercer leur souveraineté en établissant, par exemple, des classifications de sécurité ou des niveaux spécifiques de sensibilité des données. Ceux-ci devraient être appliqués de manière cohérente dans l'ensemble de la politique en matière de données (et d'informations).
- Le développement d'une infrastructure de données devrait être exploré en tant que mécanisme permettant d'exercer un contrôle, mais doit être contextualisé en tenant compte des impacts environnementaux, des infrastructures de sûreté et de sécurité, des coûts dupliqués pour les communautés de données locales et des coûts globaux.
- Les capacités du secteur public devraient être investies pour informer les initiatives nationales et efficaces de contrôle des données.
- Les droits des personnes concernées devraient prévoir expressément un contrôle efficace des données personnelles. Les fiducies et les gestions de données devraient être explorés comme une autre forme de contrôle efficace des données personnelles (et des autres données).

→ ACTIONS

- Les autorités chargées de la protection des données (DPA) doivent être pleinement habilitées, notamment en ce qui concerne la souveraineté des données ;
- Les APD sont encouragées à adopter des pratiques de coopération internationale et régionale en prenant note des différents stades de mise en œuvre et d'application dans les États membres ;
- L'évaluation des risques et l'engagement multipartite devraient être utilisés pour concevoir des solutions de localisation des données dans la politique par les rédacteurs, incluant la participation de la société civile ;
- La politique en matière d'infrastructure de données doit être alignée sur les impératifs de contrôle des données par les rédacteurs de politiques, mais doit tenir compte de la cybersécurité, de la protection des données personnelles, des risques environnementaux et du coût ;
- L'administration publique et la politique d'investissement devraient s'aligner sur les capacités de contrôle des données en priorité ;
- Le renforcement des capacités en matière de protection des données, de cybersécurité et de gouvernance des données institutionnelles dans les organismes concernés devrait être assuré par la politique et l'allocation des actifs.

MÉCANISMES PERMETTANT D'EXERCER UN CONTRÔLE SUR LES DONNÉES

Il existe des mécanismes permettant d'exercer un contrôle sur les données, comme les fiducies de données. Les fiducies de données et/ou les gestions de données sont des formes alternatives de solutions de gouvernance discrètes dans le contexte des données. Une fiducie légale est un instrument juridique utilisé pour gérer des biens, tant corporels qu'incorporels. Une fiducie permet à une personne de détenir des actifs (dont elle n'est pas propriétaire) au profit des bénéficiaires de la fiducie. La personne qui détient les actifs a été autorisée à le faire et doit aux bénéficiaires de cette fiducie une obligation fiduciaire d'agir de manière responsable dans la gestion de leurs actifs. Cette structure juridique traditionnelle a été posée comme un moyen de gérer des collections de données pour le compte de groupes et de faciliter le partage de données en masse dans des situations où les modèles de licence ou de données ouvertes risquent de ne pas être réalisables, comme un moyen de favoriser l'innovation en facilitant un accès équitable (Stalla-Bourdillon et al., 2019).

L'Open Data Institute définit les fiducies de données comme fournissant « ...une gérance indépendante et fiduciaire des données » (Open Data Institute, 2018). L''élément fiduciaire a été ajouté à la définition (par opposition à la simple définition comme une forme de fiducie légale) car il s'agit d'un élément essentiel de responsabilité et d'obligation, qui constitue un fondement important du concept (Open Data Institute, 2020). En outre, elle peut inclure des solutions de protection de la vie privée par conception dans l'architecture de tout mécanisme conçu pour faciliter la confiance, donc dans la garantie de la vie privée en substance et en processus (Stalla-Bourdillon et al., 2019). Alors que les lois sur la protection des données peuvent créer des normes sur la façon dont les données d'une personne peuvent ou ne peuvent pas être traitées, en dehors du consentement ou du recours en cas de violation, les mécanismes permettant aux personnes d'agir sur

leurs données sont limités - ainsi, les fiducies de données aident à faciliter la réalisation du contrôle des données. Les fiducies de données offrent aux personnes concernées un mécanisme par lequel elles peuvent fournir (ou « partager ») leurs données, tout en leur retirant la responsabilité exclusive de « garantir » le respect de la protection des données par les acteurs des secteurs public et privé grâce à l'établissement d'une relation fiduciaire.

5.4.2 TRAITEMENT ET PROTECTION DES DONNÉES

Définition des problématiques

Alors que les principes de contrôle des données permettent de délimiter et de définir les obligations relatives aux données à caractère personnel et non personnel, les principes relatifs au traitement des données visent à définir les orientations politiques pour le traitement des données à caractère personnel, comme nous l'avons vu précédemment. La réglementation des données à caractère non personnel est déterminée par la catégorisation des données et les régimes d'accès spécifiques.

Ces formes d'orientation sont importantes en tant que mécanisme permettant de réaliser la protection de la vie privée et des données. Le traitement des données à caractère personnel représente un élément essentiel de la gouvernance des données et de la création d'un environnement de confiance. L'instauration de la confiance est considérée comme un élément nécessaire à la promotion d'une économie numérique et de données saine. Restreindre les limitations du processus aux données personnelles signifie que ces restrictions n'entravent pas les flux de données pour le commerce numérique ; mais pour garantir cette absence d'entrave, il faut des politiques de données cohérentes dans toute la région, qui soient basées sur des principes communs mais flexibles (Nations Unies, 2017).

Les droits des personnes concernées, en tant qu'aspect du traitement des données à caractère personnel, offrent également des avantages auxiliaires pour aider à garantir l'intégrité et la qualité des données.

Une approche de la protection de la vie privée dès la conception peut être adoptée lors de l'élaboration de technologies et de systèmes numériques, en vertu de laquelle la protection de la vie privée sera intégrée par défaut dans la technologie et les systèmes au cours du processus de conception et de développement (Cavoukian, 2009). Il peut s'agir, par exemple, d'intégrer la minimalité dans la collecte des données ou d'automatiser une anonymisation rigide. Cela implique qu'un produit soit conçu en accordant la priorité à la protection de la vie privée, au même titre que les autres objectifs poursuivis par le système. Cette conception doit intégrer une compréhension particulière de la manière dont les personnes utilisent les produits et de leur capacité à faire valoir leur droit à la vie privée.

Les techniques de désidentification, y compris l'anonymisation et la pseudonymisation, peuvent faciliter certaines utilisations des données tout en assurant une protection au moins partielle. La pseudonymisation peut être réalisée par l'utilisation d'un signifiant ou d'un masque ne pouvant être relié à une personne identifiable que par des données supplémentaires. Si l'anonymisation et la pseudonymisation peuvent permettre aux prestataires de services privés et au secteur public de faire un meilleur usage des données, elles dépendent de l'état actuel de la technologie et des mathématiques. Au fur et à mesure que de nouvelles approches mathéma-

tiques sont développées et que la puissance de traitement des ordinateurs augmente, des données considérées comme dépersonnalisées peuvent devenir identifiables. Bien que les réglementations en matière de protection des données exigent souvent la désidentification, ces techniques sont insuffisantes si les personnes concernées ne disposent pas de droits juridiques solides et si le régulateur n'a pas la capacité de faire respecter la protection des données.

