AFRICAN UNION
الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

Addis Ababa, Ethiopia P. O. Box 3243 Telephone: 5517 700 Fax: 5517844
Website: www.au.int

CONSEIL EXÉCUTIF
Quarantième session ordinaire
20 janvier - 03 février 2022
Addis-Abeba, Éthiopie

EX.CL/1308(XL)
Original: anglais

RAPPORT DE LA QUATRIEME SESSION ORDINAIRE DU COMITE TECHNIQUE SPECIALISE (CTS) DE L'UNION AFRICAINE SUR LA COMMUNICATION ET LES TIC (CTS - CCICT), 25-27 OCTOBRE 2021

AFRICAN UNION

الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

QUATRIÈME SESSION ORDINAIRE DU COMITÉ TECHNIQUE SPÉCIALISÉ DE L'UNION AFRICAINE SUR LA COMMUNICATION ET LES TIC (CCITC-4) PAR VIDÉOCONFÉRENCE 25-27 OCTOBRE 2021

RAPPORT DE LA REUNION MINISTÉRIELLE

27 octobre 2021

INTRODUCTION

La Quatrième session ordinaire du Comité technique spécialisé (CTS) de l'Union africaine sur la communication et les TIC (CCICT) s'est tenue par visioconférence le 27 octobre 2021. La Session a été précédée de la réunion des experts, qui a eu lieu les 25 et 26 octobre 2021.

PARTICIPATION

1. Ont participé à la Session les 37 États membres suivants : Algérie, Angola, Botswana, Burkina Faso, Burundi, Cameroun, Tchad, République centrafricaine, Comores, Congo (République démocratique), Congo (République), Côte d'Ivoire, Djibouti, Égypte, Guinée équatoriale, Érythrée, Éthiopie, Gabon, Gambie, Ghana, Kenya, Lesotho, Libye, Maroc, Mozambique, Namibie, Niger, Rwanda, République arabe sahraouie démocratique, Sénégal, Afrique du Sud, Tanzanie, Togo, Tunisie, Ouganda , la Zambie et le Zimbabwe. La liste des participants figure en Annexe I.

2. Ont également participé à la Session l''ADUA/NEPAD et la Communauté économique régionale (CER) ci-après : la Communauté économique des États de l'Afrique centrale (CEEAC).

3. Ont également participé à la Session les organisations et agences africaines et internationales suivantes : l'Union africaine des télécommunications (UAT), l'Union panafricaine des postes (UPAP) et Smart Africa.

4. Les organisations suivantes étaient également présentes : Union internationale des télécommunications (UIT), Union européenne (UE), Banque mondiale (BM), GIZ, Internet Society (ISOC), Huawei et ICT Research Africa.

I. CEREMONIE D'OUVERTURE

5. Le Point concernant l'ouverture a été sauté et le temps prévu a été consacré à la recherche du Quorum pour que la réunion puisse démarrer.

II. ÉLECTION DU BUREAU DE LA QUATRIÈME SESSION ORDINAIRE DU COMITÉ TECHNIQUE SPÉCIALISÉ DE L'UNION AFRICAINE SUR LA COMMUNICATION ET LES TIC (CCITC-4),

6. En application du principe de rotation et de représentation géographique, le Bureau de la Quatrième Session du CTS a été élu, comme suit :

AFRIQUE CENTRALE	
Congo (Rep)	Président du Bureau
AFRIQUE AUSTRALE	
Afrique du Sud	1er Vice-président du Bureau
AFRIQUE DE L'OUEST	
Niger	2e Vice-président du Bureau
AFRIQUE DE L'EST	
Rwanda	3e Vice-président du Bureau
AFRIQUE DU NORD	
Egypte	Rapporteur par intérim du Bureau

7. La Région de l'Afrique du Nord mènera des consultations en son sein et communiquera en temps voulu le nom de l'État membre qu'elle aura désigné comme Rapporteur.

III. ADOPTION DE L'ORDRE DU JOUR ET DU PROGRAMME DE TRAVAIL

8. Les participants ont adopté l'ordre du jour suivant, avec amendements.

1) Cérémonie d'ouverture
2) Élection du Bureau ;
3) Adoption de l'ordre du jour et du programme de travail ;
4) Examen du Rapport des experts ;
5) Examen et adoption de la Déclaration 2021
6) Examen des Projets de cadres continentaux sur l'interopérabilité des identifications numériques et de la politique continentale des données ;
7) Examen et adoption du Rapport de la Session ministérielle ;
8) Questions diverses.
9) Cérémonie de clôture.

9. Le Programme de travail adopté est joint en annexe II

IV. EXAMEN DU RAPPORT DES EXPERTS.

10. Le Rapport des Experts a été présenté par le Rapporteur par intérim, l'Égypte. Le rapport a porté sur les résultats obtenus, les difficultés rencontrées et les commentaires faits par les experts, comme suit :

Commission de l'UA

- La Stratégie de transformation numérique (STN) pour l'Afrique, avec l'élaboration de la stratégie de l'UA pour la santé numérique et de son plan de mise en œuvre, de la stratégie de l'UA pour l'éducation numérique, et de son plan de mise en œuvre, de la stratégie de l'UA pour l'agriculture numérique, et de son plan de mise en œuvre , de la stratégie de commerce électronique de l'UA, des lignes directrices pour une approche commune de la transformation numérique de la poste en Afrique et l'élaboration du Cadre de suivi & d'évaluation de la Stratégie de transformation numérique pour l'Afrique (STN)';

- Le projet de cadre d'interopérabilité de l'UA pour l'identification numérique et le projet de cadre pour une politique continentale des données de l'UA ;

- La deuxième phase (2021-2030) du PIDA qui comprend des projets sur les TIC ainsi que sur l'eau, l'énergie et les transports. Sur un total de 69 projets, 12 projets sur les TIC ont été sélectionnés et validés par le sommet de l'UA en février 2021 pour renforcer la connectivité intra-africaine, basée sur l'approche intégrée des corridors en vue de tirer parti

des technologies numériques pour le développement d'infrastructures modernes.

- l'Initiative de politique et de réglementation pour l'Afrique numérique (PRIDA), avec notamment la sélection des conditions d'entrée sur le marché (régime d'autorisation/de licence) et la protection des données personnelles et la localisation des données comme sujets d'harmonisation des indicateurs et de la méthodologie de suivi et d'évaluation (S&E) sur les deux sujets et le développement de deux prototypes de S&E pour mesurer l'étendue de l'harmonisation de chaque sujet à travers le continent.

- La cybersécurité qui souligne les progrès réalisés dans la révision de la Convention de Malabo et l'élaboration de la politique continentale de sécurité en ligne des enfants et de la stratégie continentale de cybersécurité ;

- Les recommandations de l'UA sur les solutions numériques pour rechercher, identifier et partager des informations sur les pandémies en Afrique.

- Le renforcement de l'image de l'UA et la promotion du mandat et de l'agenda de l'UA ; l'adoption et l'utilisation de la nouvelle image de l'UA au sein de la Commission de l'UA et des organes de l'UA, la promotion de l'Agenda 2063 dans les médias traditionnels et les plateformes numériques pour renforcer la sensibilisation sur l'Agenda 2063 et mieux faire connaître l'Agenda et assurer une meilleure compréhension des mandats et programmes de l'UA ;

- Le renforcement de la visibilité, du plaidoyer et des relations publiques de l'Institution, avec le développement et le lancement de 2 applications mobiles pour toucher les utilisateurs de téléphones portables et de tablettes, les initiatives de plaidoyer pour la ratification des traités de l'UA, la tenue d'une conférence annuelle sur les femmes africaines dans les médias et la redéfinition des activités prioritaires en vue de positionner l'Union africaine et le CDC Afrique à l'avant-garde de la gestion et de la lutte contre la pandémie de Covid-19 en Afrique.

ADUA- NEPAD

- L'ADUA-NEPAD a entrepris, conformément à la Convention de Malabo sur la cybersécurité et la protection des données personnelles, des évaluations de cybersécurité dans dix États membres de l'Union africaine, à savoir le Bénin, le Tchad, la République du Congo, la République démocratique du Congo, la Guinée, le Kenya, la Mauritanie, le Maroc, le Sénégal et la Tunisie. L'ADUA-NEPAD a également publié des rapports de pays ainsi qu'un rapport consolidé – Rapport d'évaluation de la cybersécurité de l'ADUA-NEPAD (https://www.au-pida.org/download/cybersecurity-assessment-report/).

