

DOCUMENT DE RÉFLEXION No. 379

Flux de données transfrontaliers en Afrique : ambitions continentales et réalités politiques

Par Melody Musoni, Poorva Karkare et Chloe Teevan

Novembre 2024

L'Afrique doit donner la priorité à l'utilisation des données et au partage transfrontalier des données pour atteindre les objectifs de la Zone de libre-échange continentale africaine et pour stimuler l'innovation et le développement de l'IA. Des données accessibles et partageables sont essentielles à la croissance et au succès de l'économie numérique, ouvrent la voie à des innovations et à des opportunités économiques, surtout dans un paysage en évolution rapide.

Les pays africains, par l'intermédiaire de l'Union africaine (UA), ont une vision commune du partage des données par-delà les frontières afin de stimuler la croissance économique. Il se fait cependant que les politiques numériques continentales qui ont été adoptées sont souvent appliquées de manière incohérente au niveau national, où certains États membres mettent en œuvre des mesures restrictives qui limitent la libre circulation des données – la localisation des données notamment.

Le document examine des politiques nationales qui donnent souvent la priorité aux intérêts nationaux et entrent de ce fait en conflit avec les objectifs continentaux. Cela s'explique par des différences dans les idéologies politiques, les conditions socio-économiques, les préoccupations en matière de sécurité et de priorités économiques. Ce décalage entre les agendas nationaux et la stratégie plus large de l'UA est façonné par un contexte propre à chaque pays, comme le montrent les exemples du Sénégal, du Nigeria et du Mozambique, qui sont confrontés à des défis distincts dans la mise en œuvre de la vision continentale.

Le document se termine par des recommandations qui pourraient être appliquées par l'UA, les États membres et le partenariat avec l'Union européenne. Il suggère que l'UA renforce son soutien aux initiatives de partage des données et invite les États membres à se concentrer sur l'alignement des politiques, à pallier les lacunes en matière de données, à mettre en place des infrastructures de données et à trouver de nouvelles façons d'utiliser les données. Il met également en évidence les voies et moyens par lesquels l'UE peut renforcer son soutien aux objectifs de l'Afrique en matière de partage des données.

Table des matières

Glossaire.....	iii
Remerciements.....	iv
Sigles et acronymes.....	iv
Résumé analytique	vi
1. Introduction	1
2. Vision continentale des FDT.....	3
2.1. Instruments politiques de l'UA visant à promouvoir les FDT	3
2.2. Instruments politiques régionaux visant à promouvoir les FDT.....	7
2.3. Lacunes des instruments continentaux.....	8
2.3.1. Un champ d'application large	8
2.3.2. L'accent est mis sur les données à caractère personnel.....	9
2.3.3. Un manque d'orientations	9
2.3.4. Les intérêts ou contextes africains ne sont pas reflétés.....	10
3. De la vision continentale à la mise en œuvre nationale.....	11
3.1. Approches nationales en matière de flux de données	11
3.2. La façon dont sont définies les priorités de la politique nationale en matière de données.....	15
3.2.1. Une vision nationale conditionnée par des intérêts économiques et politiques ...	15
3.2.2. Influence extérieure et dépendance de trajectoire.....	16
3.2.3. Discussions cloisonnées et accords sectoriels fragmentés	17
3.3. Défis dans la mise en œuvre	18
3.3.1. Une mauvaise coordination nationale, à l'origine de mandats concurrents et d'incitations aux effets pervers.....	18
3.3.2. Une mauvaise gouvernance des données et des mécanismes peu clairs	19
3.3.3. Une mise en application limitée	19
4. Ce qu'il faut retenir des divergences entre les perspectives continentales et nationales en matière de flux de données	20
4.1. Des intérêts nationaux en concurrence avec les engagements pris au niveau continental.....	21
4.2. Influence extérieure	21
4.3. De longues négociations au niveau continental qui entraînent un manque d'alignement.....	22
4.4. Une coordination inefficace.....	22

4.5.	Pas de véritables répercussions pour les États membres de l'UA.....	22
4.6.	Données lacunaires et faible demande de FDT	23
5.	Mesures stratégiques pour renforcer les FDT en Afrique	23
5.1.	Recommandations politiques en direction de l'UA.....	23
5.1.1.	Établir un cadre de catégorisation et de partage des données pour les FDT.....	23
5.1.2.	Renforcer la capacité de mise en œuvre et de mise en application	24
5.1.3.	Créer une task force ou un groupe de travail sur l'OCPD.....	24
5.1.4.	Faciliter l'apprentissage entre pairs entre les États membres	24
5.2.	Recommandations politiques en direction des États membres de l'UA.....	24
5.2.1.	Gouvernance.....	24
5.2.2.	Facteurs favorables.....	26
5.2.3.	Capacités et compétences	26
5.2.4.	Utilisation des données	27
6.	Quel rôle l'UE peut-elle jouer pour soutenir les flux de données transfrontaliers en Afrique ?.....	28
6.1.	Contexte : la Stratégie européenne pour les données.....	28
6.2.	L'Action pour une gouvernance des données en Afrique subsaharienne	29
6.3.	Recommandations en direction de l'UE.....	30
6.3.1.	Gouvernance.....	30
6.3.2.	Infrastructures	31
6.3.3.	Cas d'utilisation.....	32
	Références	33

Liste des tableaux

Tableau 1 :	Aperçu des politiques numériques continentales.....	4
Tableau 2 :	Aperçu des politiques des CER relatives aux FDT.....	7
Tableau 3 :	Aperçu des politiques nationales dans les pays choisis pour cette étude.....	12

Glossaire

Donnée:	Information sous forme numérique et non numérique qui peut être un ensemble de différents types (confidentielle, à caractère personnel ou non, big data) provenant de différents secteurs (soins de santé, éducation, météorologie) et se trouvant à différents niveaux (par exemple, les données économiques peuvent se situer au niveau macro, sectoriel, de l'entreprise ou de l'individu).
Donnée à caractère personnel :	Toute information se rapportant directement ou indirectement à une personne vivante identifiée ou identifiable (par exemple : noms, adresses, comptes bancaires, identifiants en ligne, données génétiques, données physiologiques, données de localisation, etc.)
Donnée à caractère non personnel :	Toute information qui ne se réfère pas à une personne physique identifiée ou identifiable, ou une donnée initialement à caractère personnel mais rendue anonymisée par la suite.
Souveraineté numérique :	L'autorité ou les pouvoirs exercés par les gouvernements, généralement par le biais de politiques et de lois, sur l'infrastructure numérique, les données, les activités dans le cyberspace, y compris le contrôle des activités de leurs administrés dans le cyberspace.
Localisation des données :	Il n'existe pas de définition unique, mais il s'agit des lois et des mesures prises par les gouvernements pour restreindre le mouvement des données par-delà les frontières nationales ou limiter les endroits où les données sont stockées et par qui. Ces restrictions sont de nature variable : strictes, conditionnelles ou laissant le champ ouvert aux transferts.
Flux de données transfrontalier :	Le mouvement ou le transfert de données (à caractère personnel ou non) par-delà les frontières d'un pays, généralement par des moyens électroniques.
Valorisation des données :	Utiliser les données pour développer des solutions qui peuvent résoudre les problèmes du monde réel et promouvoir le développement durable (analyser les big data, par exemple, afin de déterminer les allocations de ressources nécessaires en vue d'améliorer la prestation de services).

Remerciements

Ce projet a été financé par la Commission européenne. L'équipe de base était également composée de Sérgio Luis Cossa et de Talla Ndiaye, qui ont fourni des informations et des détails précieux sur les cadres politiques du Mozambique pour l'un, et du Sénégal pour l'autre. Sara Giancesello, collaboratrice de l'ECDPM, a fait partie de l'équipe qui s'est rendue sur le terrain au Sénégal, et Nneka Okechukwu a contribué à préparer [l'infographie montrant l'état des lieux des politiques relatives aux données transfrontalières dans les pays africains](#). Bruce Byiers a apporté des commentaires utiles aux versions antérieures de ce rapport afin de rapprocher la question des politiques numériques de l'agenda de l'intégration régionale en Afrique. Ce rapport a également bénéficié de la mise en page et de l'assistance éditoriale de plusieurs autres collègues de l'ECDPM. Les auteurs tiennent à remercier les nombreux experts et décideurs politiques qui ont partagé leurs idées tout au long du processus de recherche. La version française de ce rapport a été traduite par Patrice Deladrier. Les auteurs assument la responsabilité de toute erreur factuelle. Pour tout retour d'information ou toute suggestion concernant de futurs travaux, veuillez contacter mmu@ecdpm.org, pk@ecdpm.org et cte@ecdpm.org.

Sigles et acronymes

ACEUM	Accord Canada-États-Unis-Mexique
ADE	Agence nationale pour le développement géospatial
AGD	Acte européen sur la gouvernance des données
ANSD	Agence nationale de la statistique et de la démographie
AUDA NEPAD	Agenda de développement de l'Union africaine
	Nouveau partenariat pour le développement de l'Afrique
BMZ	Bundesministerium für Wirtschaftliche Zusammenarbeit (Ministère fédéral allemand de la coopération économique et du développement)
CAE	Communauté de l'Afrique de l'Est
CBN	Banque centrale du Nigeria
CDP	Commission des données personnelles
CEDEAO	Communauté économique des États de l'Afrique de l'Ouest
CEEAC	Communauté économique des États de l'Afrique centrale
CEMAC	Communauté économique et monétaire de l'Afrique centrale
CER	Communauté économique régionale
CGIAR	Groupe consultatif pour la recherche agricole internationale
CNBB	Centre national de biotechnologie et des sciences biologiques
COVID-19	Maladie à coronavirus 2019
CPLP	Communauté des pays lusophones

CSD	Cadre stratégique de l'UA en matière de données
CSIRT	Équipes d'intervention en cas d'incident affectant la sécurité informatique
CUA	Commission de l'Union africaine
DPA	Autorité en charge de la protection des données
FDT	Flux de données transfrontaliers
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (Association allemande pour la coopération internationale)
IA	Intelligence artificielle
INAGE	Institut national de l'administration en ligne
INAM	Institut national de météorologie
INCM	Institut national des communications du Mozambique
INTIC	Institut national des technologies de l'information et de la communication
MUN	Marché unique numérique
NDPA	Loi nigériane sur la protection des données
NDPC	Commission nigériane sur la protection des données
NDPR	Règlement nigérian sur la protection des données
NIMC	Commission nationale de gestion de l'identité
NITDA	Agence nigériane de développement des technologies de l'information
OCDE	Organisation de coopération et de développement économiques
OCPD	Organe continental de protection des données
OFESA	Observatoire des forêts d'Afrique de l'Est et australe
PCN	Protocole sur le commerce numérique pour l'Afrique
PIB	Produit intérieur brut
RAPDP	Réseau africain des autorités de protection des données personnelles
RDC	République démocratique du Congo
RGPD	Règlement général sur la protection des données
SADC	Communauté de développement de l'Afrique australe
TIC	Technologies de l'information et de la communication
UA	Union africaine
UE	Union européenne
UEMOA	Union économique et monétaire ouest-africaine
UNECA	Commission économique pour l'Afrique des Nations unies
ZLECAf	Zone de libre-échange continentale africaine

Résumé analytique

Les données sont essentielles à l'économie numérique dans son ensemble et constituent l'épine dorsale d'une industrie de l'Intelligence Artificielle (IA) en pleine évolution. On les retrouve à différents niveaux (les données économiques, par exemple, peuvent se situer au niveau macroéconomique, sectoriel, de l'entreprise ou de l'individu), dans différents secteurs (les soins de santé, l'éducation, l'agriculture, la météorologie, etc.) et sous de multiples formes (confidentielles, à caractère personnel ou non, big data, données ouvertes, etc.). Le partage et l'utilisation des données favorisent la croissance économique, la concurrence, la recherche et les avancées scientifiques (surtout les innovations en matière d'IA qui dépendent fortement des données pour échafauder des algorithmes) ainsi que la transparence.

Les flux de données transfrontaliers (FDT) en Afrique sont essentiels pour la nouvelle zone de libre-échange continentale africaine (ZLECAf) et le marché unique numérique (MUN). Ils pourraient également s'avérer essentiels à la constitution d'ensembles de données suffisamment importants que pour alimenter les modèles d'IA sectoriels conçus en Afrique et répondant aux besoins de celle-ci. Des mesures restrictives telles que la localisation stricte des données pourraient entraver la croissance économique et avoir un impact négatif sur le commerce et l'investissement.

L'Union africaine (UA) a développé un ensemble varié d'instruments juridiques et politiques visant à promouvoir la transformation numérique et une économie numérique intégrée en Afrique. Les instruments continentaux et régionaux incarnent diverses valeurs (démocratie, État de droit, transparence, justice sociale, paix et sécurité), divers objectifs (croissance économique, intérêt géopolitique, stabilité politique) et divers instruments (convergence réglementaire, renforcement des capacités, accords commerciaux, partenariats multilatéraux), ce qui se traduit par des approches diverses et variées en matière de partage des données.

Bien que chaque instrument vise des objectifs politiques spécifiques, ils se complètent entre eux et forment collectivement une approche cohérente du partage transfrontalier de données en Afrique, en mettant fortement l'accent sur la protection et la sécurité des données. Ces instruments encouragent la libre circulation des données et les transferts intracontinentaux, déconseillent la localisation stricte des données (mesures qui restreignent complètement les transferts de données en dehors d'un pays ou imposent le stockage local) et préconisent la localisation conditionnelle qui autorise les transferts de données dans des conditions clairement définies. Cela témoigne du fait que l'Afrique pourrait aller beaucoup loin si ses pays travaillaient main dans la main au développement du commerce numérique dans le cadre de la ZLECAf, et à l'avènement d'une économie de données dynamique et innovante qui pourrait à son tour fournir les ensembles de données permettant de développer un IA construite en Afrique.

Il n'y a pas de politique continentale unique sur les flux de données transfrontaliers (FDT), mais on note des synergies évidentes entre les divers cadres juridiques et politiques numériques au niveau de l'UA. Tous ces cadres continentaux soulignent la nécessité d'un partage

transfrontalier des données (le Cadre stratégique de l'UA en matière de données, par exemple) et fournissent des règles d'orientation pour faciliter ce partage en mettant l'accent sur la confiance et la sécurité, en particulier des données à caractère personnel (la convention de Malabo, par exemple). Ils encouragent également l'harmonisation des cadres nationaux. Beaucoup de ces instruments n'ont été adoptés ou formulés que récemment (le Protocole sur le commerce numérique pour l'Afrique de la ZLECAf et la Stratégie continentale de l'UA en matière d'IA) et il faut encore procéder à une évaluation plus solide de leur cohérence et de leur homogénéité.

Au sein des communautés économiques régionales (CER), les politiques se sont principalement concentrées sur la réglementation des données à caractère personnel et sur la protection des droits des personnes concernées.

Une des critiques fréquemment entendues à propos des cadres politiques africains, c'est qu'en dépit de politiques bien pensées, leur mise en œuvre reste souvent déficiente : il est vrai que les lacunes de ces instruments ont entravé leur adoption au niveau national. Ils peuvent ratisser trop large, manquer d'orientations claires pour leur mise en œuvre et s'avérer contraignants pour les États membres. À l'inverse, des définitions plutôt larges élaborées afin de tenir compte des divers contextes des États membres peuvent se traduire par une flexibilité excessive. L'absence de mécanismes et de cadres clairs en matière de partage des données conduit à devoir se passer d'un train d'union important entre la politique et la pratique et à se heurter à un défi de mise en œuvre. Ce document met en évidence ces lacunes qui peuvent involontairement entraver les FDT.