RECOMMANDATIONS

- Il est nécessaire d'établir des APD indépendantes, financées et efficaces. En outre, pour garantir l'efficacité, les mesures de redevabilité sont essentielles pour aider l'autorité de protection des données à définir clairement son champ d'action. Il faut établir des cadres pour le traitement légal des données qui prévoient des sanctions dissuasives claires pour garantir la conformité. Ils doivent couvrir tous les acteurs pertinents du traitement des données.
- L'évaluation des risques liés aux données à caractère personnel doit être obligatoire lors du déploiement du développement technologique des données à caractère personnel.
- Un sous-principe important, qui doit être mis en action avec des cadres de traitement des données pour les acteurs publics et privés, est celui de la minimisation. La minimisation de la collecte des données à caractère personnel est l'un des mécanismes les plus efficaces pour atténuer les risques et les préjudices des personnes concernées.
- Il convient d'explorer les codes de conduite pour promouvoir les données et les besoins spécifiques du secteur. Ces codes, approuvés par l'APD concernée, peuvent fournir une expertise sectorielle et industrielle dans la gestion des risques et préjudices réels qui peuvent être associés au traitement, et garantir les meilleures pratiques dans la gestion de ces préjudices. Ils peuvent également contribuer à l'examen des exceptions sectorielles qui peuvent être nécessaires pour qu'une économie des données constructive puisse prospérer, tout en s'inscrivant dans un programme de développement durable plus large, par exemple en facilitant la recherche (dans le domaine de la santé ou dans d'autres domaines du développement social).

→ ACTIONS

- Des cadres de traitement des données devraient être établis en partenariat avec tous les partenaires concernés, mais pilotés idéalement par l'APD. Ces cadres devraient s'aligner sur les principes suivants : consentement et légitimité, limitation de la collecte, spécification de la finalité, limitation de l'utilisation, qualité des données, garanties de sécurité, ouverture (qui inclut la notification des incidents, corrélation importante avec les impératifs de cybersécurité et de cybercriminalité), responsabilité et spécificité des données.
- Les APD devraient être établies de toute urgence parallèlement aux législations nationales sur la protection des données à caractère personnel.

5.4.3 ACCÈS AUX DONNÉES ET INTEROPÉRABILITÉ

Définition des problématiques

L'accès et l'accessibilité des données s'entendent à la fois en termes de formes réactives d'accès facilitées par les lois et les réglementations, ainsi que par des formes proactives d'accès aux données (comme les données publiques ouvertes) (Charte des données ouvertes, 2015). L'accessibilité implique également le partage des données entre les différents acteurs ou services, un avantage important de la nature non rivale des données. Pourtant, cela nécessite une interopérabilité entre ces différents acteurs (Jones & Tonetti, 2020). Dans le contexte de la concurrence, les données ne sont pas facilement transférables d'une manière qui facilite les effets d'échelle entre les entreprises (Rinehart, 2020). Exiger des formes de portabilité des données reste une stratégie réglementaire clé pour faciliter la concurrence et les avantages pour les consommateurs, bien que les réalités n'aient pas encore été établies comme définitivement bénéfiques (Mitretodis & Euper, 2019 ; Rinehart, 2020). Du point de vue de la vie privée, en dehors des simples changements d'interopérabilité, la nature de la collecte des big data signifie que la portabilité des données a une incidence sur la vie privée d'autres utilisateurs (Nicholas & Weinberg, 2019).

RECOMMANDATIONS

- Les normes de données ouvertes devraient être prioritaires dans la création et la maintenance des données publiques. La création des données selon ces normes n'exclut pas la mise en place de mécanismes de contrôle ou de limitation de l'accès dans des catégories des données définies à des fins impératives.
- La portabilité des données doit être soutenue. La portabilité des données peut être une forme de droit de la personne concernée, défini comme le droit d'obtenir les données qu'un responsable du traitement détient sur elle, dans un format structuré, couramment utilisé et lisible par machine, et de les réutiliser à ses propres fins. La portabilité peut être facilitée par une politique de portabilité des données dans le secteur public, et par l'établissement de droits spécifiques de portabilité des données dans les contextes de consommation.
- Les partenariats de données (y compris les options telles que les banques de données) doivent être privilégiés en tant que mécanismes permettant de faire progresser les données ouvertes de qualité et préservant la vie privée.
- Pour tenter de faciliter la spécificité, la catégorisation des données peut être une méthode permettant d'assurer la cohésion des cadres de traitement des données au sein des allocations relatives au traitement, et des principes de sécurité. La catégorisation à laquelle il est fait référence ici ne correspond pas aux typologies sectorielles considérées de manière plus générale, mais plutôt à un mécanisme spécifique permettant de réaliser des formes particulières de risques qui s'alignent sur les types de données et d'informations et peuvent inclure des catégories sensibles (telles que les données relatives aux enfants) et des classifications de sécurité pertinentes, par rapport à des formes de données qui sont déjà dans le domaine public.
- Les restrictions sur le traitement doivent être clairement articulées et limitées, afin de ne pas interférer avec le traitement à faible risque qui pourrait être de plus en plus essentiel à la formation de l'IA par le traitement de données à grande échelle.

→ **ACTIONS**

- Les États membres devraient mettre en place une politique d'ouverture des données qui fixe des normes ouvertes pour la production et le traitement des données, de sorte que lorsque la décision d'ouvrir les données est prise, les coûts élevés pour s'assurer qu'elles sont utilisables et manipulables sont évités.
- Les lois sectorielles et les codes de conduite des APD devraient être examinés pour garantir un accès légal aux données, conjointement avec la politique en matière de données ;
- Les APD devraient avoir une double fonction d'accès à l'information et de protection de la vie privée ;
- Des initiatives multisectorielles d'ouverture des données devraient être mises en œuvre sur des secteurs de données prioritaires comme la santé, la recherche et la planification.

5.4.4 SÉCURITÉ DES DONNÉES

Définition des problématiques

La sécurité des données comprend l'ensemble des politiques, normes, règlements, législations et pratiques visant à protéger la confidentialité, l'intégrité et la disponibilité des données contre les accès non autorisés, la corruption ou le vol, tout au long du cycle de vie des données. Ces principes fondamentaux de la sécurité des données définissent également les trois principaux domaines de responsabilité de la sécurité de l'information. Le concept de sécurité des données englobe de nombreux aspects, de la sécurité physique du matériel des centres de données et des dispositifs de stockage aux contrôles d'accès administratifs, en passant par la sécurité logique des réseaux, des logiciels et des applications. Il inclut également les procédures et politiques organisationnelles.

La confidentialité, l'intégrité et la disponibilité des données, d'un point de vue réglementaire, dépendent des politiques et de la législation nationale en matière de cybersécurité. La sécurité des données (y compris la confidentialité, l'intégrité et la disponibilité) ne dépend pas de l'emplacement physique des serveurs qui hébergent ces données. Elle est plutôt fonction des règles normatives - notamment les normes, les politiques, les règlements, les lois et les protocoles (tels que les normes de données et les interfaces techniques), ainsi que la mise en œuvre des technologies et des mesures de sécurité (telles que le cryptage, le pare-feu et les contrôles d'accès) - qui sont mises en place par les prestataires de services publics ou privés dans la manière dont ils stockent, accèdent, partagent et utilisent les données.

Le renforcement de la législation sur la sécurité des données et des mesures techniques peut à la fois améliorer la confidentialité, l'intégrité et la disponibilité (sécurité positive) et porter atteinte aux libertés et droits fondamentaux que sont la vie privée, la dignité et la sécurité en ligne (sécurité négative). Par exemple, pour protéger la sécurité des données des utilisateurs, certains pays peuvent imposer des restrictions au partage et au transfert des données en adoptant une législation sur la cybersécurité. Celles-ci peuvent constituer des obstacles à la libre circulation des données. Du point de vue de la cybersécurité, certains États peuvent penser que les données sont plus sûres si elles sont stockées à l'intérieur des frontières nationales. Les États peuvent s'y référer à tort comme à des principes de souveraineté des données, alors que ces mesures sont simplement des formes de protectionnisme et de localisation des données.