- L'ADUA-NEPAD collabore également avec le Forum mondial sur l'expertise en matière de cybersécurité (GFCE) sur un projet visant à renforcer l'acquisition de connaissances sur les capacités en matière de cybersécurité afin de permettre aux États membres de l'UA de mieux comprendre les capacités en matière de cybersécurité, d'identifier leurs besoins nationaux dans ce domaine et d'y répondre, et de renforcer leur cyber-résilience.

- Le deuxième plan d'action prioritaire du Programme PIDA (PIDA PAP II) a été adopté par la Conférence de l'UA en février 2021. Sur les 69 projets retenus, 11 concernent le secteur des TIC.

UPAP

- Dans le cadre de la mise en œuvre du projet sur la connectivité et l'électrification et la connectivité des bureaux de poste dans les zones rurales du Kenya, du Malawi, de la Tanzanie et de l'Ouganda des progrès notables ont été enregistrés dans la mobilisation des fonds ainsi que dans la mise en œuvre du projet.

- L'UPAP et les États membres ont mis en œuvre des stratégies de lutte contre la COVID-19, y compris l'amélioration des transferts de fonds et des services en ligne. Des mesures supplémentaires ont été mises en place, comme suit :

- L'UPAP a conseillé aux pays membres d'émettre des EmiS (messages du système d'information d'urgence) sur les effets de la COVID-19, les bonnes pratiques à adopter pendant la période de pandémie ainsi que sur les moyens à mettre en place pour que la poste continue d'être utile ;

- L'UPAP a diffusé en avril 2020 un questionnaire destiné à évaluer la situation dans les États membres et la façon dont ils faisaient face aux situations critiques ;

- L'UPAP a tenu un webinaire avec l'AFRAA le 12 mai 2020 et est parvenue à la conclusion que la poste offre des services essentiels et que les gouvernements devaient en conséquence être sensibilisés afin qu'ils facilitent l'acheminement du courrier par avion cargo.

UAT

- Préparation de la Conférence mondiale des radiocommunications de l'UIT (CMR-23), de l'Assemblée mondiale de normalisation des télécommunications 2020 (AMNT-20), de la Conférence mondiale sur le développement des télécommunications 2021 (CMDT-21), des réunions préparatoires africaines de l'UIT PP-22

ÉTUDES RÉALISÉES ET RAPPORTS ÉLABORÉS PAR L'UAT

(a) **Stratégie 4IR** : l'UAT, avec le soutien du Gouvernement d'Afrique du Sud, a recruté un cabinet de consultants et a élaboré le projet de 4ème stratégie industrielle (4IR) qui a été présenté aux membres de l'UAT pour la première fois en octobre 2020 à un atelier de validation, et qui a été ensuite révisé en tenant compte des contributions et des commentaires des membres, et a été soumis à la session du Conseil de l'UAT de 2021.

(b) **Gestion des déchets électroniques** : L'UAT a également élaboré des lignes directrices pour la gestion des déchets électroniques en Afrique ; elle travaille en liaison avec les membres pour la mise en œuvre de ces lignes directrices. L'UAT souhaite collaborer davantage avec la CUA pour soutenir ce processus puisque tous les deux travaillent au service du continent.

(c) **Concours de l'innovation numérique** : L'UAT a également organisé deux éditions du « Concours de l'innovation numérique 2020 & 2021 » en collaboration avec l'UIT et d'autres partenaires afin de promouvoir l'esprit d'innovation en Afrique et de donner une opportunité exceptionnelle aux jeunes Africains d'exprimer leurs idées innovantes et leurs talents et de reconnaître le rôle important que cet écosystème joue dans la réalisation du développement numérique en Afrique. L'édition 2021 du Concours a permis d'identifier des institutions africaines qui créent un environnement favorable aux innovations des jeunes dans le domaine des TIC. Parmi les institutions qui participent au concours, figurent des organismes d'élaboration de politiques, des incubateurs, des universités et des organismes à but non lucratif. Ce choix est la reconnaissance du rôle crucial que ces organisations jouent et de l'importance que revêt l'investissement dans un secteur porteur pour les innovateurs. Le Concours s'est terminé avec une cérémonie de remise de prix en octobre 2021. Au cours de la cérémonie, les 10 lauréats ont reçu des prix en numéraire et ont reçu le "Prix UAT 2021 pour la Meilleure pratique de l'écosystème de l'UAT en Afrique pour les innovations des jeunes dans le domaine des TIC".

(d) **Stratégie de migration vers IPv6** : l'UAT a élaboré un cadre stratégique de migration vers IPv6 pour l'Afrique. L'UAT, en partenariat avec Afrinic, se propose également d'élaborer un programme de renforcement des capacités à cet égard et compte travailler avec ses membres et les parties prenantes à la mise en œuvre de la stratégie, en collaboration avec la CUA et les organisations sœurs à l'appui du processus puisque toutes comme l'UAT travaillent au service du continent.

(e) **Cadre modèle d'acquisition de compétences en ligne** : L'UAT a également élaboré un cadre modèle d'acquisition de compétences en ligne pour l'Afrique afin de répondre aux besoins futurs du marché numérique de l'Afrique et compte travailler en liaison avec ses membres, les partenaires et les parties prenantes à la mise en œuvre de ce modèle, en collaboration avec la CUA et des organisations sœurs, en appui à ce processus puisque nous tous travaillons au service du continent. La Journée des TIC de l'UAT " TIC-UAT" sera célébrée le 7 décembre 2021, sous le thème "Développement des compétences numériques pour la transformation numérique de l'Afrique".

PROGRAMMES EN COURS OU RÉCEMMENT ACHEVES

- **Radiocommunication**

a) Formulation de recommandations sur la mise en œuvre des technologies émergentes pour guider les pays africains dans la mise en œuvre de ces technologies émergentes, y compris la technologie 5G ;

b) Élaboration de recommandations pour guider les pays africains dans les pratiques modernes de gestion du spectre ;

c) Optimisation du Plan de fréquences de radiodiffusion FM (le Plan GE84) pour l'Afrique destiné à identifier de nouveaux canaux pouvant être utilisés pour soutenir la croissance de la radio FM en Afrique ;

d) Élaboration d'une stratégie pour l'introduction de la radiodiffusion sonore numérique en Afrique ;

e) La premier Plan d'attribution du Spectre en Afrique (AfriSAP) destiné à servir de référence pour les plans de spectre sous-régionaux et/ou nationaux a été élaboré ;

f) L'harmonisation des fréquences pour les télécommunications d'urgence (PPDR) a été assurée parallèlement à l'AfriSAP ;

g) L'élaboration d'une stratégie de gestion des ressources orbitales et des fréquences satellitaires visant à optimiser l'acquisition, la conservation et l'utilisation de ces ressources en Afrique a été achevée ;

h) La formulation de recommandations tendant à guider les pays africains dans la mise en œuvre des politiques, des réglementations et des pratiques en matière de spectre permettra d'assurer la connectivité dans les zones rurales.

- **Secteurs de la normalisation et du développement**

a) Élaboration d'un cadre modèle/de lignes directrices sur les centres de données et les services et infrastructures cloud pour l'Afrique ;

b) Élaboration d'un livre blanc sur les bonnes pratiques en matière de connectivité et d'accessibilité en Afrique et d'un cadre régional pour faciliter l'accès aux câbles sous-marins de tous les pays, en particulier les pays enclavés.

c) Élaboration d'une politique et de normes communes de sécurité numérique pour la sécurité des réseaux et des systèmes d'information ;

d) Renforcement des capacités en partenariat avec Huawei en ce qui concerne les technologies émergentes et les outils numériques (cloud computing, etc.) ;

e) Livre blanc sur l'accès et la connectivité et le cadre de coopération pour faciliter l'accès aux câbles sous-marins « FO » pour les pays enclavés ;

f) Étude pour la mise en place d'un Observatoire des TIC pour l'Afrique.