À cela s'ajoutent des défis au niveau de la mise en œuvre, parmi lesquels le manque de transposition des instruments continentaux en droit national (la convention de Malabo, par exemple) ou l'élaboration de stratégies nationales alignées sur les lignes directrices continentales (le Cadre stratégique de l'UA en matière de données, la Stratégie continentale de l'UA en matière d'IA, par exemple). Il arrive souvent que les politiques nationales donnent la priorité à des intérêts locaux qui peuvent éclipser la vision continentale. Il ressort de notre recherche que diverses idéologies, contextes socio-économiques, préoccupations en matière de sécurité et priorités économiques façonnent les politiques relatives au partage des données, ce qui se traduit par des variations entre les trois pays que nous avons considérés dans cette étude de cas, à savoir le Mozambique, le Nigeria et le Sénégal. La mise en œuvre dépend aussi des capacités socio-politiques dont un État dispose pour coordonner ses organismes ; or, ces capacités varient considérablement d'un pays à l'autre et sont sujettes à des retards administratifs et à des contestations. Une coordination inefficace, des mandats concurrents et des incitations aux effets pervers peuvent également nuire à l'efficacité de la mise en œuvre.

La conjugaison de ces facteurs permet d'expliquer l'écart que l'on constate entre la politique et la pratique, d'une part, et entre les processus nationaux et continentaux, d'autre part.

L'avènement d'une économie globale des données en Afrique nécessitera des efforts, tant au niveau continental que national. Ce document formule des recommandations pour renforcer

les cadres d'orientation et de mise en œuvre au niveau continental, ainsi que pour traiter les différences politiques et les défis de mise en œuvre au niveau national afin d'éviter la fragmentation et de permettre l'interopérabilité.

L'UE est un partenaire important des pays africains en matière de commerce, d'investissement et de développement, et peut jouer un rôle dans le soutien des FDT en Afrique. Elle pourrait notamment partager certaines de ses expériences dans la mise en œuvre de sa propre Stratégie pour les données et tirer parti du pilier numérique de la Global Gateway pour soutenir l'économie africaine des données. Soutenir les initiatives de partage de données en Afrique est conforme à l'objectif de l'UE de mener la coopération internationale en matière de données et d'élaborer des normes mondiales. En effet, l'UE soutient déjà l'UA et ses États membres dans l'élaboration de politiques en matière de données par l'intermédiaire de l'initiative "Gouvernance des données en Afrique".

1. Introduction

Les données jouent un rôle important dans l'économie numérique au sens large et constituent l'épine dorsale de l'économie de l'Intelligence Artificielle (IA). On les retrouve à différents niveaux (les données économiques, par exemple, peuvent se situer au niveau macroéconomique, sectoriel, de l'entreprise ou de l'individu), dans différents secteurs (les soins de santé, l'éducation, l'agriculture, la météorologie, etc.) et sous de multiples formes (confidentielles, à caractère personnel ou non, big data, données ouvertes, etc.) (Beyleveld et Sucker, 2022). Le partage et l'utilisation des données favorisent la croissance économique, la concurrence, la recherche et les avancées scientifiques (surtout les innovations en matière d'IA qui dépendent fortement des données pour échafauder des algorithmes) ainsi que la transparence (Mwaya 2022, The Economist 2018).¹ Selon la mesure dans laquelle ils sont autorisés, l'accès aux données et leur partage dans les secteurs public et privé peuvent procurer des avantages économiques et sociaux d'une valeur comprise entre 1 et 2,5 % du PIB; les restrictions, a contrario, peuvent réduire la production commerciale jusqu'à 7 % et provoquer une hausse des prix (Mwaya 2022). Les flux de données transfrontaliers (FDT) constituent un moteur important de l'économie numérique africaine, laquelle était estimée à 115 milliards de dollars US en 2022 (Endeavor Nigeria 2022) et pourrait croître de 57% au cours des 5 prochaines années (CSEA 2021). Même si la plupart des infrastructures et des échanges numériques des pays africains se font avec des partenaires situés en dehors de l'Afrique, il est essentiel de disposer de FDT fluides en Afrique pour desservir la zone de libre-échange continentale africaine (ZLECAf) et le marché unique numérique (MUN) nouvellement établis.² Ils pourraient également s'avérer essentiels à la constitution d'ensembles de données suffisamment importants que pour alimenter des modèles d'IA conçus en Afrique, dans des secteurs spécifiques notamment. Des mesures restrictives telles que la localisation stricte des données pourraient entraver la croissance économique et avoir un impact négatif sur le commerce et l'investissement (Beyleveld 2021, rapport GSMA 2021, Oloni 2024).

Sur le papier, les pays africains conviennent que les FDT intra-africains sont essentiels pour réaliser la vision continentale décrite dans des documents politiques clés tels que l'Agenda 2063, la stratégie de transformation numérique et l'accord de la ZLECAf. Ces documents préconisent des FDT continentaux gratuits pour stimuler le MUN tout en garantissant le respect de la vie privée, la protection des données et la sécurité nationale. Des instruments récents tels que le protocole sur le commerce numérique de la ZLECAf, la convention de Malabo, le Cadre stratégique de l'UA en matière de données et la Stratégie continentale en matière d'IA

¹ Dans la chaîne de valeur des données : les producteurs de données génèrent des données à partir de l'internet des objets et des sources traditionnelles de big data ; les agrégateurs de données les extraient, les formatent et les rassemblent ; les présentateurs de données simplifient des ensembles de données complexes pour les utilisateurs ; les conseillers (insight providers) génèrent de la valeur à partir d'analyses avancées telles que des algorithmes d'apprentissage automatique et des modèles statistiques (Naidoo 2020).

² Selon l'UA, un marché unique numérique panafricain suppose une meilleure connectivité (à haut débit) entre les pays et les régions du continent, l'élimination des frais d'itinérance, une réglementation harmonisée et de l'innovation numérique pour une plus grande intégration économique conforme à ce que prévoit la ZLECAf ([Stratégie de transformation numérique](#)).

témoignent des efforts déployés pour améliorer le partage des données sur l'ensemble du continent.

Dans les faits, cependant, les États membres de l'UA abordent les FDT chacun à leur manière, en accordant des moyens variables à la mise en œuvre de la vision continentale. L'infrastructure numérique limitée, les cadres politiques incohérents qui entravent le partage intelligible des données et les efforts déployés pour lutter contre la domination étrangère dans l'économie numérique de l'Afrique, laquelle influence aussi la souveraineté numérique, sont autant de facteurs qui entraînent des restrictions sur les FDT (série d'entretiens de Soule, 2023). Cette situation soulève des préoccupations en matière de souveraineté des données et incite les dirigeants africains à prendre des mesures de localisation des données pour réguler leur flux. Ils craignent que la perte de contrôle sur les données ne débouche sur un monopole intellectuel et un colonialisme des données, qui étouffe l'esprit d'entreprise africain par l'usage d'outils non africains inadaptés et qui se sert des données africaines pour générer des profits ailleurs tout en privant leurs pays de sources potentielles de revenus (Sampath et Tregenna 2022). Il s'en suit que les FDT restent limités en Afrique, avec seulement cinq pays figurant parmi les cent premiers pays connectés numériquement et ouverts au partage des données ([Global Competitiveness Index for 2020](#)).

Dans ce document, nous examinons dans quelle mesure la vision continentale du partage et des flux de données est mise en œuvre au niveau national. Nous recensons et commentons les divergences entre la politique et la pratique en analysant tout d'abord la mesure dans laquelle les politiques continentales promeuvent les FDT en Afrique et en examinant ensuite la manière dont les cadres politiques et juridiques continentaux et nationaux sont corrélés. Nous explorons les raisons pour lesquelles les politiques nationales divergent des engagements pris au niveau continental en examinant les facteurs qui façonnent le paysage actuel de la politique numérique dans les pays que nous avons sélectionnés. Enfin, nous formulons des recommandations politiques exploitables au niveau continental, national et européen pour combler le fossé entre la politique et la pratique afin de promouvoir l'intégration régionale et le partage des données à l'échelle continentale.

Pour illustrer les différents paysages politiques en matière de données ou « contextes de données », nous avons sélectionné trois pays au titre d'études de cas : le Sénégal, le Nigeria et le Mozambique. Le Sénégal est l'un des premiers pays à avoir adopté une stratégie relative aux données inspirée du Cadre stratégique de l'UA en matière de données (CSD) et à montrer comment ce cadre peut être transposé dans une politique nationale. Le Nigeria, bien qu'il représente l'une des économies numériques les plus dynamiques d'Afrique, a tardé à élaborer une stratégie claire en matière de données et n'a adopté que récemment une loi sur la protection des données à caractère personnel. Le Mozambique, l'un des pays d'Afrique les moins bien préparés au numérique, n'a pas de stratégie en matière de données et ne dispose d'aucun autre cadre réglementaire pour la gouvernance des données.

Notre travail s'appuie sur une revue de la littérature, une analyse approfondie des politiques et stratégies africaines et plus de 60 entretiens avec des fonctionnaires, des experts et des

représentants du secteur privé travaillant sur la gouvernance des données en Afrique. Nous avons mené des entretiens en personne au Nigeria, au Sénégal et au Mozambique, ainsi qu'en ligne avec des fonctionnaires et des experts d'Afrique et d'Europe.

Notre document est organisé comme suit : la section 2 examine la vision continentale et régionale des FDT et leurs lacunes. La section 3 synthétise les principales caractéristiques des politiques nationales observées dans les trois pays ayant fait l'objet de notre étude de cas. La section 4 identifie les facteurs qui expliquent l'écart entre les cadres et la vision nationaux et continentaux. La section 5 formule des recommandations en direction de l'UA et des organes concernés, des gouvernements nationaux ainsi que de l'UE, compte tenu de son rôle essentiel dans l'écosystème de la gouvernance des données en Afrique.

2. Vision continentale des FDT

L'Union africaine (UA) dispose d'un large éventail d'instruments juridiques et politiques pour promouvoir la transformation numérique et l'intégration régionale (des données) en Afrique. Bien que chaque instrument puisse poursuivre un objectif politique spécifique, ils sont tous complémentaires et cohérents dans leur approche du partage des données, tout en soulignant l'importance de la protection et de la sécurité de celles-ci. La convention de Malabo, notamment, figure en bonne place parmi ces cadres, en mettant l'accent sur la confiance et la sécurité lors du traitement des données à caractère personnel. Ces instruments encouragent la libre circulation des données et les transferts intracontinentaux, déconseillent la localisation stricte des données (mesures qui restreignent complètement les transferts de données en dehors d'un pays ou imposent le stockage local) et préconisent la localisation conditionnelle qui autorise les transferts de données dans des conditions clairement définies (Musoni et al. 2023). Cette section met en évidence les différentes politiques continentales et régionales qui dénotent l'approche de l'UA en matière de gouvernance des FDT continentaux, et identifie certaines de leurs lacunes.

2.1. Instruments politiques de l'UA visant à promouvoir les FDT

Les FDT ne font pas l'objet d'une seule et unique politique continentale. Ce sont plusieurs instruments continentaux qui transposent la vision décrite ci-dessus. Bien que nombre de ces instruments n'aient été adoptés/formulés que récemment et qu'il faille encore procéder à une évaluation plus solide de la cohérence et de l'homogénéité entre eux, il semble à première vue que des synergies sur les FDT se dégagent en fil rouge de ces divers cadres juridiques et politiques numériques au niveau de l'UA. Tous soulignent la nécessité d'un partage transfrontalier des données (CSD, Stratégie continentale en matière d'IA) et fournissent les règles directrices pour les faciliter (convention de Malabo, PCN). Ils encouragent également l'harmonisation des cadres nationaux.

Tableau 1 : Aperçu des politiques numériques continentales

Politique	Finalité	Position par rapport aux FDT
Stratégie de transformation numérique pour l'Afrique 2020 - 2030	Plan global visant à tirer parti des technologies numériques pour transformer les économies et les sociétés africaines, axé sur quatre piliers fondamentaux : l'infrastructure numérique, les compétences numériques, l'innovation numérique et l'esprit d'entreprise, ainsi que l'environnement porteur et les réglementations.	Soutient la ZLECAf en promouvant le commerce numérique, le commerce électronique, le partage des données intra-africain ainsi que le développement de normes de données et de cadres d'interopérabilité. Plaide en faveur de cadres politiques, juridiques et réglementaires harmonisés, y compris la protection des données conformément à la convention de Malabo. Cette stratégie est pionnière en matière de réglementation permettant la libre circulation des données à caractère non personnel. À la suite de son adoption, plusieurs politiques, cadres et initiatives se sont concentrés sur l'élaboration ou la mise en œuvre de ses piliers fondamentaux.
Cadre stratégique de l'UA en matière de données, 2022	Cadre de gouvernance des données couvrant à la fois les données à caractère personnel et non personnel. Il présente une vision, des principes, des priorités stratégiques et des recommandations pour développer des systèmes de données nationaux afin de tirer parti des données des citoyens, des entités gouvernementales et des industries.	Plaide pour des politiques équilibrées en matière de localisation des données, en soulignant les avantages du partage par rapport à l'accumulation des données. Encourage les États membres à évaluer les coûts et les avantages de la localisation, en tenant compte des droits de l'homme et des priorités plus larges du développement économique. Invite les pays africains à passer de la localisation des données à la promotion de flux de données libres et sûrs, tout en protégeant les droits de l'homme, en assurant la sécurité et en garantissant un accès équitable et le partage des avantages (Musoni 2024).
Cadre d'interopérabilité des systèmes d'identification numérique de l'UA, 2023	Fixe des règles d'interopérabilité pour les données d'identification numérique afin de permettre aux citoyens de participer à l'économie numérique et de faciliter les paiements et les services financiers	Introduit en décembre 2023, bien que le statut d'adoption du cadre reste incertain. Les pays de la Smart Africa ³ sont potentiellement intéressés par le développement de systèmes d'identification numérique interopérables permettant d'échanger des informations de manière sûre et transparente (Smart Africa Digital ID Blueprint) sous la conduite du Bénin.