Un principe difficile à faire respecter en matière de sécurité des données est celui de la transparence. Si les pays continuent d'enregistrer une augmentation du nombre d'attaques signalées aux forces de l'ordre, les améliorations dans ce domaine sont presque entièrement dues aux réglementations sur la protection des données, et les incidents signalés sont principalement des violations de données. D'autre part, l'augmentation de la transparence sur la sécurité des données comprend à la fois des aspects techniques tels que le signalement des vulnérabilités de type « zero-day » et l'adhésion aux normes internationales de cybersécurité, ainsi que des aspects politiques liés à l'évaluation de la maturité des cyber capacités. La transparence sur la sécurité des données a le potentiel d'améliorer les mécanismes de défense techniques et procéduraux contre les attaques et de renforcer les pratiques de collaboration fondées sur le partage des informations.

RECOMMANDATIONS

- Les États membres devraient élaborer des politiques nationales de cybersécurité ainsi que les mesures juridiques et techniques nécessaires pour soutenir la confiance dans leur espace numérique.
- Les États membres sont encouragés à coopérer au niveau régional pour élaborer des normes de cybersécurité à respecter dans les secteurs public et privé afin d'accroître la croissance économique régionale.
- Les politiques en matière de données devraient s'aligner sur les politiques de cybersécurité et de cybercriminalité, et la législation traitant de la cybercriminalité devrait respecter les droits de l'homme.
- Un régime de sanctions commun pour les cyberattaques devrait être établi.

→ ACTIONS

- Les États membres, qui n'ont pas encore entrepris la mise en place de mesures de cybersécurité, devraient immédiatement élaborer des plans de cybersécurité et les rationaliser au sein des structures de gouvernance publiques afin de promouvoir la solidité et de réduire les vulnérabilités.
- Les institutions de cybersécurité telles que les équipes de réponse aux incidents de sécurité informatique (CSIRT) devraient être intégrées dans l'élaboration des politiques en matière de données.
- Les rôles de traitement des données en tant que forme de protection de la sécurité devraient être spécifiés dans la politique par les décideurs.
- Le renforcement des capacités en matière de protection des données, de cybersécurité et de gouvernance institutionnelle des données dans les organismes concernés devrait être assuré par le biais des politiques et de l'allocation des ressources, et pourrait être soutenu par les APD.

5.4.5 FLUX DE DONNÉES TRANSFRONTALIERS

Une question de plus en plus importante concernant le commerce international et régional est le transfert transfrontalier de données à caractère personnel et des autres données (Deloitte, 2016). Dans le contexte africain, les cadres internationaux et régionaux qui facilitent les transactions transfrontalières et les flux de données à caractère personnel entre les pays sont es-

sentiels pour la création de marchés communs et notamment pour la réalisation de l'Accord de libre-échange africain. Le transfert transfrontalier de données à caractère personnel, en particulier, est façonné par l'approche de la souveraineté des données qu'un pays souhaite poursuivre, qui renvoie au principe juridique selon lequel les informations (généralement sous forme électronique) sont réglementées ou régies par le régime juridique du pays dans lequel ces données résident. Comme indiqué, ce concept est remis en question par la réalité moderne des mouvements de données. Il convient toutefois de prendre acte des critiques formulées à l'encontre de la théorie des "flux de données" et de l'étendue de ses avantages pour les dividendes numériques dans le développement, et de reconnaître que des quantités importantes de flux de données se produisent en réalité horizontalement au sein des entreprises plutôt qu'entre elles (CNUCED, 2021).

Il convient également de mentionner la position commune selon laquelle le transfert de données dépend de l'existence d'un niveau de protection adéquat dans le pays récepteur (Razzano et al., 2020). Toutefois, ce qui constitue ce niveau « adéquat » sera souvent déterminé par l'autorité de protection des données d'un pays, ou par une autorité similaire. Ainsi, en l'absence d'une loi sur la protection des données dans le pays récepteur, le transfert de données à caractère personnel ne peut pas faire l'objet d'une réglementation appropriée, à moins que la loi d'un pays n'interdise le transfert de données vers les pays ne disposant pas d'un niveau de protection adéquat, ou par l'établissement d'obligations bilatérales au moyen de l'établissement d'un contrat entre les parties au transfert.

En réalité, de larges limitations du transfert transfrontalier de données pourraient faire perdre des opportunités commerciales et réduire la capacité d'une organisation à faire du commerce international, ce qui entraînerait une réduction de l'empreinte géographique et une perte de compétitivité sur le marché (Razzano et al., 2020). Une réglementation des données synchrone avec les réglementations d'autres juridictions contribue à la confiance mutuelle et jette les bases d'un échange de données en toute confiance, y compris (mais pas seulement) des données à caractère personnel. En ce sens, la réglementation de la protection des données personnelles permet et améliore la confiance et le commerce dans la circulation transfrontalière des personnes, des biens et des services (Information Society, 2018).

RECOMMANDATIONS

- Les cadres de protection des données devraient fournir des normes minimales pour les flux de données transfrontaliers ;
- L'établissement de normes et de standards devrait expressément garantir la réciprocité comme principe central de l'autorisation des flux transfrontaliers ;
- La spécificité des données devrait être privilégiée afin d'éviter des restrictions involontaires au partage productif des données ;
- Les considérations relatives à l'application de la loi devraient être intégrées dans le processus d'élaboration des politiques ;
- Pour garantir une résolution transfrontalière efficace, un certain degré de capacité doit être assuré entre les agences ;
- Les membres de l'Union africaine devraient définir rigoureusement un cadre et des modalités de régulation des flux de données transfrontaliers, et identifier l'entité et les personnes africaines habilitées à gérer ce système.

→ **ACTIONS**

- Les APD devraient établir des normes minimales pour le transfert des données ;
- Le renforcement des capacités en matière de protection des données, de cybersécurité et de gouvernance institutionnelle des données dans les organismes concernés devrait être assuré par l'allocation de politiques et d'actifs, et piloté idéalement par les APD en conjonction avec les établissements d'enseignement, et les programmes et unités de compétences du gouvernement.

5.4.6. DEMANDE DES DONNÉES

Si d'importantes recommandations relatives aux données et à l'économie numérique visent à contribuer à la création d'un écosystème de données plus large, certaines interventions politiques spécifiques sont aussi à mettre en œuvre pour stimuler la demande de données. Les utilisateurs de données peuvent être le secteur public, des entreprises privées (de différentes tailles), ainsi que des utilisateurs individuels et des citoyens. Toutefois, il convient de développer les capacités de tous ces profils afin de stimuler la demande de données, les cultures de données et l'innovation. Le rôle de la politique dans la promotion de l'utilisation productive des données par les parties prenantes est facilité par les domaines politiques précédents, mais peut également nécessiter des considérations plus spécifiques. Cela est d'autant plus vrai que la réalité des données pour de nombreux acteurs locaux au sein de l'écosystème des données est celle d'une pénurie de données plutôt que d'une saturation.

RECOMMANDATIONS

- Les communautés de données devraient être considérées comme prioritaires dans la politique d'innovation. Ces communautés nécessitent des incitations et un soutien de la politique nationale, y compris la promotion active des pôles de données et d'autres formes d'innovation communautaire qui puissent contribuer à engendrer des compétences et une culture des données, et être soutenues par les acteurs de la société civile de manière plus générale ;
- Les dispositions réglementaires relatives à la gestion des données devraient prévoir des bacs à sable réglementaires pour encourager le développement local des données.

→ **ACTIONS**

- Les communautés de données devraient être intégrées dans les processus d'élaboration des politiques de données par les décideurs politiques ;
- Les communautés de données devraient être associées à la mise en place d'initiatives de données publiques ouvertes par les responsables ministériels de la mise en œuvre ; et
- Les universités devraient être incluses en tant qu'acteurs politiques pertinents pour aider à établir la « base de connaissances » dans laquelle l'économie locale des données peut puiser des connaissances scientifiques et technologiques.