11. Les défis identifiés sont les suivants :

(i) les ressources limitées pour mettre en œuvre la Stratégie de transformation numérique pour l'Afrique et l'absence de cadre et de mécanisme pour le suivi et l'évaluation de la mise en œuvre de la stratégie ;

(ii) les restrictions de voyage du fait de la pandémie de COVID-19 et la fermeture de bureaux des gouvernements en raison de la COVID-19 (un défi pour lequel l'information en ligne est limitée) ;

(iii) Le faible nombre d'États membres et de régions ayant une politique d'économie numérique qui crée un environnement propice au commerce électronique et à l'économie numérique ;

(iv) la participation limitée au partage ou à la collecte des données ; la faible mobilisation des ressources pour la préparation des projets PIDA, en particulier les ressources nationales ;

(v) les retards dans les accords PIDA entre les pays et le non-alignement des cadres juridiques et réglementaires pour les pays concernés et les retards dans la nomination des points focaux sectoriels PIDA de certains États membres/ministères ;

(vi) l'insuffisance du budget et le manque de personnel dans la Direction de la communication ;

(vii) L'insuffisance du financement pour des projets comme les codes d'adressage et les codes postaux, l'électrification et la connectivité. ;

(viii) l'adoption de solutions numériques pour les services financiers postaux, en particulier après la pandémie de Covid-19 ; et

(ix) les coûts de transport élevés en raison de l'application des taux de fret pour le transport du courrier au lieu des taux courrier plus faibles de l'UPU/IATA ;

(x) la mise en œuvre de stratégies de lutte contre la COVID-19, y compris l'intensification des transferts de fonds et des services électroniques offerts.

12. Le rapport est joint en annexe III**.**

13. Les ministres ont pris note du rapport et ont fait des commentaires, comme suit:

(i) Féliciter les experts pour le travail qu'ils ont fait en cette période difficile ;

(ii) Demander qu'il soit mentionné que l'Égypte exerce les fonctions de rapporteur en tant que représentant de la région de l'Afrique du Nord qui poursuit ses consultations en vue de désigner un pays pour occuper ce poste.

V. Examen du cadre d'interopérabilité des identifications numériques de l'UA et du cadre pour une politique continentale des données de l'UA

14. Après la présentation des deux cadres, les ministres ont formulé les recommandations suivantes :

Cadre de l'UA pour l'interopérabilité des identifiants numériques

(i) Les États membres doivent apporter leur contribution dans un délai d'un mois au projet de Cadre de l'UA pour l''interopérabilité des identifiants numériques afin de faciliter son adoption par les organes délibérants de l'UA.

(ii) Féliciter la Commission de l'UA pour l'excellent travail qu'elle a effectué.

Cadre pour une politique continentale des données de l'UA

(i) Les États membres doivent apporter leur contribution dans un délai d'un mois au projet de cadre stratégique continental des données afin de faciliter son adoption par les organes délibérants de l'UA.

(ii) Féliciter la Commission de l'UA pour l'excellent travail qu'elle a effectué.

VI. Examen et adoption de la Déclaration 2021 (Annexe IV)

15. La déclaration a été adoptée avec des amendements.

VII. Examen de la date et du lieu de la prochaine session du CTS

16. La République du Congo a proposé d'accueillir la 5ème session ordinaire du CTS en 2023.

17. La date du CTS sera fixée en temps voulu, en collaboration avec le Bureau du CTS et la Commission de l'UA.

VIII. Examen et adoption du rapport de la session ministérielle

18. La Commission de l'UA a été chargée de communiquer le rapport aux États membres.

IX. Questions diverses

19. Aucune question n'a été soulevée sous ce point.

X. Clôture de la réunion

20. Dans son mot de clôture, S.E. Dr Amani ABOU-ZEID, Commissaire de l'UA aux infrastructures et à l'énergie a remercié le Président du Bureau sortant du CTS sur la communication et les TIC pour son leadership dans la conduite des travaux du CTS pendant la période 2019-2021, et l'a félicité pour les résultats obtenus dans les deux secteurs malgré le défi que pose la pandémie actuelle de COVID-19.

21. La Commissaire a ensuite vivement souhaité la bienvenue au nouveau président du CTS sur la communication et les TIC et au Bureau élu et leur a donné l'assurance qu'elle et son équipe travailleront sans relâche avec le Bureau pour améliorer la transformation numérique de l'Afrique.

22. Enfin, la Commissaire a assuré aux ministres que la Commission de l'Union africaine continuera à établir des partenariats et des collaborations plus solides et à travailler avec toutes les parties prenantes pour mettre à profit les technologies, et faire en sorte qu'elles soient inclusives et sûres et soient utilisées pour renforcer la dynamique du redressement post-Covid-19.

23. S.E. Le Ministre Léon Juste IBOUMBO, Ministre des Postes, des Télécommunications et de l'Economie numérique de la République du Congo, Président élu du Bureau a félicité les Ministres et autres participants pour leur engagement et leur participation active malgré le contexte difficile.

24. Le Président a exprimé la gratitude de la République du Congo à ses pairs, en particulier les ministres de la région de la CEEAC, pour son élection à la présidence du Bureau, confirmant ainsi la pertinence de la vision de la République du Congo en numérisation

25. S.E M. IBOMBO s’est félicité du travail accompli par le Bureau présidé par l’Égypte et a exprimé le souhait de pouvoir bénéficier de la précieuse expérience des membres du Bureau sortant

26. Avant de conclure son discours, le Ministre a informé les participants de l'opérationnalisation par son pays du Centre africain de recherche sur l'Intelligence artificielle et a souligné la disponibilité du Congo à recevoir tous les Africains

QUATRIÈME SESSION ORDINAIRE DU COMITÉ TECHNIQUE SPÉCIALISÉ SUR LA COMMUNICATION ET LES TIC (CTS-CTIC)

27 OCTOBRE 2021 PAR VISIOCONFÉRENCE

AU/STC-CICT-4/MIN/Decl.
ORIGINAL: ANGLAIS

DÉCLARATION DU CTS-CTIC 2021

PRÉAMBULE

NOUS, Ministres de la Communication et des TIC de l'Union africaine, réunis par visioconférence, le 27 octobre 2021, dans le cadre de la quatrième (4e) session ordinaire du **Comité technique spécialisé sur les communications et les technologies de l'information et de la communication (TIC)** ;

GUIDÉS PAR l'Acte constitutif de l'Union africaine (UA) ;

RAPPELANT les Décisions Assembly/AU/Dec.227 (XII) et Assembly/AU/Dec.365(XIVI), adoptées respectivement en janvier 2009 et juillet 2011, sur la configuration des Comités techniques spécialisés (CTS) et les modalités de leur mise en œuvre ;

AYANT A L'ESPRIT la Déclaration Assembly/AU/Decl.1(XIV), adoptée lors de la 14e session ordinaire de la Conférence de l'UA sur les technologies de l'information et de la communication en Afrique, défis et perspectives de développement, tenue en février 2010 à Addis-Abeba (Éthiopie);

CONSIDÉRANT la Déclaration Assembly/AU/Decl.2(XVIII), adoptée lors de la 18e session ordinaire de la Conférence de l'UA, tenue en janvier 2012 à Addis-Abeba (Éthiopie) sur le Programme de développement des infrastructures en Afrique (PIDA) et la Décision Assembly/AU/Dec.529(XXIII) de la 23e session ordinaire de la Conférence de l'UA tenue en juin 2014 à Malabo (Guinée équatoriale), qui a adopté la Convention de l'Union africaine sur la sécurité du cyberespace et la protection des données personnelles ;

CONSIDÉRANT ÉGALEMENT la Déclaration Assembly/AU/Decl.3(XXX) sur la gouvernance de l'Internet et le développement de l'économie numérique en Afrique, adoptée lors de la 30e session ordinaire de la Conférence de l'UA, qui s'est tenue les 28 et 29 janvier 2018 à Addis-Abeba (Éthiopie) ;

RAPPELANT la Décision 1074 (XXXVI) du Conseil exécutif sur les rapports des Comités techniques spécialisés, notamment de la 3e session ordinaire du CTS sur les communications et les TIC, tenue les 25 et 26 octobre 2019 à Charm el-Cheikh (République arabe d'Égypte), qui a approuvé la Stratégie de transformation numérique pour l'Afrique (*Digital Transformation Strategy for Africa - DTS*) en vue d'exploiter les technologies et l'innovation numériques pour la transformation des sociétés et des économies africaines, et a demandé à la Commission d'entreprendre, entre autres, ce qui suit :