³ [Smart Africa](#) est une initiative prise par certains dirigeants africains, visant à favoriser un développement socio-économique durable grâce à la numérisation. Amorcée par 7 gouvernements africains, elle regroupe aujourd'hui 39 pays.

	numériques. Établit des normes et des processus pour un partage fiable et sécurisé des données à caractère personnel.	
Stratégie continentale de l'UA en matière d'IA, 2024	Décrit une approche continentale de la construction de l'économie de l'IA par le développement et l'utilisation de celle-ci, en mettant l'accent sur les capacités infrastructurelles telles que les centres de données, l'informatique en nuage et des données de qualité pour le développement de l'IA dans les États membres.	Adoptée à la suite d'intenses discussions multipartites , y compris au sujet du Livre blanc sur l'IA de l'AUDA NEPAD. Recommande aux États membres d'élaborer des politiques et des stratégies en matière de données permettant l'accès et le partage de données à caractère non personnel. Demande instamment la mise en place de cadres de gouvernance des données assorties de normes pour un partage éthique, responsable et sécurisé des données. Souligne la nécessité d'une coordination intra-africaine en matière d'IA, plaide en faveur d'une coopération régionale en matière de données ouvertes et propose un instrument régional pour guider le partage et les transferts de données transfrontaliers.
Livre blanc de l'AUDA NEPAD pour une IA responsable, 2024	Identifie les domaines que les pays africains doivent privilégier pour tirer efficacement parti de l'IA. Ces domaines sont le développement du capital humain, les infrastructures et les données, la création d'un environnement porteur, la stimulation de l'économie de l'IA et la mise en place de partenariats durables.	Incite les pays africains à développer de solides capacités de stockage des données afin de réduire leur dépendance à l'égard de l'étranger, de stimuler l'innovation locale, d'attirer les investissements et de stimuler la croissance économique. Se dit favorable aux investissements dans des centres de données locaux, en préconisant des cadres de gouvernance des données et en promouvant la souveraineté des données afin de libérer tout le potentiel des initiatives basées sur les données en faveur du développement économique et de l'innovation. Recommande l'adoption de lois et de réglementations favorisant le stockage et le transfert de données au sein de l'Afrique, en encourageant le développement d'une infrastructure de données solide afin de réduire la dépendance à l'égard des installations de stockage de données non africaines. Propose des mesures pour que les FDT puissent relever les défis et saisir les opportunités liés à la gouvernance et à la souveraineté des données, surtout dans le contexte de l'IA en Afrique.

<p>Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel, 2014</p>	<p>Instrument juridiquement contraignant portant sur le commerce électronique, la protection des données à caractère personnel et la cybersécurité. Établit des règles pour les transactions électroniques afin de promouvoir le commerce électronique à l'échelle du continent. Mandate les États membres pour qu'ils adoptent des politiques et des stratégies en matière de cybersécurité et promeuvent la coopération internationale. Fournit des orientations sur le traitement des données à caractère personnel.</p>	<p>Autorise le transfert conditionnel de données (Oloni 2024). Exige des États membres qu'ils adoptent des lois sur la protection des données garantissant les droits individuels et obligeant les responsables du traitement des données⁴ à assurer une protection adéquate lors du partage avec des États non membres de l'UA (article 14 (6)(a)). En substance, la convention de Malabo promeut la libre circulation des FDT tout en protégeant les droits grâce à des garanties établies.</p>
<p>Protocole sur le commerce numérique de la ZLECAf, 2024⁵</p>	<p>Cherche à réglementer et à faciliter les transactions numériques grâce à des règles continentales communes, en surmontant les problèmes de fragmentation, afin d'atteindre l'objectif de la ZLECAf. Façonne les FDT en Afrique au-delà du périmètre de la convention de Malabo, car il se concentre sur les données à caractère personnel ou non dans le contexte du commerce numérique.</p>	<p>Encourage les États parties à faciliter les transferts de données tout en garantissant la protection des données et de la vie privée, à supprimer les obstacles tels que les exigences locales en matière de stockage des données et à promouvoir l'innovation en matière de données par l'établissement de politiques et de normes sur la mobilité et la portabilité des données. Prévoit des exceptions permettant aux États membres de s'écarter de la règle générale de la libre circulation des données, pour autant que les mesures adoptées servent des "objectifs légitimes de politique publique" ou "protègent des intérêts essentiels de sécurité". Toutefois, ces exceptions doivent éviter toute discrimination arbitraire ou injustifiable, ne doivent pas servir de restrictions déguisées au commerce numérique et ne doivent limiter les transferts de données que dans la mesure nécessaire pour atteindre leur objectif.</p>

⁴ Le responsable du traitement est toute personne (physique, morale, publique, privée, organisation, association, etc.) qui décide de collecter et de traiter des données à caractère personnel et qui en détermine les finalités.

⁵ Cette analyse se base sur la version du PNC qui a [fuité](#).

2.2. Instruments politiques régionaux visant à promouvoir les FDT

Au sein des communautés économiques régionales (CER), les politiques relatives aux FDT se sont exclusivement concentrées sur la réglementation des données à caractère personnel et la sauvegarde des droits des personnes concernées. Le tableau 2 résume les politiques de quatre CER africaines, à savoir la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), la Communauté de développement de l'Afrique australe (SADC), la Communauté économique des États de l'Afrique centrale (CEEAC) et la Communauté de l'Afrique de l'Est (CAE), ainsi que leurs approches respectives en matière de transfert de données à caractère personnel.

Tableau 2 : Aperçu des politiques des CER relatives aux FDT

Politique	Finalité	Position par rapport aux FDT
2010 Acte additionnel relatif à la protection des données à caractère personnel de la CEDEAO	Traité contraignant inspiré de la convention de Malabo, réglementant le traitement des données à caractère personnel entre les États membres.	Établit des exigences d'adéquation permettant des transferts vers des États non membres avec une protection adéquate de la vie privée, des libertés et des droits individuels dans le traitement des données. ⁶ À l'exception de la Gambie, de la Guinée-Bissau et du Libéria, tous les membres ont adopté des lois nationales sur la protection des données (Musoni, Domingo, Ogah 2023), la Guinée, le Mali, le Niger et le Togo copiant apparemment les dispositions de l'Acte additionnel (Abdulfauf 2024).
2013 Loi type sur les données à caractère personnel de la SADC	Loi type non contraignante énonçant les principes, les droits et les obligations en matière de protection des données que les États membres doivent prendre en compte lors de l'élaboration de leur législation nationale.	Prévoit des conditions spécifiques (selon que l'État membre appartient ou non à la SADC) pour le transfert de données à caractère personnel. ⁷ Le Mozambique et les Comores sont les seuls pays à ne pas avoir de loi nationale sur la protection des données.
2013 Loi type de l'ECCAS et Directive sur la protection du consommateur de la Communauté économique et	Son champ d'application est similaire à celui de la loi type de la SADC (King'ori 2024).	Trois articles sur les transferts transfrontaliers de données ; restreint les transferts de données à caractère personnel vers des pays non membres de la CEEAC, à moins que la juridiction destinataire ne puisse assurer un niveau de protection adéquat par

⁶ Article 36 de l'Acte additionnel de la CEDEAO.

⁷ Articles 43 et 44.

monétaire d'Afrique centrale (CEMAC)		rapport à la loi type de la CEEAC, ou que le responsable du traitement des données n'offre des garanties suffisantes en matière de protection. ⁸ Le Burundi, le Cameroun et la République centrafricaine n'ont pas encore adopté de lois nationales sur la protection des données.
2008 Cadre juridique de la CAE pour la cyberléislation	Dispositions sur une série de questions allant de la protection des données à la protection des consommateurs, en passant par les transactions électroniques, la propriété intellectuelle et la fiscalité.	Pas de dispositions explicites relatives aux FDT. L'adoption récente de lois sur la protection des données en RDC, au Kenya, au Rwanda, en Ouganda et en Tanzanie serait le résultat de la pression exercée par l'Europe ⁹ plutôt que de la pression ou de l'urgence de se conformer à la convention de Malabo (Fidler 2024).

2.3. Lacunes des instruments continentaux

Les instruments continentaux et régionaux incarnent diverses valeurs (démocratie, État de droit, transparence, justice sociale, paix et sécurité), divers objectifs (croissance économique, intérêt géopolitique, stabilité politique) et divers instruments (convergence réglementaire, renforcement des capacités, accords commerciaux, partenariats multilatéraux), ce qui se traduit par des approches diverses et variées en matière de partage des données (Shahin et al. 2024). Les lacunes de ces instruments ont entravé leur adoption au niveau national. Ils peuvent ratisser trop large, manquer d'orientations pour la mise en œuvre et s'avérer contraignants pour les États membres. Dans d'autres cas, des définitions plutôt larges donnent aux États membres une flexibilité excessive. Cette section met en évidence ces lacunes qui peuvent involontairement entraver les FDT.

2.3.1. Un champ d'application large

Les instruments de l'UA peuvent avoir un champ d'application très large. La convention de Malabo couvre "la protection des données, le commerce électronique, la cybersécurité et la cybercriminalité", regroupant "les droits de l'homme, le droit pénal et le droit commercial en un seul instrument" (Ayalew 2022). La lenteur de son adoption – il a fallu neuf ans pour que 15 pays seulement la ratifient, et n'en font pas partie des acteurs majeurs comme l'Égypte, le Nigéria,

⁸ Voir également King'ori 2024.

⁹ Le règlement général sur la protection des données de l'UE 2016/679. La convention du Conseil de l'Europe sur la protection des données (conventions 108 et 108+). Les entreprises ont estimé qu'il était rentable d'avoir une conformité au RGPD en Afrique et ont fait pression pour obtenir des lois similaires afin de faciliter cette mise en conformité. Le RGPD, considéré comme une référence mondiale, a influencé les réglementations africaines – un phénomène connu sous le nom d'effet de Bruxelles.

l'Afrique du Sud et l'Éthiopie (où siège l'UA) – nuit également à sa crédibilité (Ifeanyi-Ajufo 2024).

D'autres instruments sont complets au point d'en devenir vagues ou d'imposer des conditions onéreuses aux États membres. Le PCN de la ZLECAf compte de nombreuses annexes inachevées qui risquent d'embrumer ses dispositions précises. Tout en encourageant la libre circulation des données, le PCN prévoit des exceptions pour des "objectifs légitimes de politique publique", mais il est difficile de définir et de prouver la légitimité de ces objectifs. Certains craignent que les exceptions soient fréquemment utilisées sans qu'il y ait suffisamment de recours pour contester les décisions ou obtenir un verdict (CIPIT 2024). D'autres soulignent que des cadres tels que le CSD exercent une pression sur les États membres pour qu'ils en fassent trop (Saturday and Nyamwire 2023).

2.3.2. L'accent est mis sur les données à caractère personnel

Jusqu'il y a peu, la plupart des discussions se sont concentrées sur la protection des données à caractère personnel par le biais d'instruments exécutoires et ont accordé peu d'attention à la gouvernance et au partage d'autres types de données pour promouvoir les FDT intra-africains. Malgré son adoption tardive, la convention de Malabo, par exemple, est un instrument juridiquement contraignant conçu pour protéger les données à caractère personnel. Plusieurs pays sont en train d'adopter des lois sur la protection des données à caractère personnel, avec des régulateurs de données chargés de contrôler et de faire respecter la conformité. Le CSD de l'UA a fait œuvre de pionnier en élargissant son centre d'intérêt pour y inclure des lignes directrices détaillées sur l'utilisation des données à caractère non personnel. Il ne s'agit toutefois pas d'un instrument juridiquement contraignant. Le PCN de la ZLECAf est plus prometteur, car il réglemente aussi bien les données à caractère personnel que celles qui ne le sont pas. Il devrait être juridiquement contraignant, mais il reste encore des problèmes à résoudre (cf. ci-dessous).

Le partage intra-africain de données à caractère non personnel dans le cadre d'accords sectoriels spécifiques peut ne pas être encadré par des cadres continentaux. Les pays africains partagent des données relatives au climat et à l'environnement afin de mieux se préparer aux catastrophes naturelles ou de préserver la biodiversité.¹⁰ Ces accords sont généralement axés sur des objectifs politiques spécifiques, tels que la santé publique pendant la pandémie de COVID-19, plutôt que sur le développement économique, qui est aujourd'hui au cœur des discussions relatives aux FDT. (Koch 2022).

2.3.3. Un manque d'orientations

Certains instruments de l'UA ne donnent pas assez d'orientations aux États membres et aux CER. La convention de Malabo, en particulier, donne peu d'indications sur le plan de la localisation des données et des règles ou mécanismes précis à mettre en place pour le transfert de données (Beyleveld and Sucker 2024; King'ori 2024). De même n'apparaissent pas

¹⁰ L'OFESA (Observatoire des forêts d'Afrique de l'Est et australe) est une initiative régionale de surveillance et de gestion des ressources forestières qui recourt aux FDT entre ses États membres. Voyez <https://ofesa.rcmrd.org/en/>.

dans l'Acte additionnel de la CEDEAO des termes aussi cruciaux que le transfert transfrontalier et les droits concernant les plaintes auprès des régulateurs ou la portabilité des données (Saturday and Nyamwire 2023). La Stratégie de transformation numérique pour l'Afrique n'est en outre assortie d'aucun cadre de mise en œuvre pour ses différents piliers, ce qui nuit à sa crédibilité. Le CSD est prometteur, car il fournit une feuille de route claire aux États membres pour la mise en œuvre des politiques. Certains pays africains, dont le Bénin, le Burundi, l'Égypte, la Gambie, Madagascar, le Mozambique, le Ghana, le Rwanda, la Tanzanie, l'Ouganda et la Zambie, ont demandé l'aide de l'UA pour la mise en œuvre nationale, et la GIZ, soutenue par une initiative plus large de Team Europe, aide l'UA à fournir un appui technique à certains pays.

2.3.4. Les intérêts ou contextes africains ne sont pas reflétés

Les instruments de l'UA ont tendance à s'inspirer des bonnes pratiques d'autres régimes, or cette émulation peut avoir des conséquences inattendues. La convention de Malabo, par exemple, s'inspire de la Directive sur la protection des données de l'UE (aujourd'hui remplacée par le Règlement général sur la protection des données (RGPD)) (Ayalew 2022), tandis que le PCN de la ZLECAf s'inspire de l'Accord Canada-États-Unis-Mexique (ACEUM) (Gathii 2024; Whittle 2024). Certaines des personnes que nous avons interrogées se sont inquiétées du fait que l'adoption de cadres élaborés dans des contextes différents pourrait ne pas correspondre aux réalités africaines ou les négliger. D'autres études font également allusion à ce risque (Beyleveld and Sucker 2024; Saturday and Nyamwire 2023).

L'économie africaine des données et de l'IA étant dominée par des entreprises étrangères, on peut craindre que certaines dispositions du PCN de la ZLECAf aient été influencées par ces entreprises pour protéger leurs propres intérêts. Le PCN de la ZLECAf accorde, par exemple, des droits de secret quasi absolus aux entreprises de logiciels (généralement étrangères), ce qui pourrait entraver le transfert de technologies et de compétences en limitant l'accès par inadvertance des développeurs et des gouvernements africains à des logiciels et à des algorithmes essentiels (CIPIT 2024). L'approche inspirée de l'ACEUM qui consiste à laisser le champ libre aux FDT n'est pas sans risque potentiel pour la vie privée des citoyens, ce qui conditionne l'avenir de l'Internet. En effet, cette approche est actuellement reconsidérée aux États-Unis en raison du risque d'abus de pouvoir par les grandes entreprises technologiques et des préoccupations qu'elle suscite sur le plan de la sécurité nationale (Gathii 2024, Kilic 2024). Ces dispositions figurent pourtant dans le PCN de la ZLECAf.

Les critiques portent aussi sur le fait que nombre de ces processus politiques sont influencés par des entités extérieures. Certaines personnes interrogées estiment que les conditions favorables que le PCN de la ZLECAf accorde aux grandes entreprises technologiques résultent du soutien qu'USAID accorde au secrétariat de la ZLECAf par le biais de l'initiative "2020 Digital Transformation with Africa"; d'autres, en revanche, affirment que le processus a été mené par des experts africains pour garantir une mainmise africaine. Le CSD, élaboré avec le soutien des institutions de l'UA, de Team Europe et de Research ICT Africa, est un autre exemple de ce phénomène. L'Allemagne, par l'intermédiaire de la GIZ, a apporté son soutien à l'élaboration du CSD, dont la mise en œuvre est par ailleurs soutenue par l'Union européenne et plusieurs de

ses États membres.¹¹ Bien que la GIZ insiste sur l'appropriation de ce processus par l'UA, certaines personnes interrogées ont exprimé des doutes quant au niveau d'implication réelle des États membres de l'UA et d'autres parties prenantes.