5.4.7 GOUVERNANCE DES DONNÉES POUR LES SECTEURS ET LES CATÉGORIES SPÉCIALES DES DONNÉES

Certaines catégories de données et certains secteurs spécifiques nécessitent une gouvernance des données adaptée qui tienne compte des problèmes particuliers qui affectent cette catégorie ou ce secteur. Les catégories telles que les données sur la santé ou les données sur les enfants ne sont pas les mêmes que les typologies sectorielles telles que les données financières, mais toutes deux peuvent nécessiter un traitement distinct. Toutefois, le traitement spécial crée une menace de silos de données rendant les données moins utilisables et peuvent augmenter les coûts de conformité, en particulier s'il existe des réglementations ou des exigences incompatibles. Un traitement spécial est parfois nécessaire mais doit être en harmonie avec la gouvernance générale des données et ce cadre politique.

Une recommandation clé de l'accès aux données et de l'interopérabilité est que les types de données qui nécessitent une attention particulière doivent être identifiés et clairement spécifiés afin que l'accès spécial et les autres exigences relatives à ces données s'intègrent aux règles générales en matière de données. Comme indiqué dans la section 'Localisation des données', des types de données clairement spécifiés sont parfois soumis à des exigences de localisation des données afin de poursuivre des objectifs politiques propres à ce type de données. Dans les recommandations sur le traitement et la protection des données, il est recommandé que des codes de conduite, soumis à l'approbation de l'autorité nationale chargée de la protection des données, puissent être utilisés pour les exigences spécifiques au secteur.

RECOMMANDATIONS

- Les états membres devraient éviter les régimes de données spéciaux qui ne sont pas intégrés aux régimes de données nationaux et qui n'intègrent pas les principes de bonne gouvernance des données.
- Les mécanismes et les politiques de gouvernance devraient permettre le développement d'une gouvernance des données par catégorie et par secteur pour les données relatives aux enfants, les données relatives à la santé et d'autres types de données sensibles ou de données spécifiques à un secteur qui justifient un traitement distinct par le biais de processus conformes aux principes du cadre.

5.5. GOUVERNANCE INTERNATIONALE ET RÉGIONALE

Au niveau transnational et continental - en particulier pour fournir des capacités de cybersécurité et répondre aux préoccupations en matière de protection des données liées à l'évolution de l'économie des données - la coopération entre les pays revêt une importance croissante. L'étendue de la coopération nécessaire comprend le dialogue entre les gouvernements, la collaboration avec le secteur privé et des processus efficaces et intégrés pour enquêter et poursuivre les violations transfrontalières. Une architecture de confiance mondiale tenant compte des limites des systèmes nationaux existants ou autrement fragmentés est essentielle pour garantir une économie numérique et l'inclusion numérique (Banque africaine de développement, 2019).

Certaines initiatives internationales et continentales servent d'étapes fondatrices pour accélérer la mise en œuvre.

L'Union africaine et les initiatives régionales se concentrent respectivement sur les données génétiques[18] codées numériquement et sur les données géographiques et environnementales. La Commission de l'Union africaine veillera à l'harmonie entre ces initiatives et les travaux en cours sur la politique des données.[19]

RECOMMANDATIONS:

L'Union africaine, avec le soutien des autres organisations panafricaines, devrait :

- faciliter la collaboration entre les différentes entités traitant des données à travers le continent par la mise en place d'un cadre de consultation pour les dialogues politiques au sein de la communauté de l'écosystème numérique afin de préserver l'intérêt de chaque acteur ;
- renforcer les liens avec les autres régions et coordonner les positions communes de l'Afrique sur les négociations internationales liées aux données afin de garantir l'égalité des chances dans l'économie numérique mondiale ;
- soutenir le développement d'infrastructures de données régionales et continentales pour accueillir des technologies avancées axées sur les données (telles que le big data, l'apprentissage automatique et l'intelligence artificielle) ainsi que l'environnement favorable et le mécanisme de partage des données nécessaires pour assurer leur circulation à travers le continent.

5.5.1 NORMES DES DONNÉES CONTINENTALES

Pour faciliter la coopération transfrontalière, il est important de parvenir à un consensus sur les normes de données, partie intégrante de la promotion de l'interopérabilité. Ces formes de consensus multipartites devraient faire référence au travail effectué par l'Organisation internationale de normalisation et à d'autres formes de consensus international obtenues dans des contextes sectoriels spécifiques. Toutefois, si la normalisation internationale est importante pour la compétitivité, il convient de noter que ces normes internationales peuvent ne pas être suffisantes pour les besoins de la région. Ceci est démontré, par exemple, dans le cas des défis linguistiques rencontrés dans le contexte des données spatiales ou géographiques.

18 La catégorie des données génétiques codées numériquement comprend les données génétiques des êtres humains. Lorsqu'il s'agit d'individus identifiables, ces données doivent être considérées comme des données sensibles et traitées conformément à la convention de Malabo. Mais il existe d'autres types de données génétiques codées numériquement qui nécessitent un traitement spécifique/particulier et qui ne sont ni sensibles ni personnelles. Il s'agit notamment des données génétiques démographiques et des données génétiques d'organismes autres que les êtres humains. L'Union africaine collabore actuellement avec d'autres pays parties à la Convention sur la biodiversité (CBD) pour veiller à ce que les données numériques encodées soient traitées comme des ressources biologiques au sens de la CBD. La convention stipule que les ressources biologiques comprennent " les ressources génétiques, les organismes ou éléments de ceux-ci, les populations ou tout autre élément biotique des écosystèmes ayant une utilisation ou une valeur effective ou potentielle pour l'humanité ". La convention régit à la fois l'accès et le partage des avantages afin de permettre la recherche et d'exiger que les personnes qui sont les gardiennes de la biodiversité partagent les avantages de cette recherche. L'application des règles de la convention permettra un flux de données bénéfique tout en garantissant que les Africains en profitent.

19 La stratégie régionale de données pour la gestion des zones marines et côtières en Afrique de l'Ouest promeut une gestion plus durable des ressources naturelles grâce au partage mutuel des données.

RECOMMANDATIONS

- Le consensus sur les normes de données devrait faire référence aux travaux de l'Organisation internationale de normalisation, entre autres forums pertinents ;
- Les normes doivent toutefois être établies avec des réflexions spécifiques sur les facteurs contextuels ayant un impact sur le continent.

→ ACTIONS

- Créer ou habiliter un mécanisme au sein de la CUA pour centraliser les engagements régionaux sur les normes de données.

5.5.2 PORTAIL DE DONNÉES OUVERTES ET AUTRES INITIATIVES

Il existe déjà d'importantes initiatives de données ouvertes centralisées qui devraient continuer à être soutenues au nom d'une économie de données régionale solide. Il s'agit notamment du portail central de données ouvertes de la Banque africaine de développement (*https://dataportal.opendataforafrica.org/*). En outre, il existe des initiatives institutionnelles (voir par exemple : *https://www.datafirst.uct.ac.za/dataportal/index.php/catalog/central/about*) et des communautés de volontaires (voir par exemple : *https://africaopendata.org/*).

5.5.3 INSTRUMENTS CONTINENTAUX

Le large éventail d'instruments pertinents existants est décrit au chapitre 4. Toutefois, deux domaines spécifiques méritent d'être soulignés.

Mécanisme de flux de données transfrontalier

Il est possible de tirer parti de ce cadre pour entamer une collaboration en vue de la mise en place d'un mécanisme régional de circulation transfrontalière des données, facilité par un instrument global, tel que ceux de l'OCDE et de l'ANASE.

Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel

Il est recommandé que la Convention de l'UA soit ratifiée dès que possible afin de servir d'étape fondatrice pour l'harmonisation du traitement des données. Des protocoles additionnels à la Convention devraient également être explorés afin de refléter les changements intervenus depuis la rédaction initiale.

Accord de libre-échange continental africain

La ZLECAf offre la possibilité de coopérer sur un certain nombre d'aspects importants du cadre politique, notamment dans l'élaboration des accords sur la concurrence, la propriété intellectuelle et l'investissement.