(i) Mobiliser les ressources nécessaires à la mise en œuvre de la Stratégie globale de transformation numérique pour l'Afrique et élaborer la matrice de mise en œuvre de cette Stratégie ;

(ii) promouvoir la stratégie dans toutes les activités pertinentes de l'UA, notamment celle des CTS ;

(iii) Élaborer des stratégies/plans de mise en œuvre sectoriels de la DTS, en particulier ceux qui revêtent une importance critique et qui ont déjà été identifiés en vue de la mise en place d'une DTS globale pour le continent;

(iv) Élaborer des lignes directrices sur la confidentialité, les services par contournement (*Over The Top services* ou OTT), un cadre continental sur la politique des données et une feuille de route et des orientations pour l'harmonisation et le déploiement du spectre pour les réseaux à large bande mobiles et sans fil actuels et futurs tels que les télécommunications mobiles internationales (TMI) 2020/5G ;

(v) Consacrer des ressources appropriées à la mise en œuvre d'un programme complet de cybersécurité qui comprend une assistance aux États membres de l'UA en vue de l'adoption de cyberstratégies, de cyberlégislations et de la création d'équipes d'intervention informatique d'urgence (CERT) ou d'équipes d'intervention en cas d'incident informatique (CIRT);

(vi) Soumettre un rapport sur l'audit des actifs communs du réseau électronique panafricain, accompagner des implications financières avant d'appliquer la recommandation des ministres concernés de transférer ses actifs à l'Organisation régionale africaine de communications par satellite (RASCOM) ; et,

(vii) S'assurer qu'un Guide de marque ou de style de communication et des politiques et procédures de communication sont institués au sein de l'organisation.

TENANT COMPTE de l'avènement de la pandémie de COVID-19 et de la réponse du secteur de la communication et des TIC à cette pandémie, telle qu'énoncée dans la déclaration du Bureau du CTS-CTIC réuni le 5 mai 2020 ;

RECONNAISSANT les efforts déployés par la CUA, les agences spécialisées et les organisations régionales de l'UA ainsi que par les organisations internationales dans la promotion et la mise en œuvre de la Stratégie de transformation numérique pour l'Afrique (DTS), dans l'élaboration de stratégies numériques sectorielles pour l'éducation, la santé, l'agriculture, le commerce électronique et le secteur postal, dans la rédaction du cadre de politique continentale sur les données et du cadre d'interopérabilité pour l'identification numérique, de la stratégie continentale de cybersécurité, du document de politique sur la protection en ligne des enfants, ainsi que de la méthodologie et du modèle d'harmonisation visant à collecter les données des projets en cours ou terminés liés à la transformation numérique dans les États membres et les CER afin d'améliorer la coordination et faciliter les synergies ;

AYANT À L'ESPRIT la demande sans précédent de technologies numériques pour faciliter l'endiguement de la pandémie de COVID-19 et **SALUANT** les diverses initiatives

visant à freiner la propagation de la COVID-19 et à atténuer ses effets sociétaux et économiques ;

RAPPELANT la vision de la Stratégie de transformation numérique pour l'Afrique pour une société et une économie numériques intégrées et inclusives en Afrique, qui améliorent la qualité de vie des citoyens africains, renforcent le secteur économique existant, permettent sa diversification et son développement, et assurent l'appropriation continentale, l'Afrique jouant le rôle de producteur et non plus seulement consommateur dans l'économie mondiale ;

RAPPELANT ÉGALEMENT l'engagement de poursuivre la mise en œuvre de la stratégie de communication et de plaidoyer de l'UA, d'améliorer la visibilité de l'UA et construire son image dans le cadre de l'Agenda 2063 ;

RAPPELANT EN OUTRE la Déclaration solennelle sur le 50e anniversaire de l'OUA/UA de mai 2013 dans laquelle les chefs d'État et de gouvernement ont déclaré leur engagement à hisser le drapeau de l'UA et à chanter l'hymne de l'UA et à faire de même avec les drapeaux et les hymnes nationaux, et à promouvoir et harmoniser l'enseignement de l'histoire et des valeurs africaines, ainsi que du panafricanisme dans toutes les écoles et établissements éducatifs dans le contexte de la promotion de l'identité et de la renaissance de l'Afrique ;

TENANT COMPTE de l'importance de la communication, de l'image de marque, du plaidoyer et des relations publiques pour la réputation, la reconnaissance et l'appréciation de l'Union africaine auprès de toutes ses partenaires ;

CONSCIENTS DE LA NÉCESSITÉ de célébrer le 20e anniversaire de l'Union africaine en 2022 au niveau continental et de la nécessité de rehausser la marque de l'UA auprès de toutes les populations africaines dans le contexte de la propagation de la COVID-19 ;

CONSIDÉRANT le rapport de la session d'experts, qui s'est tenue virtuellement les 25 et 26 octobre 2021 ;

AYANT ÉLU le Bureau suivant du CTS-CTIC pour une durée de deux (2) ans :

AFRIQUE CENTRALE	
République du Congo	Président du Bureau
AFRIQUE AUSTRALE	
Afrique du Sud	1e Vice-président du Bureau
AFRIQUE DE L'OUEST	
Niger	2e Vice-président du Bureau
AFRIQUE ORIENTALE	
Rwanda	3e Vice-président du Bureau
AFRIQUE DU NORD	
A Déterminer	Rapporteur du Bureau

PRENONS NOTE du rapport du Bureau et **FÉLICITONS** le Bureau pour ses réalisations;

FÉLICITENT ÉGALEMENT la Commission de l'UA pour avoir élaboré des politiques novatrices et des cadres continentaux tournés vers l'avenir pour l'interopérabilité des cartes d'identité numériques et la politique en matière de données, qui sont conformes aux meilleures pratiques mondiales.

PRENONS ÉGALEMENT NOTE du progrès accompli pour avoir accéléré la mise en œuvre de la stratégie de transformation numérique dans des secteurs essentiels, notamment par l'élaboration de la stratégie numérique de l'UA pour la santé et son plan de mise en œuvre, de la stratégie numérique de l'UA pour l'éducation et son plan de mise en œuvre, de la stratégie numérique de l'UA pour l'agriculture et son plan de mise en œuvre, de la stratégie de l'UA pour le commerce électronique, du cadre de politique de données pour l'Afrique, du cadre d'interopérabilité de l'UA pour l'identification numérique, initiative visant à réviser la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel ("Convention de Malabo") afin de la rendre conforme aux derniers standards et normes mondiaux en matière de cyberespace ; l'initiative visant à élaborer la stratégie continentale de cybersécurité et la politique de l'Union africaine en matière de sécurité et d'autonomisation des enfants en ligne, la méthodologie et l'outil de suivi et d'évaluation destinés à mesurer le degré d'harmonisation des politiques et réglementations en matière de TIC et de numérique, ainsi que la création de l'identité de marque de l'UA et la création d'un environnement propice à la mise en place du marché unique numérique de l'Afrique, conformément à la ZLECAf, ainsi que le travail effectué pour créer l'identité de marque de l'UA ;

NOUS ENGAGEONS PAR LA PRÉSENTE À :

1. **CONTRIBUER** à la réponse continentale coordonnée à la pandémie de COVID-19 en vue de l'atténuation de ses effets négatifs ;

2. **POURSUIVRE** l'élaboration de politiques et de réglementations pour faciliter le déploiement et l'utilisation d'outils numériques sûrs et sécurisés afin de renforcer la lutte contre la COVID-19 ;

3. **FOURNIR** un retour d'information dans un délai d'un mois pour enrichir le projet de cadre d'interopérabilité de l'UA pour l'identification numérique et le projet de cadre de politique des données continentales de l'UA afin de permettre l'adoption des deux cadres par les organes délibérants de l'UA ;

4. **MOBILISER** les ressources nécessaires pour mettre en œuvre le cadre de politique des données continentales de l'UA ;

5. **PRENDRE NOTE** des résultats du rapport d'audit de l'actif commun du Pan African e-Network (PAeN) pour la télémédecine et la télé-éducation, ainsi que de l'initiative visant à remanier le réseau pour fournir des services de télé-éducation et de cybersanté actualisés.

6. **RÉAFFIRMER** la reconnaissance des postes en tant qu'infrastructure nationale importante pour l'inclusion numérique, sociale, financière et commerciale, ainsi qu'en tant que réseau physique qui complète les besoins numériques des personnes - reliant les mondes physique et numérique ;

7. **POURSUIVRE** les réformes politiques et réglementaires du secteur postal aux niveaux national, régional et continental et faciliter l'augmentation des investissements dans l'infrastructure numérique et renforcer le rythme de sa transformation numérique.