Enfin, ces instruments visent à faciliter les FDT *en Afrique*, alors qu'une grande partie de l'infrastructure et des services numériques sont importés *d'autres continents*. En soi, les politiques régissant les transactions extra-africaines sont plus pertinentes pour le "développement numérique" en Afrique (Stuart 2024a). Ces politiques diffèrent d'un pays à l'autre, sans bénéficier d'une gouvernance uniforme.¹²

3. De la vision continentale à la mise en œuvre nationale

La mise en œuvre au niveau national n'est pas non plus exemptée de défis (CSEA 2021). Elle peut impliquer l'adoption d'une législation (la convention de Malabo, le PCN, par exemple) ou l'adoption de stratégies nationales suivant les lignes directrices continentales (le CSD, la Stratégie continentale en matière d'IA), la conformité nécessitant un suivi et l'application des règles en cas d'infraction. Mais il arrive souvent que les politiques nationales donnent la priorité à des intérêts nationaux qui peuvent contredire ou éclipser la vision continentale. La mise en œuvre dépend des capacités socio-politiques dont un État dispose pour coordonner ses organismes ; or, ces capacités varient considérablement d'un pays à l'autre et sont sujettes à des retards administratifs et à des contestations (Jaïdi et al. 2024). Faute de disposer des capacités de base nécessaires (les capacités institutionnelles et les structures de gouvernance, les cadres réglementaires, la capacité administrative en termes de personnel formé, les ressources financières, etc.) pour soutenir la mise en œuvre de ces instruments, le fossé se creuse entre la politique et la pratique. Cette façon de vouloir en faire "trop, trop tôt et avec trop peu" est décrite par certains experts comme un palier portant prématuré (Pritchett 2019).

3.1. Approches nationales en matière de flux de données

Diverses idéologies, contextes socio-économiques, préoccupations en matière de sécurité et priorités économiques façonnent les politiques relatives au partage des données, ce qui se traduit par des variations d'un pays à l'autre. Dans cette section, nous examinons les facteurs qui déterminent les politiques nationales de trois pays africains, à savoir le Mozambique, le Nigeria et le Sénégal, car il est important de comprendre ces facteurs afin de formuler des recommandations politiques visant à combler le fossé entre les processus continentaux et nationaux.

¹¹ La GIZ dirige la mise en œuvre du programme. Elle a élaboré un cadre de mise en œuvre, accueilli le premier [Data Innovation Forum](#) en novembre 2023, et est en train de déployer un cadre au niveau national.

¹² La ZLECAf est un accord de libre-échange et non une union douanière, ce qui signifie que les États membres ne peuvent pas régir collectivement le commerce numérique extra-africain, si ce n'est par l'intermédiaire de communautés économiques régionales qui couvrent spécifiquement ce domaine.

Tableau 3 : Aperçu des politiques nationales dans les pays choisis pour cette étude

<p>Nigeria</p>	<p>2011, Banque centrale du Nigeria (CBN) : lignes directrices pour le secteur bancaire¹³</p> <p>2013 Agence nationale de développement des technologies de l'information (NITDA) Lignes directrices pour le développement du contenu nigérian dans les TIC (NITDA ICT Guidelines),¹⁴ amendées en 2019</p> <p>2019 Politique nationale en matière d'informatique dématérialisée</p> <p>2019 Règlement nigérian sur la protection des données (NDPR) sous l'égide de la NITDA, suivi par la Loi nigériane sur la protection des données (NDPA) entrée en vigueur fin 2023. La Commission nigériane sur la protection des données (NDPC) contrôle et applique la NDPA en fonction d'une liste blanche pour faciliter les FDT, y compris avec les pays qui ont ratifié la convention de Malabo et d'autres. (Cadre</p>	<p>N'a ni signé ni ratifié la convention de Malabo</p> <p>Signataire de l'Acte additionnel de la CEDEAO sur les données à caractère personnel</p> <p>A tenu compte du CSD de l'UA lors de l'élaboration de son projet de stratégie nationale en matière de données</p> <p>La NDPC est membre du RAPDP/NADPA (Réseau africain des autorités de protection des données personnelles)</p>	<p>Approche évolutive - accent mis précédemment sur le traitement local des données (lignes directrices de la NITDA en matière de TIC ou lignes directrices de la CBN, par exemple). En l'absence d'une vision claire telle que la stratégie nationale sur les données ou la NDPA pour protéger les données à caractère personnel (le Nigeria étant considéré comme en retard par rapport à d'autres pays), l'efficacité a été assurée en se concentrant sur la promotion de l'innovation locale par le biais de mesures strictes sur les flux de données.</p> <p>L'accent est désormais mis sur la gestion des données à l'intérieur du Nigeria et sur le transfert des données. La politique et la stratégie nationales en matière d'économie numérique, ainsi que le projet de stratégie nationale en matière de données, établissent un équilibre entre la confidentialité des données et les FDT. La NDPA autorise le transfert de données à caractère personnel ; la politique nationale en matière d'informatique dématérialisée remet en cause les prises de position politiques antérieures sur le stockage local des</p>
----------------	---	--	--

¹³ La ligne directrice 4.4.8 stipule que toutes les transactions nationales doivent être traitées en utilisant les services d'un commutateur local et ne doivent pas être acheminées en dehors du pays (Central Bank of Nigeria Guidelines on Point of Sale Card Acceptance Services 2011).

¹⁴ Les lignes directrices 12.1(4) et 14.2(3) imposent aux entreprises de TIC d'héberger les données des clients et des abonnés au Nigeria et toutes les données gouvernementales doivent être hébergées localement (NITDA Guidelines for Nigerian Content Development in ICT).

	<p>nigérian de mise en oeuvre, Annexe C)</p> <p>2020 Politique et stratégie nationales en matière d'économie numérique</p> <p>Projet de stratégie nationale en matière de données</p>		<p>données en autorisant les transferts en dehors du Nigeria si les dispositions stipulées sont respectées.^{15 16}</p> <p>Le Décret de 2020 relatif à la présence économique significative dans le cadre de l'impôt sur le revenu des sociétés définit les conditions dans lesquelles les entreprises non résidentes sont assujetties à l'impôt sans exiger le stockage local des données.</p> <p>La construction de centres de données locaux a changé de motivation, passant de la localisation des données, assimilée à de la souveraineté en matière de données, au renforcement des capacités nationales afin de muer le Nigeria en une plaque tournante du marché africain des données, répondant aux besoins régionaux / continentaux en matière d'informatique dématérialisée. (Africa Data Center Map: Smart Africa, du Couëdic 2014). Ateliers intensifs avec les parties prenantes pour définir ses stratégies en matière d'IA et de données.</p>
--	---	--	---

¹⁵ Le transfert de données est autorisé si le destinataire des données est soumis à une loi, à des règles d'entreprise contraignantes, à des clauses contractuelles, à un code de conduite, à un mécanisme de certification qui assure un niveau de protection adéquat en ce qui concerne les données à caractère personnel. Les FDT sont également autorisés par la NDPA si la personne concernée donne son consentement, si le transfert est nécessaire à l'exécution d'un contrat, pour des raisons d'intérêt public, pour la protection des intérêts vitaux des personnes concernées ou d'autres personnes, etc.

¹⁶ La politique nationale en matière d'informatique dématérialisée prévoit que les institutions publiques fédérales feront appel à des fournisseurs de services dématérialisés qui stockent les données dans des juridictions ayant des niveaux de protection des données équivalents à ceux du Nigeria, avec des conseils de la NITDA sur les lieux de stockage de données acceptables. Cette politique impose par ailleurs la localisation de certaines données gouvernementales, exigeant que les informations confidentielles, sensibles et classifiées soient stockées sur place ou sur le territoire nigérian (Oloni 2024).

Mozambique	<p>Une loi sur la protection des données à caractère personnel est en cours de rédaction</p> <p>2021, Politique et stratégie nationales en matière de cybersécurité suite à la ratification de la convention de Malabo</p> <p>Lois sectorielles, par exemple les conditions strictes imposées par la Banque centrale au secteur bancaire</p>	<p>A signé et ratifié la convention de Malabo</p> <p>La loi type de la SADC sur la protection des données est prise en compte dans l'élaboration de la loi nationale sur la protection des données.</p>	<p>Met l'accent sur la cybersécurité, en couvrant des secteurs tels que la banque et la conservation, en vue d'éviter la liste noire de l'UE (Chevalier and Sciales 2023). Soutien pleinement la convention de Malabo considérée comme l'occasion de "contrôler les règles du jeu" et de parvenir à une gouvernance autonome (Fidler 2024). A également adhéré à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest). Considère que la souveraineté sur les données passe par leur localisation ; développe des centres de données nationaux dans le but de stocker les données localement.</p>
Sénégal	<p>2008 Décret sur la protection des données, portant également création d'une Commission des données personnelles (CDP)</p> <p>Stratégie "Sénégal numérique 2025" (SN2025)</p> <p>2023 nouveau projet de décret sur la protection des données</p> <p>2023 Stratégie nationale des données</p> <p>2023 Stratégie nationale de développement de l'IA</p>	<p>A ratifié la convention de Malabo</p> <p>Signataire de l'Acte additionnel de la CEDEAO sur les données à caractère personnel</p> <p>Stratégie nationale des données adoptée dans le droit fil du CSD de l'UA</p> <p>La CDP est membre du RAPDP/NADPA (Réseau africain des autorités de protection des données personnelles)</p> <p>La CDP est membre depuis 2014 de l'Association francophone des autorités de protection des données personnelles (AFAPDP)</p>	<p>Obligation de localiser les données pour contrôler la collecte, le stockage et le traitement des données sénégalaises conformément à la législation sénégalaise, suite aux instructions de l'ancien président.</p> <p>La stratégie nationale des données vise à exploiter les données en tant que catalyseur d'un développement socio-économique inclusif fondé sur la confidentialité, la transparence, l'équité et la sécurité (Houeto 2023). A également souscrit à la Convention 108 et à son protocole additionnel, renforçant ainsi son engagement en faveur de la protection des données.</p>

			La protection des données à caractère personnel est une priorité essentielle, avec des exigences strictes en matière de flux de données transfrontaliers. Des discussions sont en cours pour modifier et mettre à jour le décret de 2008 relatif à la protection des données, car celui-ci ne tient pas compte de l'évolution des données induite par les réseaux sociaux et parce qu'il convient de l'aligner sur d'autres avancées technologiques.
--	--	--	--

3.2. La façon dont sont définies les priorités de la politique nationale en matière de données

Au niveau national, l'élaboration des politiques est influencée par diverses motivations telles que le discours public, l'opinion des experts, l'influence des médias, les intérêts politiques et commerciaux, et cette liste n'est pas exhaustive. Non seulement ces facteurs interagissent et évoluent dans le temps, mais ils varient également d'un pays à l'autre, ce qui se traduit par des visions et des perspectives nationales différentes sur la question du partage des données. Des discussions cloisonnées ne font que compliquer davantage l'harmonisation de ces différentes visions.

3.2.1. Une vision nationale conditionnée par des intérêts économiques et politiques

Les politiques nationales en matière de données accordent souvent la priorité aux intérêts économiques et politiques. Dans les trois pays considérés, les discussions se concentrent principalement sur les cadres nationaux, les FDT intracontinentaux n'étant pas une priorité pour l'instant, malgré leur valeur économique reconnue.

Au Nigeria, la priorité politique consiste à encourager l'innovation locale et le développement économique. Certains secteurs sont soumis à des restrictions sur les FDT afin de créer plus d'opportunités pour les entreprises locales, notamment par le biais d'une obligation de localisation des données.¹⁷ Les experts critiquent toutefois ces mesures pour leur faible logique économique, compte tenu de l'insuffisance des infrastructures et de la cybersécurité, qui

¹⁷ Auparavant, les arguments souvent invoqués pour justifier le traitement et le stockage locaux des données étaient la protection des droits à la vie privée, le développement des TIC et des secteurs bancaires locaux, les avantages fiscaux et la protection de la souveraineté du Nigeria (Adeleke 2021 ; Beyleveld et Sucker 2022).

augmentent les coûts et réduisent les avantages (Adeleke 2021, Abdulrauf and Abe 2021).¹⁸ Sur la liste blanche des pays que le Nigéria considère comme sûrs pour le partage des données et qui n'est motivée que par des intérêts économiques et politiques, apparaissent en outre des pays comme le Bahreïn et les États-Unis, qui ne disposent d'aucune législation nationale solide sur la protection des données.

Dans d'autres cas, l'aspect économique n'est pas la motivation première du stockage local des données. Au Mozambique, le Centre national de biotechnologie et des sciences biologiques (CNBB) stocke les données localement, quels que soient les coûts induits, afin de protéger la confidentialité et la propriété intellectuelle de ces données. Le gouvernement s'efforce néanmoins d'accroître l'utilisation, actuellement faible (environ 50 %), de son centre national de données, soit en obligeant les institutions publiques à y stocker leurs données par décret national¹⁹ par exemple, soit en les persuadant de le faire par le biais de l'Institut national de l'administration en ligne (INAGE). L'Agence nationale pour le développement géospatial (ADE) a été mise en place à une vitesse impressionnante, l'État ayant un intérêt politique à renforcer sa capacité à évaluer la richesse des ressources naturelles du pays, même si l'agence a une mission beaucoup plus large. Cela montre que les intérêts politiques et économiques peuvent s'aligner sur l'objectif des FDT et qu'ils ne sont pas toujours pris en compte.

Par ailleurs, bien qu'il ait ratifié la convention de Malabo, le Mozambique ne figure pas sur la liste blanche du Botswana, qui préfère favoriser des partenaires commerciaux tels que l'Afrique du Sud et le Kenya. (Musoni 2022).

3.2.2. Influence extérieure et dépendance de trajectoire

Le contexte sénégalais est différent. En 2021, le pays a inauguré un centre de données national grâce à un financement chinois et des équipements de Huawei. Selon certains analystes, cette initiative a démontré l'attrait du modèle de gouvernance des données chinois qui "exige que tous les serveurs soient situés à l'intérieur des frontières d'un pays, ce qui permet à l'État d'avoir un accès total aux informations" (Olander 2021). Les progrès demeurent cependant limités en ce qui concerne le rapatriement et le stockage des données du secteur public dans les installations nationales, malgré les efforts déployés par l'ancien président Macky Sall. Les centres de données privés et certifiés sont, en revanche, largement utilisés.²⁰ Ce centre de données témoigne de la maturation des relations entre la Chine et les pays africains, qui passent ainsi du commerce et des prêts à des engagements plus politiques en s'inspirant de la sphère de la gouvernance qui était traditionnellement le pré carré de l'UE (Karkare et al.

¹⁸ Selon Stuart (2024b), "une caractéristique essentielle de l'Internet et sans doute l'une des plus mal comprises, c'est qu'il ne connaît pas de frontières. En Internet, même les sites web locaux d'un pays ou d'une ville, "n'existent" pas forcément à cet endroit. En fait, il est plus que probable qu'ils existent dans plusieurs endroits et plusieurs pays, même si leur hébergeur est une entreprise locale. Cela signifie que toute tentative visant à limiter les flux de données transfrontaliers, à localiser les données ou à imposer la localisation des centres de données se heurtera à d'importants problèmes pratiques et entraînera certainement des pertes d'efficacité et des augmentations de coûts".