RECOMMANDATIONS

- Encourager et faciliter les flux de données au sein des États membres de l'UA et entre eux en élaborant un mécanisme de flux de données transfrontaliers qui tienne compte du contexte africain, à savoir les différents niveaux de préparation au numérique, la maturité des données ainsi que les environnements juridiques et réglementaires.
- Faciliter la circulation des données entre les secteurs et au-delà des frontières en élaborant un cadre commun de catégorisation et de partage des données qui tienne compte des grands types de données et de leurs différents niveaux de confidentialité et de sécurité.
- Travailler en étroite collaboration avec les autorités nationales chargées de la protection des données personnelles des États membres de l'UA, avec le soutien du Réseau africain des autorités (RAPDP), afin d'établir un mécanisme et un organe de coordination qui supervisent le transfert des données personnelles au sein du continent et garantissent le respect des lois et règles existantes en matière de sécurité des données et des informations au niveau national.
- Permettre le partage des données et l'amélioration de l'interopérabilité entre les États membres de l'UA et d'autres mécanismes de l'UA, notamment le mécanisme de coopération policière de l'Union africaine (AFRIPOL).
- Œuvrer à la création d'un cyberespace sûr et résilient sur le continent, qui offre de nouvelles opportunités économiques, par l'élaboration d'une stratégie de cybersécurité de l'UA et la création de centres opérationnels de cybersécurité afin d'atténuer les risques et les menaces liés aux cyberattaques, aux violations de données et à l'utilisation abusive d'informations sensibles.
- Mettre en place des mécanismes et des institutions, ou renforcer ceux qui existent déjà, au sein de l'Union africaine, afin de renforcer les capacités et de fournir une assistance technique aux États membres de l'Union africaine en vue de l'incorporation au niveau national de ce cadre politique en matière de données.
- Il est recommandé que les négociations de la ZLECAf sur le chapitre de la concurrence établissent des normes minimales pour garantir que les données à caractère non personnel putativement exclusives soient accessibles aux innovateurs, aux entrepreneurs et aux autres acteurs de la chaîne de valeur afin d'encourager la concurrence sur le continent.
- Les membres de la ZLECAf devraient envisager d'inclure des dispositions dans le chapitre de la concurrence qui obligent les autorités de la concurrence examinant les questions de structure du marché à prendre également en compte les effets de la structure du marché sur la sécurité et la vie privée. Il est important d'éviter la concentration des courtiers en données ou des plateformes à l'échelle nationale et régionale, car cela crée un risque de défaillance unique ou de quelques points de défaillance aux conséquences considérables.
- Les membres de la ZLECAf devraient également envisager d'inclure des dispositions dans le chapitre de la propriété intellectuelle de la ZLECAf qui clarifient le statut des données par rapport à la propriété intellectuelle, stipulant en particulier :
    - que si le droit d'auteur est étendu aux bases de données et aux compilations de données, il ne s'applique que lorsque les bases de données et les compilations sont créées par des auteurs humains et présentent une originalité et ne s'étend

qu'à la reproduction de la sélection et de la disposition originales des données dans la base de données et non aux données elles-mêmes ;

- que tout droit d'auteur ou autre droit de propriété intellectuelle, y compris les secrets commerciaux, qui permet le contrôle des données ne s'applique pas aux données à caractère personnel ; et
- que tout droit d'auteur ou autre droit de propriété intellectuelle, y compris les secrets commerciaux, qui permet le contrôle des données est limité par les dispositions de la réglementation sur la concurrence.

→ **ACTIONS**

- Les États membres doivent ratifier la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel et élaborer des protocoles supplémentaires, le cas échéant, pour refléter les changements intervenus depuis la rédaction initiale ;
- Établir ou habiliter un mécanisme au sein de la CUA pour centraliser les engagements régionaux sur les normes de données ;
- Une fois adopté, des alignements avec le processus de la ZLECAf devraient immédiatement être explorés ;
- Inclure les questions liées aux données dans les négociations sur les chapitres de la concurrence et de la propriété intellectuelle de la ZLECAf ; et,
- S'accorder sur des critères communs et cohérents pour évaluer l'adéquation des niveaux de protection des données à caractère personnel sur le continent afin de faciliter et de permettre le transfert transfrontalier des données et de normaliser leur protection.

5.5.4 INSTITUTIONS ET ASSOCIATIONS CONTINENTALES ET RÉGIONALES

Les institutions et associations régionales constituent un mécanisme central permettant de créer une voix régionale unifiée sur les questions de données. De nombreuses associations existent déjà, et veiller à ce que la mise en œuvre de ce cadre s'adresse aux associations existantes est une recommandation prioritaire. Les organismes continentaux et régionaux sont particulièrement importants en raison de la nature transfrontalière du flux de données nécessaire pour tirer des bénéfices des données.

Communautés économiques et de développements régionaux

Les communautés économiques régionales, en tant qu'éléments constitutifs de l'Union africaine, peuvent aider les États membres à créer des capacités, à adapter leur politique en matière de données et à parvenir à un consensus sur l'harmonisation de cette politique, à participer à l'élaboration de normes et à permettre la circulation des données.

Arbitres en matière de droits de l'homme

La Cour africaine des droits de l'homme et des peuples, la Cour de justice de l'Afrique de l'Est et la Cour de justice de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) offrent des forums et des capacités qualifiées pour trancher des litiges complexes sur la vie privée et l'égalité, qui sont pertinents pour la protection des données à caractère personnel et l'utilisation des données à des fins de discrimination injuste.

Le Tribunal de la SADC, une fois habilité pourrait également offrir un forum pour les différends relatifs aux données, bien que dans le cadre d'un mandat plus limité. Les mécanismes d'arbitrage continentaux et régionaux sont les mieux placés pour résoudre les différends transfrontaliers en matière de données.

Réseau africain des régulateurs de données

Donner des moyens d'action aux APD et améliorer le niveau d'application des cadres législatifs et réglementaires au niveau national aident considérablement les individus à jouir de leurs droits numériques. La promotion et le soutien des associations existantes, telles que le Réseau africain des Autorités de Protection des données, constituent également un moyen de renforcer ces capacités.

Associations d'autorités de régulation des TIC

Il existe des associations régionales des régulateurs en matière des TIC (ARTAC, WATRA, CRASA et EACO) qui constituent d'importants mécanismes d'apprentissage par les pairs en matière d'association transfrontalière. Elles peuvent également faciliter la collaboration et le partage des connaissances au fur et à mesure que les instruments et les normes transfrontaliers sont explorés.

Associations sectorielles

Des associations sectorielles, telles que le Forum africain de l'administration fiscale, devront contribuer à la réalisation des recommandations relatives à l'économie des données en particulier. Compte tenu de l'importance de l'identité numérique dans l'économie des données, l'Association des bureaux d'enregistrement nationaux est également importante.

Forum africain de la concurrence

Le Forum africain de la concurrence (FAC) se décrit comme « un réseau informel d'autorités nationales et multinationales africaines de la concurrence ». Le FAC peut créer des capacités pour les autorités de la concurrence afin de mieux réglementer les questions liées aux données.

RECOMMANDATIONS

- Renforcer la coopération réglementaire et le partage des connaissances entre les pays et régions d'Afrique en renforçant les capacités au Réseau africain des autorités de protection des données et des Associations régionales des régulateurs des TIC.
- Les mécanismes d'arbitrage continentaux et régionaux existants devraient être explicitement habilités à traiter les questions relatives aux données qui sont impliquées dans les droits numériques et les droits sur les données, ainsi que les litiges transfrontaliers sur les données.
- Les autorités fiscales africaines devraient collaborer par le biais du Forum africain de l'administration fiscale (ATAF) pour élaborer une position africaine afin de représenter plus efficacement l'intérêt commun dans le processus de réforme de la fiscalité internationale, comme l'érosion de la base de l'impôt et le transfert de bénéfices (BEPS).
- Mettre en place un Forum annuel d'innovation des données pour l'Afrique qui servira de plateforme pour des discussions multipartites, facilitera les échanges entre les Pays et sensibilisera les décideurs politiques sur le potentiel des données comme moteur de l'économie numérique actuelle.