PAR LA PRESENTE, DEMANDONS AUX ETATS MEMBRES DE :

8. **METTRE** en place et soutenir l'adoption de politiques et de réglementations adéquates qui facilitent le déploiement et l'utilisation d'outils et de solutions numériques pour permettre l'intersectorialité et l'interopérabilité des données afin d'améliorer les réponses COVID-19 ;

9. **PROMOUVOIR** la détaxation de l'accès aux contenus sanitaires et éducatifs en tant qu'intervention critique et urgente, pour contrer la pandémie et soutenir les apprenants et les étudiants confinés chez eux en raison de la fermeture des écoles, collèges et universités ;

10. **UTILISER** des plates-formes, des portails et des applications numériques, en particulier ceux développés par des Africains pour des Africains, qui peuvent aider à retracer, suivre et tester les personnes qui sont entrées en contact avec une personne infectée, tout en conciliant les impératifs de santé, les préoccupations en matière de vie privée et la protection des données ;

11. **CONSTRUIRE** des partenariats avec des entreprises technologiques privées, des entrepreneurs sociaux, des organisations nationales et internationales afin d'utiliser les technologies existantes pour gérer la crise du COVID-19 ;

12. **ENCOURAGER** la conception de nouvelles applications et de nouveaux services pour aider à la lutte contre le COVID-19, pour faciliter des services tels que la livraison de nourriture et d'autres articles essentiels aux personnes les plus démunies en optimisant l'ensemble de la chaîne d'approvisionnement via des services gouvernementaux numériques ;

13. **ENCOURAGER** le partage des meilleures pratiques en matière de numérisation de leur secteur postal pour permettre à la CUA de finaliser et de diffuser les lignes directrices sur l'approche commune de la transformation postale numérique d'ici le 31 décembre 2021 ;

14. **RENFORCER** les programmes de renforcement des capacités en matière de TIC et de cybersécurité sur le continent et **CONNECTER** les personnes non connectées pour combler le fossé numérique et faire en sorte que tous les citoyens bénéficient de l'utilisation de solutions technologiques numériques innovantes pour avoir accès aux services de base en ligne ;

15. **CONNECTER** et impliquer les bureaux de poste dans la mise en œuvre des stratégies de lutte contre le COVID-19, y compris l'élargissement de l'offre de transferts de fonds et de services électroniques ;

16. **PROMOUVOIR** la mise en œuvre du guide de style de la marque et de la communication de l'UA et des politiques et procédures de communication, et veiller à l'adoption et à l'utilisation de la marque de l'UA dans tous les États membres ;

17. **COOPÉRER** avec la CUA en mettant à disposition leurs radiodiffuseurs publics nationaux pour diffuser des informations provenant de la Commission au cours des mois de septembre 2022 et mai 2023, lorsque le continent célébrera respectivement le 20e anniversaire de la CUA et le 60e anniversaire de l'OUA. Cela sera fait dans le but de s'assurer que tous les citoyens africains en savent plus sur les célébrations et le rôle de l'UA, dans le contexte de la construction de l'identité de l'UA ;

18. **PROMOUVOIR** l'engagement avec les ministères de l'éducation au sein des États membres pour encourager l'adoption de l'enseignement et la diffusion des symboles continentaux tels que l'hymne de l'UA et promouvoir l'inclusion de l'Agenda 2063 dans les programmes nationaux ;

19. **ENCOURAGER LA NUMÉRIFICATION DES CERTIFICATS DE SANTÉ HARMONISÉS INTEROPÉRABLES,** conformes aux exigences de PANABIOS[1] en matière de voyages de confiance, afin d'assurer la mobilité continue des citoyens africains sur le continent pour accroître le commerce intra-africain et faciliter la mise en œuvre de la ZLECAf ;

20. **SOUTENIR et FACILITER** la mise en œuvre continentale des modèles de suivi et d'évaluation sur l'harmonisation des conditions d'entrée sur le marché et des cadres juridiques et réglementaires de la protection des données ;

21. **ENCOURAGER L'UTILISATION** de la méthodologie et de l'outil

[1] PanaBIOS est conçu par des technologues et des spécialistes de l'intelligence artificielle africains pour fournir une technologie, des données et des informations sur la biosurveillance et le dépistage biologique afin de permettre la création de corridors de santé publique dans le cadre de l'initiative Open Corridors de l'UA.

d'harmonisation pour mesurer le degré d'harmonisation des cadres politiques, juridiques et réglementaires des TIC et du numérique aux niveaux régional et continental ;

22. **RENFORCER** la coopération réglementaire au niveau continental afin de répondre collectivement aux nouveaux défis découlant de la numérisation et de la convergence croissante des services ;

23. **ACCÉLÉRER** la mise en œuvre du projet PIDA-PAP2 sur les TIC et plaider pour l'intégration des technologies numériques dans le développement d'infrastructures intelligentes ;

24. **RÉALISER** deux projets pilotes le long des principaux couloirs du PIDA et dans les zones reculées, conformément à la stratégie de l'UA visant à débloquer l'accès aux infrastructures et aux services de base pour les zones rurales et reculées ;

25. **METTRE EN PLACE** des groupes de travail multi-institutionnels sur l'identification numérique et la politique des données au niveau national.

26. **S'APPROPRIER** le cadre d'interopérabilité de l'UA pour l'identification numérique et le cadre continental de l'UA pour la politique en matière de données, dès leur adoption, et susciter l'adhésion de plusieurs parties prenantes pour permettre une circulation et une utilisation efficaces et responsables des données au niveau national.

27. **DEMANDER EN OUTRE AUX ÉTATS MEMBRES ET AUX CER** d'accélérer l'élaboration de politiques, d'agendas et de cadres nationaux sur l'économie et le commerce numériques, et d'intensifier la coopération et l'engagement des parties prenantes privées et les dialogues pour élaborer des normes communes qui serviront à l'avenir de base à l'harmonisation des cadres en vue de l'intégration des économies numériques sur le continent.

INSTRUIT LA COMMISSION DE L'UA DE :

28. **RELANCER** le projet de cadre d'interopérabilité de l'identification numérique et le cadre de politique des données continentales aux États membres pour des contributions finales et finaliser les documents pour permettre leur adoption par les organes politiques de l'UA.

29. **POURSUIVRE** le développement des stratégies, cadres politiques et projets numériques suivants :

    (i) Stratégie d'éducation numérique de l'UA et plan de mise en

œuvre, Stratégie d'agriculture numérique de l'UA et plan de mise en œuvre, Stratégie de commerce électronique

(ii) Stratégie de la cybersécurité continentale

(iii) Politique continentale de sécurité et d'autonomisation des enfants en ligne ;

(iv) Révision de la Convention de Malabo sur la cybersécurité et la protection des données personnelles et accélération de son entrée en vigueur ;

(v) Transformation numérique du secteur postal en Afrique ;

(vi) Stratégie continentale visant à renforcer l'harmonisation des politiques numériques et des cadres juridiques et réglementaires pour soutenir l'établissement d'un marché unique numérique en Afrique ;

(vii) Mise en correspondance des projets ou activités numériques avec les actions proposées par le DTS ;

(viii) Architecture de la mise en œuvre du DTS et cadre de suivi et d'évaluation.

(ix) Reconception du réseau électronique panafricain pour fournir des services de santé et d'éducation en ligne ;

(x) Stratégie d'IA continentale

(xi) Statistiques sur la connectivité numérique et la préparation au numérique des pays africains ;

30. **COLLABORER** avec les institutions régionales et les parties prenantes concernées afin d'élaborer un plan d'action pour guider la mise en œuvre du cadre de la politique continentale de l'UA en matière de données (à court, moyen et long terme) dès son adoption, y compris des actions immédiates pour atteindre le même niveau de préparation aux données au niveau continental.

31. **COORDONNER** l'élaboration d'un cadre commun de catégorisation des données et d'un mécanisme de flux transfrontaliers de données qui tiennent compte des différents types de données, de leurs différents niveaux de confidentialité et de sécurité, ainsi que des différents niveaux de maturité des données et de préparation au numérique des pays africains.