¹⁹ [Regulation of the Electronic Government Framework](#).

²⁰ <https://uptimeinstitute.com/uptime-institute-awards/country/id/SN>

2020). Dans le même temps, le Sénégal a travaillé en étroite collaboration avec la GIZ et l'UE pour élaborer sa stratégie nationale des données²¹ qui met l'accent sur la protection et la sécurité des données à caractère personnel, preuve que la coopération avec la Chine dans un domaine n'exclut pas la coopération avec Team Europe dans un autre.

La dépendance de trajectoire, en vertu de laquelle les résultats du présent sont façonnés par des événements et des décisions du passé, rejaillit aussi sur la façon dont les cadres politiques et les structures institutionnelles se présentent dans un pays donné. Les règles de partage des données du Mozambique dans le secteur bancaire sont influencées par les pratiques portugaises et témoignent de son passé colonial et de ses relations économiques et commerciales actuelles. Comme dans de nombreux autres domaines politiques, le pays recherche plus souvent la collaboration en matière de données au sein de la Communauté des pays lusophones (CPLP) ou de son sous-groupe africain (PALOP).²² De même, les cadres réglementaires sénégalais s'apparentent quelque peu au système français.

La concurrence géopolitique entre les États-Unis, la Chine et l'UE influence indirectement les politiques nationales. Les liens commerciaux étroits avec l'UE incitent à adopter les approches européennes en matière de protection des données (Fidler 2024). Le Nigeria a accéléré l'adoption de sa loi sur la protection des données en raison des exigences liées aux prêts européens (Musoni, Domingo, and Ogah, 2023). La stratégie nationale du Mozambique en matière de cybersécurité, motivée par la nécessité d'éviter l'inscription sur la liste noire de l'UE, s'aligne sur la convention de Malabo et s'inspire de la législation portugaise (Chevalier and Sciales 2023).

3.2.3. Discussions cloisonnées et accords sectoriels fragmentés

La plupart des ministères, départements et organismes publics n'utilisent pas de données pour leurs prises de décision et fonctionnent de manière indépendante, la coopération et la communication étant limitées en raison d'une culture du secret et d'un manque de confiance. L'accès aux données d'une autre entité publique passe souvent par des procédures longues et hiérarchiques, ce qui retarde la prise de décision. Les discussions en vase clos et les approches fragmentées des institutions et des régulateurs à l'égard des FDT intracontinentaux risquent de faire obstacle à l'obtention d'informations intersectorielles essentielles.²³ C'est ce que montre l'amalgame entre la souveraineté des données et la localisation des données, récemment étudié par Soulé (2024).

Les décideurs politiques sont généralement enclins à traiter l'économie numérique de la même manière que l'économie des biens (physiques), ce qui a une incidence sur les FDT. Contrairement aux ressources industrielles traditionnelles comme le pétrole, les données sont

²¹ <https://smartafrica.org/senegal-unveils-its-national-data-strategy/>

²² La loi nationale mozambicaine sur la protection des données à caractère personnel, actuellement en cours de discussion, s'inspire des lois existantes dans d'autres pays lusophones, dont le Portugal, tout en s'alignant sur la convention de Malabo.

²³ La question des données fait l'objet de discussions dans divers domaines thématiques tels que le commerce numérique, la cybersécurité et l'IA au sein de comités d'experts distincts qui communiquent peu entre eux

inépuisables et non rivales, ce qui signifie que, plus on y accède et plus on les utilise, plus leur valeur augmente. Les politiques, en particulier l'interprétation de la souveraineté numérique, ont toutefois tendance à privilégier la monopolisation plutôt que le partage des ressources.

Dans la pratique, et malgré les défis évoqués précédemment, on constate un partage des données dans les trois pays considérés. Dans de nombreux cas, il est régi par des accords sectoriels, multilatéraux ou au niveau des entreprises. Ces accords comblent les lacunes des cadres nationaux en définissant des règles sectorielles pour les acteurs transfrontaliers. Le partage des données dans le secteur bancaire, par exemple, est régi par des règles et réglementations obligatoires (édictees par la banque centrale), tandis que la météorologie ou les données commerciales sont régies par des accords multilatéraux, et dans d'autres secteurs encore, tels que la conservation, le partage de données s'inspire des bonnes pratiques internationales (sur une base volontaire).

3.3. Défis dans la mise en œuvre

Une des critiques fréquemment entendues à propos des cadres politiques africains, c'est qu'en dépit d'un large éventail de bonnes politiques, la mise en œuvre reste déficiente, alors qu'on constate des défis communs à l'ensemble des pays. Une coordination nationale inefficace conduit à des mandats concurrents et à des incitations perverses qui détournent l'attention de la mise en œuvre. L'absence de mécanismes et de cadres clairs en matière de partage des données conduit à devoir se passer d'un train d'union important entre la politique et la pratique et à se heurter à un défi de mise en œuvre.

3.3.1. Une mauvaise coordination nationale, à l'origine de mandats concurrents et d'incitations aux effets pervers

Étant donné la nature transversale du partage des données, plusieurs entités sont concernées par son fonctionnement, ce qui peut engendrer des frictions. Au Mozambique, les politiques liées aux technologies de l'information sont du ressort du ministère des sciences et de l'enseignement supérieur, tandis que le ministère des transports et des communications supervise les télécommunications. Ce chevauchement crée une confusion entre l'autorité de régulation des télécommunications (INCM) et l'autorité de régulation des technologies de l'information (INTIC), au point de ne plus trop savoir qui fait quoi exactement. La situation est à peu près la même au Nigeria. La loi nationale sur la protection des données supervisée par la Commission nigériane de protection des données n'a pas abrogé le règlement national sur la protection des données qui relève de l'Agence nationale de développement des technologies de l'information (cf. tableau 3 ci-dessus), ce qui entraîne un chevauchement des mandats, bien que les deux organismes soient sous la tutelle du ministère fédéral de la communication, de l'innovation et de l'économie numérique.

Dans certains cas, les décisions politiques peuvent aussi créer des incitations aux effets pervers qui ont une incidence négative sur le partage des données. Citons par exemple des entités comme la Commission nationale de gestion de l'identité (NIMC) au Nigeria et l'Agence

nationale de la statistique et de la démographie (ANSD) au Sénégal, qui imposent des frais d'accès aux données parce qu'elles sont sous-financées par le gouvernement central; cette attitude démotive les parties prenantes qui voudraient accéder aux données et compromet leurs objectifs initiaux de partage des données.

3.3.2. Une mauvaise gouvernance des données et des mécanismes peu clairs

Une mise en œuvre efficace des politiques passe par des cadres et des mécanismes clairs, or ils font souvent défaut. La plupart des pays n'ont pas adopté de cadres solides de gouvernance des données, garants d'une utilisation efficace des données et des FDT. Un autre problème courant est celui de la capacité limitée à collecter des données de qualité. Les données gouvernementales sont souvent obsolètes ou peu fiables.²⁴ Les informations statistiques du Nigéria, par exemple, continuent de s'appuyer sur le recensement de 2006, qui est émaillé de sensibilités politiques (Akinyemi 2020; Eromosele 2023; Ndemo et al. 2023). La faiblesse de l'État de droit et de son application poussent davantage encore les citoyens à ne pas partager leurs données par crainte d'une utilisation abusive (Abebe et al. 2021).

Le manque d'interopérabilité entre des statistiques vitales telles que l'impôt sur le revenu, les transactions financières ou les données sanitaires constitue un autre frein à la fourniture des services publics. (Ndemo et al. 2023). C'est ce que l'on observe au Mozambique, où de nombreux systèmes sont mis en place dans le cadre d'initiatives soutenues par des partenaires de développement, sans que l'interopérabilité ne soit suffisamment prise en compte. Ceci peut occasionner des retards, des charges administratives et une augmentation des coûts dans le cas des agences douanières et commerciales. (Livre blanc sur l'IA). Dans de nombreux pays, la situation est encore plus grave, du fait qu'il n'existe pas de cadre national clair en matière d'accès aux données et de partage des données (Ndemo et al. 2023). À l'heure actuelle, seuls 12 pays africains ont élaboré des stratégies nationales en matière de données et/ou d'intelligence artificielle. Le manque de clarté des cadres entrave également le partage des données dans des domaines qui ne sont pas politiquement sensibles mais qui revêtent une importance stratégique, comme les données scientifiques et géospatiales, ce qui entraîne des dépenses inutiles pour l'acquisition de données existantes alors qu'elles existent déjà au niveau local ou qu'elles pourraient être réutilisées (Waruru 2023).

3.3.3. Une mise en application limitée

La mise en œuvre des cadres continentaux reste incomplète lorsqu'il n'y a pas de mise en application, laquelle est souvent victime de l'absence de régulateurs indépendants. Dans la pratique, le pouvoir d'exécution des régulateurs de données est mis à l'épreuve, en particulier lorsque des acteurs influents, notamment d'autres organismes publics ou de grandes entreprises technologiques, entrent en lice.

²⁴ Dans des pays comme la RDC, l'Érythrée et le Soudan du Sud, l'activité économique est mal mesurée en raison des conflits et des troubles politiques ou en raison de l'absence d'une méthodologie claire et d'une bonne compréhension du secteur informel. (Koch 2019). En Afrique, seuls trois pays sur quatre environ mettent à jour leurs données budgétaires, leurs lois nationales et leurs informations relatives aux marchés publics dans les délais impartis, tandis que la moitié seulement publient des registres électoraux actualisés ou tiennent à jour leurs registres d'entreprise (Lämmerhirt 2019).

La convention de Malabo laisse à chaque État membre le soin de créer des autorités de protection des données ainsi que les lois que ces autorités devront appliquer, sans prévoir de mécanismes de coordination et d'harmonisation suffisants entre les pays. De nombreux pays doivent encore transposer la convention dans leur droit national ou mettre en place des autorités nationales opérationnelles (King'ori 2024).

Le Nigeria et le Sénégal ont tous deux mis en place leurs régulateurs, à savoir la NDPC pour l'un et la CDP pour l'autre, mais la mise en application n'est pas uniforme. La NDPC a récemment été critiquée pour la clémence dont elle a fait preuve dans le traitement du dossier de [violation des données](#) à la NIMC au motif qu'il s'agissait d'une "consœur" (personne interviewée). La liste blanche du Nigeria a récemment été invalidée par la Haute Cour, qui a estimé que certains des pays figurant sur cette liste, comme le Mozambique, les Comores et la Guinée-Bissau, n'assuraient pas une protection adéquate des données à caractère personnel. Bien que signataires de la convention de Malabo, ces pays ne disposent ni de lois ni d'autorités en matière de protection des données, ce qui va à l'encontre des objectifs politiques du Nigeria visant à garantir à ces citoyens une protection adéquate de leurs données.²⁵

Au Mozambique, l'application de la loi s'est généralement avérée difficile en raison du manque de capacités (techniques, humaines et financières) de l'État. Du côté du Sénégal, l'application stricte de la loi par la CDP complique singulièrement le partage des données, même non personnelles, soumis à son autorisation. De précédentes études laissent à penser que des exigences strictes en matière de cybersécurité augmentent considérablement les coûts de mise en conformité, en particulier pour les petites et moyennes entreprises (Ryle et al. 2021 cités dans Lemma 2024) qui constituent la majeure partie du tissu économique africain.

4. Ce qu'il faut retenir des divergences entre les perspectives continentales et nationales en matière de flux de données

Les approches nationales en matière de FDT s'emploient à trouver un équilibre entre différents objectifs tels que la libre circulation des données, la localisation des données à des fins de souveraineté, la protection des données à caractère personnel et la cybersécurité, en tenant compte de considérations plus pratiques telles que les intérêts économiques et politiques, l'influence extérieure et la confiance. Ces objectifs étant hiérarchisés différemment dans chaque pays (le Nigeria, par exemple, met l'accent sur le rôle de la croissance économique, tandis que le Sénégal se concentre sur la protection des données à caractère personnel et le Mozambique sur la cybersécurité), il faudra éviter la fragmentation pour parvenir à une économie des données cohérente en Afrique. Mais la relation entre les politiques nationales et les politiques régionales / continentales ne dépend pas seulement de la façon dont ces pays perçoivent les cadres continentaux : elle dépend aussi de la façon dont les relations entre les différents pays, en d'autres termes l'intégration régionale, accordent aux cadres continentaux le pouvoir d'orienter les processus nationaux.

²⁵ The Incorporated Trustees of Ikigai Innovation Institute v. National Information Technology Development Agency FHC/ABJ /CS/1246/2022.

4.1. Des intérêts nationaux en concurrence avec les engagements pris au niveau continental

S'il est une chose que les études sur l'intégration régionale nous ont apprise, c'est que les intérêts nationaux éclipsent souvent les engagements pris au niveau continental (Byiers et al. 2021). C'est évident dans le cas des FDT, où les cadres nationaux priment sur les flux de données intracontinentaux (cf. 3.2.1). Les gouvernements donnent la priorité aux besoins nationaux immédiats, sous l'impulsion de dirigeants politiques en quête de légitimité et influencés par le lobbying des entreprises (Vanheukelom et al. 2016). Sur la liste blanche du Nigéria, par exemple, figurent des partenaires commerciaux dont les régimes de données sont moins protecteurs, ce qui montre bien que ce sont les intérêts économiques plutôt que la protection des données qui prennent le pas (cf. 3.2.1). Le manque de mise en application des règles continentales fait aussi que l'on profite souvent des failles du système pour poursuivre des intérêts nationaux. Il faut y voir le reflet d'un dilemme plus fondamental au niveau national : "pourquoi mettre en œuvre des accords [continentaux] lorsque le sentiment d'appropriation est limité et que les priorités sont ailleurs ?", ce qui témoigne d'une "crise de la mise en œuvre" et entrave, du coup, l'action collective (Miyandazi 2020).

D'autres facteurs peuvent également entraver les FDT intracontinentaux : les tensions politiques à l'intérieur du pays (les coups d'État ou les insurrections, par exemple), entre les pays (la concurrence commerciale ou d'autres formes de compétition ou de rivalité, par exemple), des héritages coloniaux créant une dépendance de trajectoire en termes de langue et de processus administratifs (cf. 3.2.2.) ou encore la variabilité des trajectoires de développement et de la solidité institutionnelle des systèmes (Brand et al. 2022). À titre d'exemple, citons le programme visant à faciliter le partage de données en vue d'une identification unique pour l'intégration régionale et l'inclusion en Afrique de l'Ouest, qui a été entravé par le fait que le partage des données, en particulier sur les mouvements transfrontaliers de personnes, a été jugé sensible en raison des problèmes de sécurité nationale découlant de l'instabilité politique dans la région (entretien).²⁶

4.2. Influence extérieure

N'oublions pas non plus que les pays africains effectuent la plupart de leurs échanges commerciaux et de données avec des partenaires situés en dehors du continent (Stuart 2024a) ce qui les incite à s'aligner sur des exigences externes (strictes). Les pays dotés de solides mécanismes de cybersécurité, conformes aux cadres internationaux tels que la Convention de Budapest, peuvent hésiter à partager des données avec d'autres États africains ne disposant pas de politiques similaires. Avec une conséquence importante : les solides mécanismes que certains pays ont instaurés pour faciliter les FDT avec des partenaires extérieurs sont les mêmes qui compliquent les FDT à l'intérieur du continent. De nombreux pays ont calqué leur législation sur le RGPD de l'UE, laquelle leur a apporté des formations et un

²⁶ Le programme WURI (West Africa Unique Identification for Regional Integration and Inclusion) de la CEDEAO a été financé par la Banque mondiale pour faciliter le partage et l'échange de données ainsi que les paiements numériques transfrontaliers grâce au développement d'une carte d'identité régionale.

soutien (le [Nigéria](#) et le [Kenya](#) notamment). Cela peut amener ces pays à privilégier l'alignement sur l'UE par rapport aux voisins régionaux qui n'ont pas adopté de réglementation calquée sur le RGPD, d'où un manque d'harmonisation au plan régional (Fidler 2024).