5.6. CADRE DE MISE EN ŒUVRE

5.6.1 CADRE DE MISE EN ŒUVRE PAR ÉTAPES

Il convient de noter que si les domaines d'activité ci-dessous sont identifiés par phases, leur réalisation n'est pas strictement linéaire. En particulier, les phases 2 et 3 sont considérées comme des processus simultanés, qui peuvent se dérouler parallèlement aux activités d'incorporation au niveau national. Le cadre de mise en œuvre doit être lu conjointement avec la cartographie des parties prenantes décrite au point 5.6.2.

	Activité	Description	Principal Acteur
PHASE 1 : ADOPTION DU CADRE			
A	Les États membres adoptent le cadre stratégique		États membres
B	Conception du cadre de suivi	Mise en place d'un cadre de suivi de haut niveau	CUA
C	Établir ou habiliter un mécanisme au sein de l'UA pour centraliser les engagements régionaux en matière de données.	Les activités doivent inclure un soutien à la mise en œuvre, la coordination sur les normes de données et d'autres domaines spécifiques énoncés dans les recommandations nécessitant une collaboration régionale	CUA
PHASE 2 : APPROPRIATION			
A	Évaluer le cadre continental	Assurer l'alignement sur les instruments continentaux.	CUA, CER, AUDA-NEPAD Smart Africa.
B	Engagement des structures continentales	Engager les structures associées sur les domaines potentiels de collaboration dans la mise en œuvre du cadre.	CUA
C	Évaluation des cadres internationaux	En se concentrant sur les principes, explorer l'alignement avec les cadres des structures internationales.	CUA
D	Mobilisation des structures internationales		CUA, États membres de l'UA

	Activité	Description	Principal Acteur
PHASE 3 : SOUTIEN CONTINENTAL AUX ÉTATS MEMBRES POUR REMPLIR LES CONDITIONS PREALABLES			
A	Développement d'infrastructures à large bande et des cadres réglementaires	Mise en œuvre d'une politique plus large initiée par rapport à l'environnement de données au niveau national.	CERs, AUDA-NEPAD, ATU,-PAPU, SMART AFRICA
PHASE 4 : DOMESTICATION			
A	Engagement multipartite	En s'appuyant sur le cadre stratégique, impliquer tous les acteurs au niveau national	États membres, secteur privé, société civile,
B	Favoriser l'adhésion multipartite	En se référant à la cartographie des parties prenantes dans la Phase Deux*, assurer l'alignement des politiques.	États membres
C	Incorporer l'instrument dans les cadres nationaux	Élaborer des cadres juridiques et réglementaires, établir des régulateurs des données et des systèmes de gouvernance des données.	États membres
D	Cadre budgétaire	Allouer des ressources pour la mise en œuvre	États membres
PHASE 5 : COLLABORATION			
A	Implication dans les forums internationaux de prise de décision	Participer à des forums d'élaboration de règles et de normes en matière de données (voir la cartographie des parties prenantes).	États membres de l'UA
B	Suivi de la mise en œuvre des membres		CUA, CERs, AUDA-NEPAD, Smart Africa
C	Sensibiliser sur le mécanisme continental de centralisation des initiatives en matière de données.	Accepter les demandes directes d'assistance	CUA, Institutions Régionale
D	Participer aux activités continentales	Participer aux activités continentales décrites dans la section 10.	États membres

5.6.2 CARTOGRAPHIE DES PARTIES PRENANTES

Une cartographie sommaire des parties prenantes est fournie pour faciliter la mise en œuvre, en particulier aux phases 2, 4 et 5.

DESCRIPTION	SOUS-TYPES	OBJECTIF
INTERNATIONAL		
Nations Unies	Union Internationale des Télécommunications, Département de la sûreté et de la sécurité des Nations Unies	Alignement de la politique de développement
Organisations multilatérales	Organisation de coopération et de développement économiques, Banque mondiale	Alignement de la politique économique
Structures de gouvernance de l'Internet	Forum sur la gouvernance de l'Internet, Groupe de travail sur l'ingénierie Internet, Internet Corporation for Assigned Names and Numbers (ICANN)	Alignement des politiques numérique et Internet
Normes internationales	Organisation internationale de normalisation	Alignement des normes en matière de des données
Organisations multilatérales (sectorielles)	Organisation mondiale de la santé, Organisation mondiale du commerce	Alignement des composantes sectorielles de la politique
REGIONAL		
Communautés économiques régionales	CEDEAO, SADC, CAE, CEEAC, COMESA, IGAD, CEN-SAD, UMA,	Alignement des politiques économiques et du développement
Structures de gouvernance de l'Internet	AFRINIC, IGF Africain	Alignement des politiques numérique et Internet
Réseau communautaire (régulateurs)	Réseau Africain des autorités de protection des données, autres associations de régulateurs, Forum de l'administration fiscale africaine	Alignement des politiques intersectorielles et transfrontalières
Communauté régionale (sectorielle)	Banque africaine de développement	Alignement des composantes sectorielles de la politique en matière de données

DESCRIPTION	SOUS-TYPES	OBJECTIF
NATIONAL		
Départements nationaux	Télécommunications, Justice, Coopération internationale	Alignement des politiques en matière de donnes
Agences statistiques		Habilitation
Autorités de régulation	Protection des données, Réglementation des TIC, règlementation de la concurrence	Mise en œuvre
Au niveau de l'entreprise	Comités de gouvernance des données	Habilitation, engagement multipartite

RECOMMANDATIONS

Suite à l'approbation du cadre Stratégique en matière de données par les organes de l'UA, la Commission de l'UA, en collaboration avec les institutions régionales et les parties prenantes concernées, élaborera un plan d'action pour guider la mise en œuvre du cadre en prenant en compte la souveraineté numérique des États ainsi que les différents niveaux de développement, la vulnérabilité des populations et la numérisation au sein des États membres de l'UA, notamment les aspects liés au manque d'infrastructures TIC et l'absence de politiques et de législations en matière de cybersécurité. Le plan d'action (à court, moyen et long terme) identifiera les rôles et les responsabilités et mettra l'accent sur les priorités clés et les actions immédiates tant au niveau régional qu'au niveau continental, en fonction des niveaux de maturité des données des États membres de l'UA.

RÉFÉRENCES

African Development Bank. (2019). Annual Report 2019 | African Development Bank—Building today, a better Africa tomorrow. https://www.afdb.org/en/documents/annual-report-2019

Ahmed, S. (2021). A Gender perspective on the use of Artificial Intelligence in the African Fin-Tech Ecosystem: Case studies from South Africa, Kenya, Nigeria, and Ghana. 23rd ITS Biennial Conference. https://www.econstor.eu/handle/10419/238000?author_page=1

Andreoni, A., & Tregenna, F. (2020). Escaping the middle-income technology trap: A comparative analysis of industrial policies in China, Brazil and South Africa. Structural Change and Economic Dynamics, 54, 324-340. https://doi.org/10.1016/j.strueco.2020.05.008

Arntz, M., Gregory, T., & Zierahn, U. (2016). The Risk of Automation for Jobs in OECD Countries. https://www.oecd-ilibrary.org/content/paper/5jlz9h56dvq7-en

Ballell, T. R. de las H. (2019). Legal challenges of artificial intelligence: Modelling the disruptive features of emerging technologies and assessing their possible legal impact. Uniform Law Review, 24(2), 302–314. https://doi.org/10.1093/ulr/unz018

Carrière-Swallow, Y., & Haksar, V. (2019). The Economics and Implications of Data: An Inte- grated Perspective (No. 19/16). https://www.imf.org/en/Publications/Departmental-Papers-Pol- icy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Per-spective-48596

Cavoukian, A. (2009). Privacy by design. The 7 foundational principles. Implementation and mapping of fair information practices. Information and Privacy Commissioner.