32. **CONSIDÉRER** l'alignement du cadre de la politique continentale de l'UA en matière de données, dès son adoption, sur le processus de la ZLECAf en incluant des dispositions relatives aux données dans les négociations des chapitres sur la concurrence et la propriété intellectuelle.

33. **S'ASSURER** que le guide de style de la marque et de la communication et les politiques et procédures de communication sont institués au sein de l'organisation et des organes et institutions de l'Union africaine ;

34. **ENTREPRENDRE** un exercice de comparaison des allocations budgétaires de communication pour des institutions de nature et de taille similaires à celles de l'Union africaine afin d'établir une base de référence pour le budget de communication à utiliser comme guide pour recommander un financement adéquat ;

35. **ALLOUER** des ressources financières réalistes pour renforcer les capacités de la direction de l'information et de la communication (DIC) afin de lui permettre de communiquer mieux et plus efficacement avec les diverses parties prenantes et les différents publics sur différentes plates formes médiatiques, de manière stratégique et cohérente ;

36. **ACCORDER LA PRIORITÉ** au renforcement des capacités de la Direction de l'information et de la communication dans la première phase des Réformes institutionnelles ;

37. **METTRE EN OEUVRE** la décision du Conseil exécutif EX.CL/Dec.1069 (XXXV) de juillet 2019 selon laquelle toutes les activités de l'UA relatives aux communications seront gérées par la Direction de l'information et de la communication ;

38. **APPROUVER** les initiatives visant à inonder le continent et à atteindre les Africains par le biais des radiodiffuseurs nationaux pour entreprendre les activités suivantes pour le mois de septembre 2022 en commémoration du 20e anniversaire de l'Union africaine :

i) Diffusion de l'hymne de l'UA sur toutes les stations de diffusion nationales en début et en fin de journée ;

ii) Lever du drapeau de l'UA aux côtés des drapeaux nationaux dans les États membres ;

iii) Diffuser une vidéo de célébration qui sera produite par la DIC sur toutes les chaînes de télévision des États membres de l'UA ; cette vidéo mettra en évidence le chemin parcouru par l'Afrique dans le cadre de l'UA, ainsi que les succès remportés, les défis à relever et les mesures d'atténuation prises ;

iv) Diffuser sur les chaînes de télévision et de radio nationales une conversation en ligne sur les réseaux sociaux avec les présidents de l'Union et de la Commission, dans laquelle ceux-ci décriront l'impact de l'UA et répondront à quelques questions du public ;

39. INVITER l'AUDA-NEPAD à:

i) Accélérer la mise en œuvre des projets PIDA-PAP2 sur les TIC et œuvrer à l'élaboration des politiques et réglementations nécessaires pour faciliter la connectivité transfrontalière et l'intégration régionale ;

ii) Étendre en collaboration avec le Forum mondial sur la cyber-expertise (GFCE) et d'autres parties prenantes sur les évaluations en matière de cybersécurité et le renforcement des capacités de tous les États membres de l'UA et travailler avec les États membres à la conception de plans d'action spécifiques aux pays en ce qui concerne la cybersécurité et la cyber-résilience ;

iii) Étendre l'usage de la boîte à outils de création d'emplois du PIDA à tous les sous-secteurs des TIC, former les États membres à sa pratique et entreprendre une analyse détaillée du potentiel d'emploi du PIDA et d'autres projets importants relatifs aux TIC en Afrique ;

iv) Conformément à l'approche du corridor intégré du projet PIDA-PAP 2, tenir compte des TIC, de la numérisation et de la cybersécurité dans la mise en œuvre des projets phares de l'Agenda 2063 tels que le réseau ferroviaire intégré à grande vitesse pour l'Afrique, le marché unique du transport aérien africain (SAATM), le Zone de libre-échange continentale africaine (ZLECAf), la libre circulation des personnes ainsi que des initiatives continentales telles que le marché unique de l'électricité en Afrique (AfSEM) ;

40. DEMANDER au Secrétariat de l'Union panafricaine des postes (UPAP) d'élaborer et de mettre en œuvre, en coordination avec la CUA, un programme de référence systématique et coordonné sur la transformation numérique pour faire en sorte que les postes africaines soient à jour ;

41. DEMANDER au Secrétariat de l'Union africaine des télécommunications (UAT) d'élaborer et de mettre en œuvre, en coordination avec la CUA, des programmes et des initiatives visant à favoriser une utilisation harmonisée et optimale du spectre radioélectrique à travers le continent afin de contribuer efficacement à combler le fossé de la connectivité numérique en Afrique ;

42. APPROUVER des initiatives de même nature pour le 60e anniversaire de l'Organisation de l'unité africaine en 2023, dont le contenu remonterait aux

réalisations de 1963 au lieu de commencer à celles de 2002 comme pour le 20e anniversaire ;

43. **RÉAFFIRMER EN OUTRE NOTRE DEMANDE** aux institutions financières et partenaires multilatéraux, en particulier la BAD, la Banque mondiale et d'autres, de continuer à fournir un soutien à l'utilisation des technologies existantes pour gérer la pandémie de COVID-19, la mise en œuvre de la stratégie de transformation numérique pour l'Afrique et la mise en œuvre globale de la présente Déclaration.

RECONNAISSANCE :

44. **EXPRIMONS** notre reconnaissance à la Commission de l'UA pour l'excellente organisation de cette conférence.

Fait le 27 octobre 2021

AFRICAN UNION

UNION AFRICAINE

الاتحاد الأفريقي

UNIÃO AFRICANA

Addis Ababa, ETHIOPIA P. O. Box 3243 Telephone: 251 11 551 7700 Fax: 251 11 551 7844
Website: www.au.int

EX.CL/1308(XL) Annexe 2

PROJET DE CADRE D'INTEROPÉRABILITÉ DES SYSTÈMES D'IDENTIFICATION NUMÉRIQUE DE L'UA

Décembre 2021

TABLE DES MATIÈRES

RÉSUMÉ ANALYTIQUE

Des centaines de millions de personnes en Afrique n'ont pas d'identification (ID) légale et beaucoup d'autres ont des documents d'identité qui ne sont pas adaptés à l'ère du numérique. En conséquence, ces personnes sont confrontées à des difficultés pour accéder aux services et aux opportunités créés par la numérisation. Les identités numériques fondamentales interopérables, fiables et inclusifs, qui permettent aux gens de vérifier leur identité légale hors ligne et en ligne, peuvent aider à relever ces défis et ont un potentiel important pour accélérer la numérisation des économies et des sociétés africaines en soutenant l'esprit d'entreprise et en contribuant à la mise en œuvre réussie de la Zone de libre-échange continentale africaine (ZLECAf). C'est pour ces raisons que la plupart des pays africains modernisent actuellement leurs écosystèmes d'identification, bien qu'à des stades différents.

Le projet de Cadre d'interopérabilité des systèmes d'identification numérique de l'UA (le Cadre) définit une vision qui permettra à tous les citoyens africains d'avoir la possibilité d'accéder facilement et en toute sécurité aux services publics et privés nécessaires, à tout moment, indépendamment de leur localisation. Dans cette optique, le Cadre définit des exigences communes, des normes minimales, des mécanismes de gouvernance et un alignement plus poussé entre les cadres juridiques, en vue d'atteindre les objectifs suivants :

1. Permettre aux citoyens africains de vérifier leur identité légale hors ligne et en ligne afin d'accéder aux services des secteurs public et privé dans les États membres de l'UA ;

2. Donner aux citoyens africains le contrôle de leurs données personnelles, y compris la possibilité de ne divulguer de manière sélective que les attributs nécessaires à une transaction particulière.[2] Les informations à caractère personnel à divulguer doivent être minimales, proportionnées et ne doivent contenir que les informations pertinentes à ce genre de transaction, compte tenu de la situation particulière de l'Afrique et conformément aux meilleures pratiques internationales.

3. Renforcer la confiance et l'interopérabilité entre les systèmes d'identification fondamentaux des États membres de l'UA.