4.3. De longues négociations au niveau continental qui entraînent un manque d'alignement

De manière générale, les négociations au niveau continental se déroulent en parallèle des discussions et évolutions politiques au niveau national. Le fait qu'il faille plus longtemps pour boucler un accord continental et qu'un tel accord soit par nature un compromis entre les différentes positions des États membres explique en partie les failles dans les cadres continentaux et nationaux relatifs aux FDT. La convention de Malabo, par exemple, n'est entrée en vigueur que neuf ans après son adoption. Non seulement des discussions sont en cours en vue d'actualiser les dispositions de cette convention étant donné qu'au cours de cette période le paysage a considérablement évolué en termes de progrès numériques (Ifeanyi-Ajufo 2023; Carnegie 2023), mais au moins 34 pays disposaient d'une législation sur la protection des données, et 22 d'autorités de protection des données, avant même l'adoption de la convention.²⁷ Des pays comme l'Afrique du Sud étaient moins pressés de la ratifier car ils avaient déjà adopté une législation en matière de protection des données, la [Protection of Personal Information Act](#). D'où des divergences entre les cadres nationaux et continentaux.

4.4. Une coordination inefficace

Le manque de communication entre les entités continentales et nationales accentue le fossé. La procédure officielle de consultation formelle pour les politiques continentales commence par une note officielle, qui est d'abord transmise au ministère des affaires étrangères avant d'être envoyée au ministère responsable. Les retards dans la transmission des notes à l'agence responsable, sans parler de la concurrence des mandats (cf. 3.3.1.), conduisent à un désalignement, surtout lorsque les discussions sont cloisonnées (cf. 3.2.3.).

Dans d'autres cas, les processus nationaux peuvent être involontairement compromis par ces lenteurs administratives, même lorsque les données sont partagées. L'Institut national de météorologie du Mozambique (INAM), par exemple, fournit des prévisions météorologiques à diffuser dans le pays, mais à cause des retards dans la réception des prévisions effectuées parallèlement au niveau continental, on se retrouve avec deux corpus de données (parfois non concordantes).

4.5. Pas de véritables répercussions pour les États membres de l'UA

En règle générale, s'écarter de l'objectif ou de la vision continentale ne prête pas à conséquence pour les États membres de l'UA. Ces derniers considèrent par conséquent les organes continentaux comme des tigres de papier. L'UA et ses organes n'ont en effet pas le

²⁷ Voyez <https://dataprotection.africa/which-african-countries-have-a-data-protection-law/>

pouvoir de faire appliquer les accords continentaux sauf à ce qu'ils soient ratifiés par les États membres. Et même lorsque c'est le cas, ils n'imposent pas de mesures punitives aux pays qui ne respectent pas les dispositions convenues, comme celles de la convention de Malabo, par exemple. Il s'ensuit que l'accent est mis sur les déclarations politiques plutôt que sur la mise en œuvre effective.

4.6. Données lacunaires et faible demande de FDT

Même lorsque des cadres sont mis en place pour faciliter les FDT, il demeure important de considérer leur contenu, à savoir les données. De nombreux gouvernements africains fonctionnent avec des données obsolètes, incomplètes ou peu fiables (Chege and Wanjohi 2023, Lämmerhirt 2019; Glassman and Ezeh 2014) qui donnent lieu à une élaboration inefficace des politiques. Limiter le partage des données avec le grand public, c'est rater l'occasion de bénéficier de conseils ou d'analyses basées sur ces données, de la part de la société civile notamment. Du coup, la demande de partage de données, y compris via les FDT intracontinentaux, reste faible au final (Lämmerhirt 2019). Dans le même ordre d'idées, on constate un manque de compréhension de concepts tels que la création de valeur des données, la justice en matière de données et l'intendance des données.

5. Mesures stratégiques pour renforcer les FDT en Afrique

Garantir des flux de données sûrs et homogènes à travers l'Afrique nécessite des efforts concertés aux niveaux continental et national, avec un alignement et une harmonisation des politiques pour soutenir la vision de la ZLECAf et du MUN. Cet objectif peut être atteint grâce à une approche ascendante qui garantit l'adhésion des États membres. Le présent document décrit les mesures stratégiques à court, moyen et long-terme qui peuvent être mises en place pour renforcer les FDT en Afrique, en mettant l'accent sur des recommandations en direction de l'UA et de ses États membres. Certaines des recommandations politiques proposées se basent sur le CSD et visent à renforcer ou à mettre en évidence des principes clés pour l'UA et ses États membres.

5.1. Recommandations politiques en direction de l'UA

5.1.1. Établir un cadre de catégorisation et de partage des données pour les FDT

Une approche du type "panacée" du partage des données connaît ses limites en raison de la nature des types de données. Les données à caractère personnel (relatives à la santé, aux enfants ou à la situation financière) requièrent des garde-fous stricts, ce qui n'est pas forcément le cas des données à caractère non personnel (climatiques ou agricoles). L'UA et ses États membres devraient travailler main dans la main afin de développer des mécanismes de partage de données qui respectent ces distinctions et ces besoins, ce qui peut passer par la création de mécanismes sectoriels spécifiques pour les FDT. Dans le secteur agricole, par exemple, différents types de données pourraient être répertoriés et classés en fonction des

données non personnelles susceptibles d'être transférées en dehors du pays, sous certaines conditions.

5.1.2. Renforcer la capacité de mise en œuvre et de mise en application

Pour relever le défi que constitue le manque de mise en œuvre et de mise en application, l'UA devrait envisager la création d'un organe continental de protection des données (OCPD). À l'image du Conseil de protection des données de l'Union européenne, l'OCPD superviserait la mise en œuvre de la convention de Malabo et ferait respecter la protection des données sur l'ensemble du continent africain (Abdulrauf 2021). Cet organe expliquerait aux États membres comment interpréter ses propres dispositions relatives à divers instruments continentaux tels que la convention de Malabo, le PCN de la ZLECAf et le CSD, consulterait les autorités nationales chargées de la protection des données et renforcerait la cohérence réglementaire. À l'occasion de la révision de la convention de Malabo, l'UA devrait inclure des dispositions relatives à la création de l'OCPD. L'UA pourrait également solliciter le Réseau africain des autorités de protection des données personnelles (cf. 5.2.6.) pour la conseiller sur des questions telles que la composition, l'établissement, les fonctions, le mandat et la juridiction de l'OCPD.

5.1.3. Créer une task force ou un groupe de travail sur l'OCPD

Compte tenu de la rapidité de la transformation numérique en Afrique, il est essentiel de mettre en place des task forces ou des groupes de travail continentaux spécialisés, similaires à l'approche suivie par l'OCDE en matière de [libre circulation des données dans la confiance](#), qui se concentrent sur différents aspects des FDT, à savoir notamment les mécanismes de catégorisation des données et les normes de transfert. Un tel engagement garantirait la continuité de l'expertise et la cohérence dans l'élaboration des politiques en cas de changement de gouvernement ou d'équipe technique parmi les États membres.

5.1.4. Faciliter l'apprentissage entre pairs entre les États membres

L'apprentissage entre pairs et le partage d'expériences réussies peuvent inciter d'autres pays à s'aligner sur la vision continentale. Par exemple : la mise en œuvre de la stratégie sénégalaise en matière de données et d'IA a été facilitée grâce à un voyage d'étude effectué au Rwanda en décembre 2023. Ce voyage était dirigé par le ministère sénégalais de la communication, des télécommunications et du numérique, avec le soutien de Team Europe, de la GIZ et du Hub D4D UA-UE. De même, le ministère béninois de la numérisation a participé à un atelier de validation à Accra pour s'informer de la stratégie nationale de données du Ghana et de son processus de développement inclusif.

5.2. Recommandations politiques en direction des États membres de l'UA

5.2.1. Gouvernance

Harmoniser les perspectives politiques : les États membres devraient aligner leurs politiques nationales sur la vision continentale de l'UA en matière de FDT. Ils devront pour ce faire élaborer

ou actualiser leur législation afférente à la protection des données, au commerce électronique, à la cybersécurité et à l'intelligence artificielle afin de l'aligner sur les politiques continentales. Des pays comme le Mozambique, qui n'ont pas de politiques numériques, devraient élaborer des cadres globaux, tandis que d'autres, qui disposent déjà de politiques, comme le Nigeria et le Sénégal, devraient les réviser et les mettre à jour de manière à s'aligner sur la vision continentale. Pour comprendre l'impact des FDT, les politiques sectorielles doivent être réévaluées afin d'identifier les priorités, les domaines d'alignement ou l'absence d'alignement.

Alignement plus large de la politique numérique : les États membres devraient étudier par quels voies et moyens les bonnes pratiques internationalement reconnues en matière de protection des données, telles que la Convention 108+ et le RGPD, pourraient être adaptées à leur contexte local et élaborer des politiques nationales qui s'alignent également sur des cadres plus larges de partage des données. L'alignement de la politique numérique devrait s'étendre à d'autres domaines politiques tels que la concurrence, le commerce, la propriété intellectuelle et la fiscalité. Cela nécessiterait une forte coordination intersectorielle et un engagement multipartite afin d'éviter les approches cloisonnées. En outre, la collaboration entre les autorités en charge de la protection des données et les régulateurs de la concurrence pourrait contribuer à relever les défis posés par les flux de données transfrontaliers et à élaborer des pratiques réglementaires cohérentes.

Prendre des mesures pour pallier les lacunes en matière de données : les pays africains doivent améliorer leurs pratiques de gouvernance en matière de données afin de garantir l'accessibilité des données et de promouvoir leur intégration et leur interopérabilité. En développant des stratégies de données internes et des cadres de gouvernance, les institutions publiques peuvent générer des données fiables et actualisées tout en maximisant un emploi efficace des données et la conformité avec les réglementations et les politiques pertinentes (Saturday et Nyamwire 2023). On fait de plus en plus appel à des sources de données non traditionnelles pour résoudre les problèmes nationaux. Au cours de la COVID-19, le Nigeria s'est servi de données satellitaires et géospatiales pour estimer la pauvreté dans les zones urbaines et identifier les bénéficiaires éligibles à la sécurité sociale et aux fonds de secours de la COVID-19, grâce à un effort conjoint du bureau national de coordination des filets de sécurité sociale, d'un développeur d'IA et d'entreprises de télécommunications (GPAI 2021). Les politiques devraient inclure de nouvelles formes de données issues de la télédétection, de l'imagerie satellitaire, des capteurs, des réseaux sociaux, des dispositifs de communication, etc. (Ndemo et al. 2023). L'Afrique du Sud est un exemple à suivre à cet égard.²⁸ L'accent devrait être mis sur l'amélioration de la qualité des données ainsi que sur l'augmentation de la demande d'utilisation des données en intégrant les principes d'égalité numérique et de justice en matière de données, en fonction des capacités de l'État.

²⁸ Le plan stratégique 2020/21-2024/25 de l'Office national de la statistique sud-africain met l'accent sur l'intégration de données provenant de différentes sources, la recherche de collaborations avec d'autres producteurs de données pour l'analyse des données existantes, et l'étude du recours à des sources de données alternatives (Statistics South Africa 2020).

5.2.2. Facteurs favorables

Construire/utiliser une infrastructure de données sur le continent : l'essor économique et la souveraineté numérique passent par le développement d'infrastructures de données locales (Livre blanc de l'AUDA NEPAD sur l'IA; Musoni and Snail 2023).²⁹ Les pays africains devraient investir dans des centres de données et améliorer l'efficacité énergétique, les mesures de cybersécurité et la culture numérique pour soutenir le développement des infrastructures de données. Les efforts devraient se concentrer sur les pôles émergents en Afrique du Sud, au Nigeria, au Ghana, en Égypte, en Algérie et au Maroc (Livre blanc de l'AUDA NEPAD sur l'IA), et être assortis de mesures d'accompagnement pour s'attaquer à des obstacles structurels tels que la fourniture d'une alimentation électrique fiable, l'amélioration de l'efficacité énergétique, l'augmentation de la connectivité internet, l'amélioration des compétences en matière de culture numérique, et la garantie d'une cybersécurité forte. L'Alliance Smart Africa recommande de faciliter les affaires et l'acquisition de terrains pour les centres de données, de mobiliser des fonds et de promulguer des lois appropriées sur la gouvernance et la protection des données (Smart Africa 2022).

Renforcer la cybersécurité : le renforcement des capacités en matière de cybersécurité est essentiel pour protéger l'économie numérique africaine des menaces. Alors que les risques d'atteinte à la vie privée, d'utilisation abusive et d'exploitation ne font que croître, seul un cinquième des pays africains répondent aux exigences standard en matière de lutte contre la cybercriminalité (CSEA 2021) par manque d'expertise et de ressources et à cause de leur dépendance technologique (Diorio-Toth 2023). Les États membres devraient adopter des stratégies globales de cybersécurité, instaurer des lois nationales sur la cybercriminalité conformes à la [Ligne directrice pour une loi type sur la cybersécurité](#) et adopter la [Déclaration de Lomé](#) sur la lutte contre la cybercriminalité. Ils devraient également mettre en place des équipes d'intervention en cas d'incident lié à la cybersécurité et aligner leurs efforts sur le processus entrepris par les Nations unies en vue d'élaborer un [traité mondial sur la cybercriminalité](#). La collaboration avec des pays dotés de cadres de cybersécurité matures, comme l'île Maurice, le Maroc, l'Égypte et le Ghana, peut servir de modèle (Ifeanyi-Ajufo n.d.).

5.2.3. Capacités et compétences

Organiser une formation de sensibilisation des parties prenantes : pour promouvoir la culture des données, il faut un plaidoyer continu et un renforcement des capacités des parties prenantes afin de les sensibiliser à l'exploitation des données comme s'il s'agissait du "nouveau pétrole" (Boateng 2022), ainsi qu'aux opportunités et avantages déjà offerts par les FDT. Les pouvoirs publics devraient proposer des formations sur l'analyse des données, la gouvernance et l'économie numérique aux petites entreprises, aux régulateurs et aux jeunes. La collaboration avec des groupements de la société civile peut renforcer la sensibilisation aux droits relatifs aux données ainsi qu'aux avantages du partage transfrontalier des données.³⁰

²⁹ L'Afrique est actuellement le continent qui compte le moins de centres de données au monde. Sur le continent africain, certains pays comme l'Afrique du Sud ont un marché de centres de données important et cumulent environ deux tiers de la capacité totale du continent, alors que l'Afrique de l'Ouest représente moins de 10 % de la capacité totale des centres de données (Augustine 2022).

³⁰ Paradigm Initiative. KictaNET, Pollicy, MISA, etc.