CNUCED. (2020). Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

CNUCED. (2021). Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow [United Nations publication].

Cory, N. (2017). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Infor- mation Technology and Innovation Foundation. https://itif.org/publications/2017/05/01/cross- border-data-flows-where-are-barriers-and-what-do-they-cost

Couldry, N., & Mejias, U. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. SAGE Publications. https://eprints.lse.ac.uk/89511/1/Couldry_Data-colonialism_Accepted.pdf

Deloitte. (2017). Privacy is Paramount | Personal Data Protection in Africa Personal Data Pro- tection in Africa. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

Gillwald, A., & Mothobi, O. (2019). After Access 2018: A Demand-Side View of Mobile Internet From 10 African Countries (After Access 2018: A Demand-Side View of Mobile Internet from 10 African Countries After Access: Paper No. 7 (2018); Policy Paper Series No. 5). Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf

Global Symposium for Regulators. (2020). the Regulatory Wheel of Change: Regulation for Digital Transformation. ITU. https://www.itu.int:443/en/ITU-D/Conferences/GSR/2020/Pages/default.aspx

Hawthorne, S. (2020). Impact of Internet Connection on Gifted Students' Perceptions of Course Quality at an Online High School. Boise State University Theses and Dissertations. https://doi.org/10.18122/td/1748/boisestate

Information Society. (2018). Personal Data Protection Guidelines for Africa. A joint initiative of the Internet Society and the Commission of the African Union. https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

International Telecommunication Union. (2019). Measuring Digital Development Facts and Figures (978-92-61-29511-0). https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

International Telecommunication Union. (2020). the Regulatory Wheel of Change: Regulation for Digital Transformation. ITU. https://www.itu.int:443/en/ITU-D/Conferences/GSR/2020/Pages/default.aspx

Jones, C., & Tonetti, C. (2020). Nonrivalry and the Economics of Data. The American Economic Review, 110(9), 2819–2858. https://doi.org/10.1257/aer.20191330

Khan, M., & Roy, P. (2019). Digital identities: A political settlements analysis of asymmetric power and information. https://eprints.soas.ac.uk/32531/1/ACE-WorkingPaper015-DigitalIdentities-191004.pdf

Macmillan, R. (2020). Data Governance: Towards a Policy Framework (Policy Brief No. 9). https://www.competition.org.za/ccred-blog-digital-industrial-policy/2020/7/6/data-governance-towards-a-policy-framework

Mazzucato, M., Entsminger, J., & Kattel, R. (2020). Public Value and Platform Governance (SSRN Scholarly Paper ID 3741641). Social Science Research Network. https://doi.org/10.2139/ssrn.3741641

Mitretodis, & Euper. (2019). Interaction Between Privacy and Competition Law in a Digital Economy. Competition Chronicle. https://www.competitionchronicle.com/2019/07/interaction-between-privacy-and-competition-law-in-a-digital-economy/

Nicholas, G., & Weinberg, M. (2019). Data Portability and Platform Competition: Is User Data Exported From Facebook Actually Useful to Competitors? | NYU School of Law. New York University School of Law. https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition

OCDE. (2019). Data governance in the public sector. 23–57. https://doi.org/10.1787/9cada708-en

Open Data Charter. (2015). Open Data Charter Principles. Open Data Charter. https://open- datacharter.net/principles/

Polatin-Reuben, D., & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.902.7318&rep=rep1&type=pdf#:~:text=Weak%20data%20sovereignty%20as%20defined,on%20safeguard%2D%20ing%20national%20security.

Razzano, G., Gillwald, A., Aguera, P., Ahmed, S., Calandro, E., Matanga, C., Rens, A., & van der Spuy, A. (2020). SADC Parliamentary Forum Discussion Paper: The Digital Economy and Society. Research ICT Africa. https://researchictafrica.net/publication/sadc-pf-discussion-paper-the-digital-economy-and-society/

Rinehart, W. (2020, September 14). Is data nonrivalrous? Medium. https://medium.com/cgo-benchmark/is-data-nonrivalrous-f1c8e720820b

Saint, M., & Garba, A. (2016). Technology and Policy for the Internet of Things in Africa (SSRN Scholarly Paper ID 2757220). Social Science Research Network. https://doi.org/10.2139/ssrn.2757220

Savona, M. (2019). The Value of Data: Towards a Framework to Redistribute It (SSRN Scholarly Paper ID 3476668). Social Science Research Network. https://doi.org/10.2139/ssrn.3476668

Schmidt, C. O., Struckmann, S., Enzenbach, C., Reineke, A., Stausberg, J., Damerow, S., Huebner, M., Schmidt, B., Sauerbrei, W., & Richter, A. (2021). Facilitating harmonized data quality assessments. A data quality framework for observational health research data collections with software implementations in R. BMC Medical Research Methodology, 21(1), 63. https://doi.org/10.1186/s12874-021-01252-7

Sen, A. (2001). Development As Freedom. OUP Oxford; eBook Collection (EBSCOhost). http://ezproxy.uct.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2089308&site=ehost-live

Stork, C., & Gillwald, A. (2012). South Africa's mobile termination rate debate: What the evidence tells us (Policy Brief No. 2; South Africa). Research ICT Africa. https://researchictafrica.net/publications/Country_Specific_Policy_Briefs/South_Africa_Mobile_Termination_Rate_Debate_-_What_the_Evidence_Tells_Us.pdf

Taylor, L. (2019). Global data justice. Communications of the ACM, 62(6). https://doi.org/10.1145/3325279

Teh, H., Kempa-Liehr, A., & Wang, K. (2020). Sensor data quality: A systematic review. Journal of Big Data, 7. https://doi.org/10.1186/s40537-020-0285-1

United Nations. (2017). Looking to future, UN to consider how artificial intelligence could help achieve economic growth and reduce inequalities—United Nations Sustainable Development. https://www.un.org/sustainabledevelopment/blog/2017/10/looking-to-future-un-to-consider-how-artificial-intelligence-could-help-achieve-economic-growth-and-reduce-inequalities/

van der Spuy, A. (2021, February 23). How do we protect children's rights in a digital environment only available to some? African Post. https://researchictafrica.net/2021/02/23/how-do-we-protect-childrens-rights-in-a-digital-environment-only-available-to-some/

Wang, Y., McKee, M., Torbica, A., & Stuckler, D. (2019). Systematic Literature Review on the Spread of Health-related Misinformation on Social Media. Social Science & Medicine, 240, 112552. https://doi.org/10.1016/j.socscimed.2019.112552

Wook, M., Hasbullah, N. A., Zainudin, N. M., Jabar, Z. Z. A., Ramli, S., Razali, N. A. M., & Yusop,

N. M. M. (2021). Exploring big data traits and data quality dimensions for big data analytics application using partial least squares structural equation modelling. Journal of Big Data, 8(1), 49. https://doi.org/10.1186/s40537-021-00439-5

World Bank. (2021). Data for Better Lives. World Bank. Doi : 10.1596/978-1-4648-1600-0

World Bank, & ITU. (2020). The World Bank and International Telecommunication Union launch handbook on digital regulation [Text/HTML]. World Bank. https://www.worldbank.org/en/news/feature/2020/09/08/the-world-bank-and-international-telecommunication-union-launch-handbook-on-digital-regulation

World Economic Forum. (2016). Networked Readiness Index. Global Information Technology Report 2016. http://wef.ch/29cCKbU

Zuboff, S. (2018). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Penguin Publishing Group. https://antipodeonline.org/wp-content/uploads/2019/10/Book-review_Whitehead-on-Zuboff.pdf

ANNEXE - DÉFINITIONS PRATIQUES

Anonymisation : suppression des identifiants personnels directs et indirects des données.