Le Cadre prévoit une norme commune au niveau continental pour représenter numériquement les preuves d'identité délivrées par des sources fiables des États membres de l'UA et pour assurer l'interopérabilité sur tout le continent. Les personnes titulaires d'une pièce d'identité d'un système national pourront obtenir un justificatif d'identité numérique légal interopérable pour l'identité (IDC-ID) qui prendra la forme d'un renseignement vérifiable[3]. Des normes seront établies pour le cadre d'interopérabilité

[2] Le règlement général de l'UE sur la protection des données (RGPD)

[3] Les renseignements désignent un ensemble d'attributs concernant une personne concernée : par ex., le nom de famille, les données de naissance. Un renseignement vérifiable est une version inviolable de ces informations qui peut être vérifiée de manière cryptographique afin d'en contrôler l'authenticité.

qui définira des éléments clés de l'IDC-ID, qui démontrera la confiance accordée aux justificatifs numériques créés sous la gouvernance d'un cadre de confiance définissant les conditions dans lesquelles ces justificatifs seront délivrés par des sources fiable des États membres de l'UA.

Les États membres de l'UA sont libres de choisir la manière dont ils souhaitent délivrer ce justificatif d'identité numérique. Il pourra être stocké stockée dans un format purement numérique sur une application smartphone, un serveur en nuage, une carte à puce ou un lien permettant d'accéder à la représentation numérique qui pourra être établi à l'aide d'un code-barres à une ou deux dimensions sur un document papier (imprimé sur papier, carte plastique). Ils peuvent également décider de réutiliser cette norme pour représenter les données d'identité au niveau national, continental ou des CER, ou même émise séparément en complément de systèmes d'identification numérique préexistants.

Le Cadre sera basé sur le développement de systèmes d'identification fondamentaux interopérables, inclusifs et fiables, car ils constituent l'épine dorsale des sources de données faisant autorité sur l'identité légale des personnes et permettent ainsi à l'IDC-ID d'atteindre des niveaux d'assurance plus élevés. Les États membres de l'UA sont ainsi encouragés à renforcer leurs systèmes d'identification de base et *les principes d'identification pour le développement durable*. Ce cadre tient également compte des efforts continentaux parallèles pour créer un environnement favorable visant à protéger les données personnelles, à maintenir la cybersécurité et à sauvegarder les droits des personnes, grâce à l'adoption de la Convention de Malabo sur la cybersécurité et la protection des données personnelles[4] et à l'élaboration en cours d'un cadre politique continental sur les données.

La délivrance de l'IDC-ID pourra être achevée par une infrastructure permettant des cas d'utilisation plus avancés tels que l'authentification à distance. Ce Cadre met en évidence plusieurs options techniques à la disposition des États membres de l'UA pour mettre en œuvre cette couche, par exemple une fédération de fournisseurs d'identité assurant des mécanismes d'authentification aux détenteurs de l'IDC-ID, ou le développement de solutions de portefeuille d'identité numérique ou tout autre modèle permettant l'interopérabilité. Les États membres de l'Union africaine pourront également trouver un accord supplémentaire sur la manière d'établir cette infrastructure relative à la couche d'authentification et s'associer aux CER et à d'autres initiatives continentales qui étudient déjà la mise en place de solutions interopérables d'identification numérique fondamentales pour accéder aux services à distance.

La mise en œuvre du Cadre est fondée sur la supposition qu'il sera validé et approuvé par les États membres de l'UA. L'exclusivité potentielle, la faiblesse des mécanismes de sécurité, l'érosion de la protection de la vie privée, l'incertitude quant aux avantages d'un système d'identité numérique fondamental, le manque de capacités techniques et financières, le manque de centres de données en Afrique pour stocker les données

[4] Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, voir : https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

sensibles, la présence de systèmes d'identité non interopérables et de cadres juridiques et réglementaires obsolètes sont les défis identifiés à relever.

Ce document comprend les sections suivantes : -

1. Un **contexte** sur le travail de l'Union africaine qui a conduit à la création de ce document, un aperçu de l'état des systèmes d'identification en Afrique et une série d'initiatives favorisant l'interopérabilité des identités numérique sur le continent ;

2. Une **introduction** à la vision, aux objectifs, à la portée et aux cas d'utilisation potentiels du cadre d'interopérabilité des systèmes d'identification numérique proposé par l'UA ;

3. Une **vue d'ensemble des éléments clés constituant le Cadre**, notamment les principes directeurs pour sa conception et sa mise en œuvre, le modèle choisi, les composants clés du cadre qui devront être définis plus avant (par ex., les règles de participation, l'interopérabilité et les exigences techniques), ainsi que trois options architecturales potentielles pour mettre en place une couche d'authentification d'interopérabilité.

4. Une **feuille de route détaillée** sur l'approche progressive proposée pour la définition et la mise en œuvre du Cadre, ainsi que **des actions concrètes** à entreprendre par les États membres et l'Union africaine.

5. Hypothèses, défis et risques majeurs à traiter et mécanismes d'atténuation recommandés.

Le Cadre n'appelle pas à la création d'un système continental unifié d’identité numérique mais à l'établissement d'un cadre d'interopérabilité pour les systèmes d'identification numérique fondamentaux existants parmi les États membres de l'UA, qui tienne compte de la souveraineté numérique des États membres de l'UA, des divergences dans la mise en œuvre de l'infrastructure numérique, de la disponibilité des politiques et réglementations associées, des différents types de systèmes d'identification et de la vulnérabilité des populations pendant et après la mise en œuvre des systèmes d'identification numérique interopérables.

ACRONYMES ET ABRÉVIATIONS

ZLECAf	Zone de libre-echange continentale africaine
LCBA/FT	Lutte contre le blanchiment d'argent et le financement du terrorisme
API	Interface de programmation d'application
UA	Union africaine
CUA	Commission de l'Union africaine
CIRT	Equipes de reponse aux incidents informatiques
CRVS	Systemes d'Enregistrement des faits d'etat civil et d'etablissement des statistiques de l'etat civil
APD	Autorite de protection des donnees
AIPD	Analyse d'impact relative a la protection des donnees
CAE	Communaute d'Afrique de l'Est
CEDEAO	Communaute economique des États de l'Afrique de l'Ouest
GIZ	Gesellschaft für Internationale Zusammenarbeit
GSMA	GSM Association
HSM	Modules Materiels de Securite
TIC	Technologies de l'information et de la communication
IDC-ID	Justificatifs d'identite numerique interoperable
UIT	Union internationale des telecommunications
KYC	Systeme de gestion de la connaissance du client
LOA	Niveau d'assurance
PATF	Cadre de confiance panafricain
CER	Communaute economique regionale
RP	Partie interessee
SATA	Alliance Smart Africa Trust
Le Cadre	Cadre d'interoperabilite des systemes d'identification numerique de l'UA
CEA	Commission economique des Nations Unies pour l'Afrique
WURI	Projet d'Identification Unique pour l'Integration Regionale et l'Inclusion en Afrique de l'Ouest

Voir l'annexe I pour les definitions de travail.

CONTEXTE

1.1. Aperçu

Il est essentiel que les personnes puissent prouver leur identité pour pouvoir accéder aux services et exercer leurs droits. Traditionnellement, la preuve de l'identité pouvait se faire sur la base de la familiarité, de l'apparence et du témoignage d'autres personnes, ce qui fonctionnait dans les petites communautés informelles. À mesure que les sociétés et les économies se sont développées, des justificatifs physiques plus formels et intégrés, tels que les cartes d'identité et les passeports, ont été introduits pour établir la confiance. Cependant, à mesure que les pays évoluent vers des sociétés et des économies numériques, ces justificatifs physiques ne sont pas très utiles pour prouver l'identité sur l'internet et effectuer d'autres transactions numériques telles que les paiements numériques et le partage de données personnelles. La confiance en ligne repose ainsi sur les identités numériques, représentées par des identités numériques qui utilisent des technologies et des approches modernes pour permettre aux personnes de prouver et de vérifier leur identité en toute sécurité.

Les ID, et en particulier les identités numériques, peuvent offrir un large éventail d'avantages aux pays, tels que la bonne gouvernance, l'inclusion financière, l'égalité des sexes et l'autonomisation des femmes, ainsi qu'une meilleure protection sociale, des résultats en matière de soins de santé et d'éducation. Pour les individus, ils constituent un outil permettant de faire valoir leurs droits et leur éligibilité aux services et aux transactions. De même, ils constituent une plateforme permettant aux gouvernements et aux entreprises de rationaliser, d'étendre et d'innover dans la prestation de leurs services opérationnels grâce à la numérisation et à l'automatisation, en particulier lorsqu'ils sont envisagés comme une « pile numérique » avec des plateformes de partage de données et de paiement numérique fiables. L'apparition de la pandémie COVID-19 a montré l'importance des piles numériques, car les pays qui les avaient mises en place, en totalité ou en partie, avant le début de la pandémie ont été mieux à même de fournir rapidement et efficacement une assistance sociale et ont mieux résisté lorsque les services en personne ont dû passer en ligne. Compte tenu du fait que l'internet ne connaît pas de frontières, les identités numériques délivrées dans un pays et reconnues dans d'autres peuvent également constituer un puissant moteur d'intégration sociale et économique, que ce soit au niveau bilatéral, régional ou mondial.