Renforcer les capacités institutionnelles : la mise en place d'autorités indépendantes chargées de la protection des données est essentielle si l'on veut faire respecter une législation solide en matière de protection des données et préserver la confidentialité des données. La consultation de l'autorité nationale est cruciale lors de la définition d'une liste blanche des pays avec lesquels s'effectuera le partage des données, lors de l'instauration de mécanismes de transfert transfrontalier de données ou lors de l'élaboration de politiques et de stratégies afférentes aux données.

Ces instances doivent disposer de ressources suffisantes et être habilités à contrôler le respect de la législation et à traiter efficacement les questions de protection des données : le Nigeria, le Sénégal, l'Afrique du Sud, le Kenya, le Ghana, le Zimbabwe et l'île Maurice ont mis en place des organismes de protection des données, mais celles-ci manquent souvent de ressources et d'indépendance financière, ce qui affecte leur capacité à faire respecter les règles et à traiter efficacement les questions sensibles de protection des données (Boateng 2022, ALT Advisory, King'ori and Dorwart 2022).

L'adhésion au [Réseau africain des autorités de protection des données personnelles](#) peut faciliter la coopération régionale en matière de protection des données et de FDT, comme cela a été souligné lors d'une récente [assemblée générale annuelle](#). Les accords bilatéraux, comme ceux conclus entre l'Afrique du Sud et l'eSwatini, renforcent la coopération réglementaire et profitent des avantages des accords multilatéraux ([Régulateur sud-africain de l'information et Commission des communications de l'eSwatini](#)).

5.2.4. Utilisation des données

Soutenir les initiatives en matière de données ouvertes : ces initiatives peuvent améliorer la transparence, la fourniture de services publics et l'innovation (The African Open Data Report 2017; [Banque mondiale](#), CSEA 2021). Les gouvernements devraient créer des environnements favorables aux plateformes de données ouvertes ([Data 4 Development](#)) et s'assurer que les données sont à jour (Rapport de novembre 2023 de la GPAI) tout en expérimentant les données dans des secteurs comme la santé, l'agriculture et le climat. Au Sénégal, par exemple, Orange-Sonatel a exploité les données de ses clients, y compris les enregistrements des téléphones mobiles et les données des réseaux sociaux, pour mieux comprendre les migrations liées au climat ([Data Pop Alliance](#)). [John Hopkins et son tableau de bord de la COVID-19](#) ont facilité le partage d'informations sanitaires essentielles pendant la COVID-19. Des initiatives telles que l'[Open Data Initiative](#) du Kenya, l'[Open Data Portal](#) de l'Afrique du Sud et l'[Open Data Portal](#) de l'Office national ougandais de la statistique illustrent les efforts déployés pour promouvoir un accès transparent aux données, mais elles se heurtent souvent à l'irrégularité des mises à jour. Les plateformes non gouvernementales telles que le [CGIAR](#) et [Masakhane](#), qui se concentrent respectivement sur l'agriculture et la préservation des langues africaines, témoignent également de la valeur des données ouvertes.

L'initiative ADLI (African Data Leadership Initiative) a été lancée par Smart Africa, la Commission économique pour l'Afrique des Nations Unies et Digital Impact Alliance <https://dial.global/work/adli/>. Open Knowledge International <https://okfn.org/en/>. Open Data Institute <https://theodi.org/>. World Wide Web Foundation. Open Data Day <https://opendataday.org/>.

Expérimenter des structures innovantes : les pays africains peuvent aussi tester des approches innovantes telles que le développement de fiduciaires de données, qui permettent aux communautés d'utiliser collectivement des données au profit de chacun et d'affirmer un pouvoir collectif (Olorunju and Adams 2022). Comme on l'a vu au Kenya, ces structures ont permis à des communautés rurales d'accéder à des informations vitales sur les sources d'eau disponibles, les équipements collectifs, les pénuries d'eau ressenties et les relations entre agriculteurs et éleveurs par l'intermédiaire de gestionnaires de données communautaires. Les données générées ont ensuite été utilisées pour identifier les infrastructures hydrauliques non fonctionnelles et attirer davantage d'investissements dans la réparation des puits de forage ([Data to Policy](#)). Il importe cependant de trouver des moyens de partager des données propriétaires à des fins sociales et publiques sans compromettre la viabilité commerciale ni les intérêts liés à la propriété intellectuelle (Tshuma 2024). Il est essentiel de poursuivre des recherches sur les nouveaux modèles de partage des données, y compris les fiduciaires de données et l'intendance, afin d'évaluer les opportunités et les risques associés (GPAI 2023). La collaboration avec des partenaires de développement comme la Banque mondiale, la Banque africaine de développement, l'UNECA et des homologues africains qui réussissent à mener des initiatives en matière de données ouvertes peut améliorer le partage des connaissances et accélérer l'adoption des bonnes pratiques en matière de gouvernance des données ouvertes sur l'ensemble du continent.

6. Quel rôle l'UE peut-elle jouer pour soutenir les flux de données transfrontaliers en Afrique ?

L'UE est un partenaire commercial majeur des pays africains et investit de manière significative dans l'économie numérique de l'Afrique, qui recouvre à la fois les infrastructures matérielles et immatérielles, y compris les systèmes de données. Pour renforcer ce partenariat et soutenir les FDT en Afrique, l'UE peut s'appuyer sur le pilier numérique de Global Gateway par l'intermédiaire de ses initiatives Team Europe (TEI) et communiquer les enseignements qu'elle tire de ses efforts en matière de partage des données européennes.

Soutenir les initiatives de partage de données en Afrique est conforme à l'objectif de l'UE de mener la coopération internationale en matière de données, d'élaborer des normes mondiales et de favoriser le développement économique et technologique dans le strict respect du droit de l'UE (CE 2020). En effet, l'UE aide déjà l'UA et ses États membres à élaborer des politiques en matière de données par le biais de l'initiative "Data Governance in Africa" (D4D Hub n.d.). Ce soutien vise à créer une économie africaine fondée sur les données au bénéfice de ses citoyens et de ses entreprises (CE 2020).

6.1. Contexte : la Stratégie européenne pour les données

La Stratégie européenne pour les données vise à faciliter la libre circulation des données au sein de l'UE sur la base d'une protection harmonisée des données à caractère personnel et de normes communes pour toutes les données, en vue d'un marché unique numérique encore

en chantier. Elle propose des mesures qui visent à accroître l'utilisation et la demande de données et de produits et services fondés sur les données dans l'ensemble du marché unique (CE 2020).

La Stratégie européenne pour les données a été suivie par l'Acte européen sur la gouvernance des données (AGD), le Règlement sur les données et le Règlement sur le libre flux des données à caractère non personnel. Avec le RGPD, ces textes constituent le cadre juridique présidant au développement d'un marché européen des données en pleine évolution.

- L'AGD établit des mécanismes assurant un partage de données et des intermédiaires de données fiables, afin de créer un environnement sûr et transparent pour les flux de données transfrontaliers et intersectoriels (UE 2022).
- Le Règlement sur les données favorise l'innovation et la concurrence, en permettant aux entreprises, aux consommateurs et aux entités publiques d'accéder aux données générées par des appareils et des services (UE 2023)
- Le Règlement sur le libre flux des données à caractère non personnel (UE 2018)

Pour unifier le marché des données, l'UE développe également des espaces de données : des environnements sécurisés pour le partage de données dans des secteurs tels que la santé, la finance, l'énergie et l'agriculture. Ces espaces garantissent des niveaux élevés de confidentialité, de sécurité, de disponibilité des données, d'interopérabilité et d'innovation. Ils se concentrent sur un certain nombre de secteurs, dont la santé, la finance, l'énergie et l'agriculture (CE 2024).

Au niveau mondial, la Stratégie européenne pour les données représente une approche globale des FDT. L'initiative japonaise du G20 "Data Free Flow with Trust" poursuit des objectifs similaires, bien qu'à un niveau plus international, mais ne dispose pas de solides cadres juridiques et structures de mise en œuvre de l'UE, préférant s'appuyer sur la coordination des politiques entre les membres du G7 (Digital Agency Japan n.d.).

6.2. L'Action pour une gouvernance des données en Afrique subsaharienne

"L'Action de l'UE pour une gouvernance des données en Afrique subsaharienne" entend aider l'UA à développer un marché des données comparable à celui de l'UE, ouvrant la voie à la libre circulation des données entre les régions. Cette initiative se concentre sur la gouvernance (au niveau continental et national), les infrastructures (notamment les centres de données) et les cas d'utilisation des données, avec un budget de plus de 50 millions d'euros abondé par l'UE (30 millions d'euros), le BMZ (20 millions d'euros) et le ministère français de l'Europe et des Affaires étrangères (un peu moins de 0,5 million d'euros), pour la période allant de janvier 2023 à juillet 2026.

L'objectif global est de favoriser une économie des données axée sur le développement et l'humain en Afrique, dans le droit fil du CSD de l'UA. Il s'agit de renforcer les politiques et les réglementations relatives aux données à caractère personnel et non personnel, d'exploiter les données pour alimenter les réglementations sectorielles et d'élaborer des propositions d'investissement finançables par les banques pour des infrastructures de données sûres et

durables par l'intermédiaire de la Facilité d'investissement numérique accessible aux financeurs européens.

Cette action s'appuie sur un projet financé par le BMZ, dans le cadre duquel le projet Datafication de la GIZ a concouru à l'élaboration du CSD. La GIZ continue de fournir une assistance technique à l'UA et à ses États membres pour l'élaboration de politiques et de réglementations. La GIZ aide également l'UA à apporter une assistance technique aux États membres par le biais de son réseau de centres de transformation numérique à travers l'Afrique. Aux côtés de Smart Africa et de Data Pop Alliance, la GIZ a notamment aidé le ministère sénégalais des TIC à élaborer sa stratégie nationale des données, tandis qu'Expertise France et D4D Hub concouraient à sa stratégie nationale de développement de l'IA. Le [Ghana](#) bénéficie d'un soutien similaire, et d'autres États comme la Zambie ou le Bénin ont également demandé à pouvoir en bénéficier.

D'autres programmes de Team Europe et des États membres complètent cette action. [L'initiative FAIR Forward](#) de la GIZ, qui se concentre sur l'IA, collabore avec le ministère sud-africain des forêts, de la pêche et de l'environnement afin de mettre les données au service de l'action climatique et de soutenir la transition juste du pays. De même, l'initiative [Data4Policy](#) du BMZ identifie les données manquantes à l'élaboration des politiques et met au point des formations pour les responsables politiques. La prochaine initiative de Team Europe, Safe Digital Boost with Africa, apportera un soutien aux régions africaines dans les domaines de la cybergouvernance, du commerce électronique et de la cybersécurité, en s'alignant probablement sur l'Action pour une gouvernance des données.

6.3. Recommandations en direction de l'UE

Le modèle de gouvernance de l'UE est un atout majeur, qui a permis de promouvoir une approche réglementaire forte de la gouvernance numérique grâce à l'"effet Bruxelles". De nombreux États africains ont calqué leur législation afférente à la protection des données sur des réglementations européennes, telles que le RGPD, plutôt que de développer leurs propres approches. Toutefois, il est essentiel que l'UE et ses États membres reconnaissent le fonctionnement unique des institutions africaines et soutiennent leur évolution numérique.

Au titre du pilier numérique de la Global Gateway, Team Europe s'est engagée à accroître les investissements dans la connectivité numérique, y compris dans des centres de données. Il sera essentiel de tenir cette promesse pour montrer que l'UE peut offrir des infrastructures indispensables, parallèlement au soutien qu'elle apporte en matière de gouvernance numérique et d'environnement réglementaire. L'expérience acquise par l'UE dans le développement d'espaces de données est un exemple précieux pour les régions qui souhaitent établir leurs FDT.

6.3.1. Gouvernance

Team Europe apporte déjà son soutien au CSD de l'UA et établit des liens avec le PCN de la ZLECAf. Il faudrait s'employer en permanence à favoriser une meilleure coordination entre les

acteurs continentaux africains afin de faciliter la cohérence des politiques relatives aux FDT. Il s'agit notamment de faciliter l'échange d'informations entre l'UA, le secrétariat de la ZLECAf, Smart Africa, les CER et les États membres. L'apport d'un soutien à des événements tels que le Forum sur la gouvernance des données et l'innovation pour l'Afrique peut s'avérer crucial à cet égard.

Au niveau des États membres, Team Europe devrait adopter une **approche globale de la mise en œuvre** en soutenant des processus inclusifs qui s'alignent sur les stratégies continentales, s'appuient sur les écosystèmes locaux et prennent en compte les priorités, les défis et les opportunités au niveau local. Il est essentiel de **garantir l'appropriation locale** par le biais d'une approche multipartite, comme le démontrent les réglementations numériques de l'UE élaborées à la suite de consultations avec le secteur privé, la société civile et des groupes de citoyens. Le partenariat UE-UA offre un véritable potentiel d'accompagnement au service de processus d'élaboration des politiques numériques centrés sur l'humain et inclusifs (Abah et al. 2022).

Autant le partage d'expériences peut être essentiel à l'apprentissage entre pairs, autant un copier-coller du modèle européen à d'autres régions serait illusoire compte tenu des différences de capacités et d'intérêts, **sans parler des différences culturelles et juridiques qui doivent être prises en compte**. D'autres pays peuvent plaider en faveur d'une approche plus collective de la protection des données et, dans le cas du CSD de l'UA, d'un intérêt plus marqué pour le concept de justice en matière de données, qui vise à prévenir les discriminations et les injustices ultérieures par le biais de la classification des données.

Le renforcement des capacités peut aider les autorités locales à mieux mettre en œuvre les réglementations et les politiques, gages d'une gouvernance durable aux niveaux continental et national.

6.3.2. Infrastructures

Dans le cadre de la Global Gateway, Team Europe s'emploie déjà à généraliser le financement d'infrastructures de données en Afrique afin de remédier à d'importantes inégalités, la Facilité d'investissement numérique développant des projets susceptibles d'être financés par les institutions financières européennes. Cet effort suppose une connaissance approfondie des écosystèmes locaux et une approche ascendante de la création de coalitions (Bilal, Teevan and Tilmes 2024).

Les investissements dans les infrastructures de données doivent **être assortis de mesures garantissant leur utilité pour l'économie locale**. Il s'agit notamment d'aborder les questions de sécurité et d'accessibilité financière au travers d'interventions réglementaires, de mesures de cybersécurité et de renforcement des capacités. Team Europe **devrait renforcer son soutien aux gouvernements africains pour qu'ils adoptent des infrastructures sûres et sécurisées de partage des données**. Le développement d'un marché des données significatif en Afrique nécessite des investissements, afin de rendre les données des pouvoirs publics utilisables et partageables, car les pouvoirs publics demeurent les principaux producteurs de

données. Les investissements devraient faciliter le partage sécurisé des données des administrés, entre les organismes publics et au-delà.

6.3.3. Cas d'utilisation

Dans le cadre de l'Action pour une gouvernance des données, Team Europe soutient le développement de cas d'utilisation en Afrique et entend multiplier les initiatives locales. Parmi les actions clés figurent :

- **Le partage d'expérience** dans la mise en œuvre d'espaces de données au sein de l'UE, qui peut servir de modèle au déploiement des FDT dans d'autres régions et faire progresser des initiatives internationales telles que Data Free Flow with Trust.
- **Le financement ciblé de projets spécifiques**, tels que la numérisation des bureaux nationaux de la statistique afin de générer des données précises, actualisées et fiables, le financement de cas d'utilisation engendrant de la valeur de données, le financement d'initiatives de données ouvertes, ainsi que la mise en place et le fonctionnement d'autorités de protection des données et de bureaux d'IA dans les pays africains.