Autorités de protection des données (APD) : autorités publiques indépendantes qui contrôlent et supervisent, grâce à des pouvoirs d'enquête et de correction, l'application de la loi sur la protection des données. Elles fournissent des conseils d'experts sur les questions liées à la protection des données et traitent les plaintes qui pourraient avoir enfreint la loi.

Capacité numérique : compétences, alphabétisation, normes sociales et attitudes dont les individus et les organisations ont besoin pour prospérer, pour vivre, apprendre et travailler dans une société et une économie numériques.

Classification des données : désigne généralement le processus d'organisation des données par catégories pertinentes afin de pouvoir les utiliser et les protéger plus efficacement.

Commerce électronique : transactions commerciales effectuées par des canaux électroniques qui permettent d'acheter et de vendre des biens ou des services via l'internet, ainsi que le transfert d'argent et de données pour réaliser les ventes - par des méthodes spécifiquement conçues pour recevoir ou passer des commandes.

Consentement de la personne concernée : désigne toute volonté librement exprimée, spécifique, informée et univoque de la personne concernée par laquelle celle-ci, par une déclaration ou par un acte positif clair, manifeste son accord au traitement des données à caractère personnel la concernant.

Continental : désigne l'Afrique dans le présent cadre.

Cybercriminalité : actes illicites qui portent atteinte à la confidentialité, à l'intégrité, à la disponibilité et à la survie des systèmes de technologies de l'information et de la communication, aux données qu'ils traitent et à l'infrastructure de réseau sous-jacente (Convention de Malabo).

Cybersécurité : ensemble des technologies, processus et pratiques conçus pour protéger les réseaux, les dispositifs, les programmes et les données contre les attaques, les préjudices ou les accès non autorisés. (*https://digitalguardian.com/blog/what-cyber-security*)

Données à caractère personnel : toute information relative à une personne physique identifiée ou identifiable par laquelle cette personne peut être identifiée, directement ou indirectement notamment par référence à un numéro d'identification ou à plusieurs éléments spécifiques à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Donnéification : processus par lequel les interactions quotidiennes des êtres vivants peuvent être rendues sous forme de données et utilisées à des fins sociales et économiques.

Données ouvertes : ouvert signifie que tout le monde peut librement y accéder, les utiliser, les modifier et les partager à toutes fins (sous réserve, tout au plus, d'exigences préservant la provenance et l'ouverture. (*http://opendefinition.org/*)

Données sensibles : désigne toutes les informations personnelles relatives aux opinions religieuses, philosophiques et politiques ainsi qu'à la vie sexuelle, la race, la santé et les conditions sociales de la personne concernée (Convention de Malabo).

Écosystème de données : aux fins du présent document, il s'agit non seulement des langages de programmation, des progiciels, des algorithmes, des services informatiques en nuage et de l'infrastructure générale qu'une organisation utilise pour recueillir, stocker, analyser et exploiter des données, mais aussi de la chaîne de valeur sous-jacente associée aux données en tant que facteur de production, de la gouvernance des systèmes de données et de la protection des personnes concernées.

Harmonisation : fait d'assurer l'uniformité des systèmes par l'utilisation de normes minimales pour faciliter l'interopérabilité et de cadres juridiques et de confiance (par ex. pour les niveaux d'assurance) en vue de définir des règles et d'instaurer la confiance dans les systèmes respectifs.

Identité numérique : ensemble d'attributs et/ou de renseignements d'identification saisis et stockés électroniquement, qui identifient une personne de manière unique et permettent de distinguer un individu d'un autre.

Infrastructure des données fondamentales : technologies avancées qui facilitent l'utilisation intensive de données de qualité. Il peut s'agir de réseaux à large bande, de centres de données et de services en nuage, de matériel et de logiciels électroniques, ainsi que d'applications numériques disponibles sur l'internet.

Interopérabilité : capacité de différentes unités fonctionnelles - par ex., des systèmes, des bases de données, des dispositifs ou des applications - à communiquer, à exécuter des programmes ou à transférer des données d'une manière qui exige que l'utilisateur ait peu ou pas de connaissances de ces unités fonctionnelles (adapté de la norme ISO/CEI 2382 :2015).

Minimisation des données : principe des cadres de protection des données qui prévoit la collecte de la quantité minimale des données à caractère personnel nécessaires pour la prestation d'un élément individuel d'un service ou d'un produit.

Niveau d'assurance (LOA) : capacité à déterminer, avec un certain degré de certitude ou d'assurance, que la revendication d'une identité particulière par une personne ou une entité peut être considérée comme la «véritable» identité du demandeur (coopération public-privé ID4D). Le niveau global d'assurance est fonction du degré de confiance dans le fait que l'identité revendiquée par le demandeur est sa véritable identité (un niveau d'assurance de l'identité ou IAL), de la force du processus d'authentification (un niveau d'assurance de l'authentification ou AAL), et - en cas d'utilisation d'une identité fédérée - du protocole d'assertion utilisé par la fédération pour communiquer les informations d'authentification et d'attribut (un niveau d'assurance de la fédération ou FAL) (adapté de NIST 800- 63:2017).

Normes ouvertes : normes mises à la disposition du grand public et sont développées (ou approuvées) et maintenues via un processus collaboratif et consensuel. Les normes ouvertes facilitent l'interopérabilité et l'échange de données entre différents produits ou services et sont destinées à être largement adoptées (adopté de l'UIT-T).

Personnes concernées : toute personne physique qui fait l'objet d'un traitement de données à caractère personnel (Convention de Malabo).

Protection des données : consiste à réglementer la manière dont les données sont utilisées ou traitées et par qui, et à garantir aux citoyens des droits sur leurs données. Elle est particulièrement importante pour garantir la dignité numérique, car elle permet de remédier directement au déséquilibre de pouvoir inhérent entre les «personnes concernées» et les institutions ou les personnes qui ont collecté les données.

Pseudonymisation : traitement des données de manière qu'elles ne puissent être associées à un individu sans informations supplémentaires.

Régional : Aux fins du présent cadre, le terme « régional » fait référence aux cinq régions d'Afrique reconnues par l'Union africaine.

Respect de la vie privée et la sécurité dès la conception : méthodes consistant à intégrer de manière proactive des mécanismes de respect de la vie privée et de sécurité dans la conception et le fonctionnement des produits et services, qu'il s'agisse de systèmes informatiques ou non, d'infrastructures en réseau ou de pratiques commerciales. Cela exige que la gouvernance de la vie privée et de la sécurité soit prise en compte tout au long du processus d'ingénierie et du cycle de vie du produit.

Responsable du traitement des données : toute personne physique ou morale, publique ou privée, toute autre organisation ou association qui, seule ou conjointement avec d'autres, décide de collecter et de traiter des données à caractère personnel et en détermine les finalités.

Services en nuage : applications grand public (c'est-à-dire les médias sociaux et le courrier électronique proposés sur Internet), dans lesquelles les données ne se trouvent pas sur les appareils des individus mais sont stockées à distance dans un centre de données. Les exemples incluent Facebook, YouTube et Gmail.

Services en nuage : les services en nuages sont utilisés à la demande, à tout moment, via n'importe quel réseau d'accès, à l'aide de n'importe quel appareil connecté qui utilise les technologies de l'informatique en nuage, ils utilisent des logiciels et des applications qui se trouvent dans le nuage et non sur les appareils des utilisateurs.

Department of Infrastructure and Energy
African Union Headquaters
P.O. Box 3243, Roosevelt Street
W21K19, Addis Ababa, Ethiopia
Tel: +251 (0) 11 551 77 00
Fax: +251 (0) 11 551 78 44
www.au.int