Références

- Abah, J., Baptista, K., MacKenzie, C., Varghese, A. 2022. *Putting People at the Centre of Digital Policy. Mechanisms for Citizen Engagement in Nigeria*. Chapter in Daniels, C., Erforth, B., & Teevan, C. (Eds.). *Africa–Europe Cooperation and Digital Transformation* (1st ed.). Routledge. <https://doi.org/10.4324/9781003274322>.
- Abdulrauf, L. 2021. *Giving “teeth” to the African Union towards advancing compliance with data privacy norms*. Article, Department of Public Law, University of Ilorin, Nigeria and Institute for International and Comparative Law in Africa (ICLA), Faculty of Law, University of Pretoria, South Africa.
- Abdulrauf, L. 2024. *African Approach(es) to Data Protection Law*. In R. Atuguba Akongburo, P. Boshe, S. Dei-Tutu & M. Hennemann (Ed.), *African Data Protection Laws: Regulation, Policy, and Practice* (pp. 31-54). Berlin, Boston: De Gruyter. <https://doi.org/10.1515/9783110797909-005>.
- Abdulrauf, L. and Abe, O. 2021. *The (Potential) Economic Impact of Data Localisation Policies on Nigeria’s Regional Trade Obligations*. Johannesburg: Mandela Institute.
- Abebe, R., Kingsley, S., Aruleba, K., Obaido, G., Sadagopan, S., Birhane, A., Remy, S. L. 2021. *Narratives and Counternarratives on Data Sharing in Africa*. FAcCT ’21, March 3–10, Virtual Event, Canada.
- Adeleke, F. 2021. *Exploring Policy Trade-Offs for Data Localisation In South Africa, Kenya And Nigeria*. Johannesburg: Mandela Institute.
- Akinyemi, A. 2020. *Nigeria’s census has always been tricky: why this must change*. The Conversation
- Arnold, S. 2024. *Africa needs China for its digital development – but at what price?* Article, The Conversation.
- Atuguba Akongburo, R., Boshe, P., Dei-Tutu, S. and Hennemann, M. 2024. *African Data Protection Laws: Regulation, Policy, and Practice*. Berlin, Boston: De Gruyter. <https://doi.org/10.1515/9783110797909>.
- Augustine, A. 2022. *The Next Wave: A data centre roadmap for Africa*, Article, Techcabal.
- Ayalew, Y. E. 2022. *The African Union’s Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?* Blog of the European Journal of International Law, EJIL Talk.
- Banque mondiale. 2022. *A Digital Stack For Transforming Service Delivery: ID, Payments, and Data Sharing*. Practitioner’s note, ID4D AND G2PX, Washington, DC: Banque mondiale.
- Beyleveld, A. 2021. *Data Localisation In Kenya, Nigeria And South Africa: Regulatory Frameworks, Economic Implications And Foreign Direct Investment*. Policy Brief 07, Johannesburg: Mandela Institute.
- Beyleveld, A. and Sucker, F. 2022. *Cross-Border Data Flows in Africa: Policy Considerations for the AFCFTA Protocol on Digital Trade. Report*, Johannesburg: Mandela Institute.

-
- Beyleveld, A. and Sucker, F. 2024. *African rules on cross-border data flows: The significance of regulatory convergence and the ZLECAf Digital Trade Protocol's potential contribution*. <http://dx.doi.org/10.2139/ssrn.4741632>.
- Bilal, S., Teevan, C. and Tilmes, K. 2024. *Financing inclusive digital transformation under the EU Global Gateway*. ECDPM Discussion Paper 370. Maastricht: ECDPM.
- Boateng, R. 2022. *Data-Driven Enterprises in Africa: An Evaluation of Winners and Losers*. Abuja: CSEA AFRICA - CENTRE FOR THE STUDY OF THE ECONOMIES OF AFRICA.
- Brand, D., Singh, J. A., McKay, A. G. N., Cengiz, N. and Moodley, K. 2022. *Data sharing governance in sub-Saharan Africa during public health emergencies: Gaps and guidance*. South African Journal of Science, 118(11-12), 1-6. <https://dx.doi.org/10.17159/sajs.2022/13892>.
- Byiers, B., Apiko, P. and Karkare, P. 2021. *The ZLECAf and industrialisation: from policy to practice*. ECDPM Discussion Paper 314. Maastricht: ECDPM.
- Carnegie. 2023. *Continental Cyber Security Policymaking: Implications of the Entry Into Force of the Malabo Convention for Digital Financial Systems in Africa*. Event, Washington, DC: Carnegie Endowment for International Peace.
- CE. non daté. *Stratégie européenne pour les données. Faire en sorte que l'UE devienne un modèle et un acteur majeur d'une société dont les moyens d'action sont renforcés par les données*. Commission européenne.
- CE. 2020. *Une stratégie européenne pour les données*. Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions . COM/2020/66 final, Commission européenne.
- CE. 2024. *Shaping Europe's digital future*.
- Chege, Z. M. and Wanjohi, P. M. 2023. *A Value Chain Approach to Data Production, Use, and Governance for Sound Policymaking in Africa*. Chapter 3 in B. Ndemo et al. (eds.), *Data Governance and Policy in Africa, Information Technology and Global Governance*, https://doi.org/10.1007/978-3-031-24498-8_3.
- Chevalier and Sciales. 2023. *EU updates AML/CFT blacklist and adds five countries*. Article, Luxembourg: Chevalier and Sciales.
- CIPIT. 2024. *Commentary on the ZLECAf Digital Trade Protocol*. Youtube video, Centre for Intellectual Property and Information Technology Law.
- CSEA. 2021. *Strengthening Data Governance In Africa*. Project Inception Report, Abuja: Centre for the Study of the Economies of Africa.
- D4DHub. n. d. *Data Governance in Africa*. Website page.
- Diorio-Toth, H. 2023. *Five unique cybersecurity challenges in Africa*. Article, Kigali: Carnegie Mellon University Africa.
- du Couëdic, T. 2014. *Djibouti wants to be a global digital hub*. Article, African Business.
- Endeavor Nigeria. 2022. *The Inflection Point: Africa's Digital Economy is Poised to Take Off*. Blog.
- Eromosele, F. 2023. *It's disappointing Nigeria hasn't conducted census in 17 years — Sen Ningi*. Vanguard
- Fidler, M. 2024. *African Data Protection Laws: Politics, But as Usual*. In R. Atuguba Akongburo, P. Boshe, S. Dei-Tutu & M. Hennemann (Ed.), *African Data Protection Laws: Regulation, Policy,*

-
- and Practice (pp. 55–74). Berlin, Boston: De Gruyter. <https://doi.org/10.1515/9783110797909-006>.
- Gathii, J. T. 2024. *The ZLECAf's Digital Trade Rules are Not Fit for Africa*. Analysis, Afronomicslaw.org.
- Glassman, A. and Ezeh, A. 2014. *Delivering on a Data Revolution in Sub-Saharan Africa*. Brief, Washington, DC: Center for Global Development.
- GPAI. 2023. *The Role of Government as a Provider of Data for Artificial Intelligence: Interim Report*. November 2023, Global Partnership on AI.
- GSMA. 2021. *Cross-Border Data Flows The impact of data localisation on IoT*. Report, London: GSMA.
- Houeto, C. 2023. *Protection des données et transparence: Le Sénégal lance sa Stratégie nationale des données*. Article, Africa Cybersecurity Magazine.
- Ifeanyi-Ajufo, N. N.d. *"The current state of cybersecurity in Africa is the tendency towards a cyber-militarisation approach"*. Interview, Oxford: Global Economic Governance Programme, Blavatnik School of Government.
- Ifeanyi-Ajufo, N. 2023. *Africa's Cybersecurity Treaty enters into force*. Commentary, Directions.
- Ifeanyi-Ajufo, N. 2024. *The AU took important action on cybersecurity at its 2024 summit – but more is needed*. Article, Chatham House.
- Jaïdi, L., Byiers, B. and El Yamani, S. 2024. *Fostering investment and inclusivity in the African Continental Free Trade Area*. ECDPM Briefing Note 182. Maastricht: ECDPM.
- Kilic, B. 2024. *ZLECAf and digital governance*. Centre for International Governance Innovation.
- King'ori, M. 2024. *RECs: Towards a Continental Approach to Data Protection in Africa Perspectives from Privacy and Data Protection Harmonization Efforts in Africa*. Global report, Washington, DC: Future of Privacy Forum.
- King'ori, M. and Dorwart, H. 2022. *A Look into DPA Strategies in the African Continent*. Washington, DC: The Future of Privacy Forum (FPF).
- Koch, T. 2022. *Better data is the key to unlocking major investment in Africa*. Article, Atlantic Council's Africa Center.
- Lämmerhirt, D. 2019. *How open is government data in Africa?* Blog, Open Knowledge.
- Miyandazi, L. 2020. *The African Union should work on policy implementation to realise its ambitions*. Blog, London: LSE.
- Musoni, M. 2022a. *Eswatini: An overview of the Data Protection Act*. Article, OneTrust DataGuidance.
- Musoni, M. 2022b. *Africa: The state of cross-border transfer of personal data in the SADC region*. Article, OneTrust DataGuidance.
- Musoni, M. 2024. *The Role of Data Localisation in Cybercrime Investigations*. In R. Atuguba Akongburo, P. Boshe, S. Dei-Tutu and M. Hennemann (Ed.), *African Data Protection Laws: Regulation, Policy, and Practice* (pp. 177–202). Berlin, Boston: De Gruyter. <https://doi.org/10.1515/9783110797909-011>.

-
- Musoni, M., Domingo, E. and Ogah, E. 2023. *Digital ID systems in Africa: Challenges, risks and opportunities*. ECDPM Discussion Paper 360. Maastricht: ECDPM.
- Musoni, M., Karkare, P., Teevan, C. and Domingo, E. 2023. *Global approaches to digital sovereignty: Competing definitions and contrasting policy*. ECDPM Discussion Paper 344. Maastricht: ECDPM.
- Mwaya, J. 2022. *Dare to Share: Unleashing the Power of Data in Africa*. Commentary, Tony Blair Institute for Global Change.
- Naidoo, R. 2020. *Building a vibrant data economy in Africa*. Article, ITWeb.
- Ndemo, B., Ndung'u, N., Odhiambo, S., Shimeles, A. 2023. *Data Governance and Policy in Africa*. Information Technology and Global Governance.
- OCDE. 2019. *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*. Paris: OECD Publishing, <https://doi.org/10.1787/276aaca8-en>.
- Oloni, V. 2024. *Cross-Border Data Flows: Oiling the Wheel of the African Digital Economy*. In R. Atuguba Akongburo, P. Boshe, S. Dei-Tutu and M. Hennemann (Ed.), *African Data Protection Laws: Regulation, Policy, and Practice* (pp. 157-176). Berlin, Boston: De Gruyter. <https://doi.org/10.1515/9783110797909-010>.
- Olorunju, N. and Adams, R. 2022. *Research ICT Africa (RIA) Working Paper: African Data Trusts: New Tools Towards Collective Data Governance?* Research ICT Africa.
- Pritchett, L. 2019. *The Big Stuck in State Capability and Premature Load Bearing, Some New Evidence*. Article, Cambridge: Harvard Kennedy School.
- Sampath, P. and Tregenna, F. 2022. *Digital Sovereignty: African Perspectives*. Johannesburg: DSI/NRF South African Research Chair in Industrial Development. DOI: 10.5281/zenodo.5851685.
- Saturday, B. and Nyamwire, B., 2023. *Towards Effective Data Governance in Africa: Progress, Initiatives and Challenges*.
- Shahin, J., Hoogenboom, S., Morais, C., and Santaniello, M. 2024. *Chapter 4: Regional digital governance*. In *Handbook of Regional Cooperation and Integration*. Cheltenham, UK: Edward Elgar Publishing. Retrieved Jul 5, 2024, from <https://doi.org/10.4337/9781800373747.00012>.
- Soule, F. 2023. *Mandira Bagwandeem: The domination of foreign companies in Africa's digital landscape could impact a country's digital sovereignty*. Negotiating Africa's digital partnerships: interview series.
- Soule, F. 2024. *Digital Sovereignty in Africa: moving beyond local data ownership*. CIGI Policy Brief no. 185.
- Stuart, J. 2024a. *The Digital Trade Protocol of the ZLECAf and Digitally-Driven Development in Africa*. Blog, Tralac.
- Stuart, J. 2024b. *The ZLECAf Digital Trade Protocol – clarification of key issues*. Blog, Tralac.
- Teevan, C. 2023. *Building a digital single market: From the EU to Africa*. ECDPM Briefing note 155. Maastricht: ECDPM.
- The Economist. 2018. *How regulators can prevent excessive concentration online*. Special Report, The Economist.

-
- Tshuma, B. 2024. *Data Imaginaries and the Emergence of Data Institutions in sub-Saharan Africa*. In R. Atuguba Akongburo, P. Boshe, S. Dei-Tutu & M. Hennemann (Ed.), *African Data Protection Laws: Regulation, Policy, and Practice* (pp. 205-214). Berlin, Boston: De Gruyter. <https://doi.org/10.1515/9783110797909-012>.
- UE. 2022. *Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le Règlement (UE) 2018/1724 (Règlement sur la gouvernance des données)*. Journal officiel de l'Union européenne.
- UE. 2023. *Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données)* Journal officiel de l'Union européenne.
- Vanheukelom, J., Byiers, B., Bilal, S. and Woolfrey, S. 2016. *Political Economy of Regional Integration in Africa. What Drives and Constrains Regional Organisations?* ECDPM Synthesis Report, Maastricht: ECDPM.
- Waruru, M. 2023. *'Culture of secrecy' thwarting data sharing in Africa*. SciDev.Net, PsyhOrg.
- Whittle, D. 2024. *Digital: Some Initial Thoughts on ZLECAf's Leaked Digital Trade Protocol*. Blog, Trade Notes.

À propos de l'ECDPM

L'ECDPM est un centre indépendant de réflexion et d'action qui travaille sur la coopération internationale et la politique de développement.

Depuis 1986, les membres de notre personnel fournissent des recherches et des analyses, des conseils et un soutien pratique aux décideurs politiques et aux praticiens en Europe et en Afrique - afin de mettre les politiques au service d'un développement mondial durable et inclusif.

Nos principaux domaines d'activité sont les suivants

- la politique étrangère et de développement de l'Union européenne
- Migration et mobilité
- Économie numérique et gouvernance
- Relations l'Union africaine et l'Union européenne
- Paix, sécurité et résilience
- Gouvernance démocratique
- Reprise et transformation économiques
- Changement climatique et transition verte
- Intégration économique africaine
- Systèmes alimentaires durables

Pour plus d'informations, veuillez consulter le site www.ecdpm.org

Ce document a été réalisé avec l'aide financière de l'Union européenne. Le contenu de ce document relève de la seule responsabilité des auteurs et ne peut en aucun cas être considéré comme reflétant la position de l'ECDPM. Cette publication bénéficie également du soutien structurel des partenaires institutionnels de l'ECDPM : Autriche, Belgique, Danemark, Estonie, Finlande, Irlande, Luxembourg, Pays-Bas et Suède.

ISSN1571-7577