La sécurité et l'impact des identités numériques sont optimaux lorsqu'elles sont fondées sur l'identité légale des personnes. L'identité légale est généralement gérée par l'écosystème d'identité fondamental d'un pays, y compris l'enregistrement civil, l'identité nationale et d'autres systèmes similaires. Malheureusement, des centaines de millions de personnes en Afrique n'ont toujours pas d'identité de base, comme une identité nationale ou un certificat de naissance[5]. C'est dans ce contexte qu'en juillet 2016, la Conférence des Chefs d'État et de Gouvernement de l'Union africaine a déclaré la période 2017-2026 comme la décennie de repositionnement des systèmes

[5] Banque mondiale, Ensemble de données mondiales ID4D 2018 : https://id4d.worldbank.org/global-dataset

d'enregistrement des faits d'état civil et d'établissement des statistiques d'état civil (CRVS) en Afrique en tant qu'agenda de développement continental, régional et national et a exhorté les gouvernements à répondre par des actions appropriées.

L'Agenda 2063 : L'Afrique que nous voulons qui est le cadre stratégique pour le développement socio-économique et la transformation du continent dans une période de 50 ans a demandé une identité légale pour tous. La Stratégie de transformation numérique pour l'Afrique (STN) approuvée lors de la 36e Session ordinaire du Conseil exécutif de l'Union africaine en février 2020 à Addis-Abeba, en Éthiopie (EX.CL/Déc. 1074(XXXVI)) a également souligné l'importance de l'identité numérique en tant qu'élément constitutif de l'établissement d'un marché unique numérique (une mission qui est également partagée par l'Alliance Smart Africa) conformément à la ZLECAf.

La Stratégie de transformation numérique pour l'Afrique a également reconnu que le développement de l'économie et de la société numériques repose sur des catalyseurs importants, notamment un environnement favorable solide en matière de cybersécurité et de protection des données. La Convention de Malabo de 2014 sur la cybersécurité et la protection des données personnelles[6] établit un cadre juridique, politique et réglementaire soutenant l'établissement d'un environnement numérique sûr pour les transactions numériques, le commerce électronique et le transfert de données. Malheureusement, ce cadre juridique n'a pas encore été signé et ratifié par le nombre requis d'États membres de l'UA pour qu'il entre en vigueur, ce qui limite effectivement son efficacité[7]. Ce cadre juridique contribuera non seulement à promouvoir la confiance dans le cadre et l'inclusion, mais aussi à atténuer les risques liés à la surveillance non autorisée et à la discrimination, en particulier pour les groupes vulnérables ou marginalisés, ainsi qu'à garantir la responsabilité des instances chargées de la mise en œuvre.

1.2. État des systèmes d'identité en Afrique

Les systèmes d'identification fiables et inclusifs sont un catalyseur pour de nombreux résultats de développement tels que l'élimination de la pauvreté, la bonne gouvernance, la migration sûre et ordonnée, la protection sociale, l'égalité des sexes, et finalement jouent un rôle important dans la transformation numérique. Compte tenu du besoin fondamental d'une identification et d'une authentification électroniques sûres et précises, l'identité numérique et les autres services fiduciaires, tels que les signatures électroniques, représentent le nouvel horizon pour les pays du continent. Une fois activés par l'infrastructure numérique qui met les personnes et les organisations en ligne, l'identité numérique et les services fiduciaires peuvent être exploités par les plateformes gouvernementales et commerciales pour faciliter une variété de transactions numériques, y compris les paiements numériques. Au niveau national, l'identités numérique pourrait servir d'identifiant unique pour les systèmes centrés sur le citoyen, ce qui rendrait viable

[6] Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, voir : https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[7] En juillet 2021, 14 États membres sur 55 ont signé la convention de Malabo, dont 8 l'ont ratifiée. Pour entrer en vigueur, une ratification par au moins 15 États membres est nécessaire.

l'intégration des systèmes. Les plateformes d'identité numérique et de paiement permettent d'évoluer vers une société sans numéraire, de réaliser des gains de productivité, de réduire la corruption et la fraude et d'améliorer le confort des utilisateurs.

A travers le continent, il existe un large éventail de types de systèmes d'identification et de niveaux de liens entre le développement et la prestation de services. De nombreux pays se trouvent à des niveaux intermédiaires de développement, avec des lacunes dans la couverture des populations vulnérables et des capacités numériques naissantes, tandis que d'autres n'ont toujours pas de systèmes d'identité fondamentale ou en sont à leurs débuts. Dans l'ensemble, le nombre de pays mettant en œuvre des systèmes d'identification nationaux a augmenté de manière exponentielle au cours des deux dernières décennies, poussés par le désir d'améliorer l'efficacité et le ciblage des paiements et des transferts gouvernementaux, de renforcer l'intégrité du secteur financier (notamment par le biais de KYC (système de gestion de la connaissance du client) et de l'enregistrement des cartes SIM) et celle des élections, de renforcer la sécurité publique et de favoriser une migration sûre et ordonnée. La réforme et la modernisation de la conception du système et des approches de mise en œuvre se poursuivent, conformément à la multiplication des bonnes pratiques et des enseignements tirés des programmes d'identité réussis[8]. Un bon exemple est fourni par le Rwanda qui a mené une campagne de numérisation de son économie et d'autonomisation de sa classe moyenne en menant des actions telles que le passage à une économie sans numéraire, que le gouvernement vise à réaliser par une pénétration omniprésente de la téléphonie mobile et un accès à l'Internet à haut débit. Le Rwanda a rejoint l'Alliance Better Than Cash, un partenariat mondial qui s'engage à passer des paiements en espèces aux paiements numériques. Le Rwanda réalise déjà une augmentation de l'efficacité et des revenus en éliminant les coûts de collecte et autres dépenses. Il est également devenu un leader en matière de connaissances dans la région et il partage ses meilleures pratiques avec d'autres pays désireux de suivre une voie similaire (Cadre d'investissement numérique au service des ODD, UTI/DIAL, 2019).

Les capacités numériques des systèmes d'identification se sont considérablement accrues, même si l'identification numérique dans le contexte des transactions en ligne n'en est encore qu'à ses débuts. Au cours de la dernière décennie, de nombreux pays se sont engagés dans des efforts de modernisation de leurs systèmes d'identification, dans le but de créer une plateforme numérique et de délivrer des justificatifs d'identité qui sous-tendent une variété d'utilisations et de services. Ces réformes impliquent fréquemment une transition du papier vers des systèmes numériques utilisant la capture et la gestion électroniques des données, et introduisant pour l'instant des mécanismes de vérification et d'authentification numériques de l'identité, principalement dans le cadre de transactions en personne. La majorité (85 %) des pays africains disposent de systèmes d'identification nationaux étayés par une base de données électronique, bien que nombre d'entre eux s'appuient encore sur des registres et des processus d'état civil sur papier, et que de nombreux systèmes offrent une utilité limitée pour la prestation de services. Les

[8] Une enquête menée en 2018 auprès de responsables gouvernementaux africains a révélé que 60 % des pays africains prévoyaient de lancer un système d'identification ou de moderniser le système existant d'ici à la fin de 2020.

données biométriques sont collectées par plus de 70 % des pays africains au moment de l'enregistrement afin de garantir l'unicité des identités. Bien que certains pays - comme l'Afrique du Sud, le Kenya, le Lesotho, le Nigeria et le Rwanda - proposent des services de vérification numérique de l'identité (aux ministères, aux banques, etc.) pour valider les informations d'identité ou les justificatifs dans une base de données centrale, l'authentification pour la plupart des transactions continue de reposer sur l'inspection manuelle des cartes d'identité physiques. Les solutions d'identité numérique permettant une authentification sécurisée pour les services et les transactions électroniques n'en sont encore qu'à leurs débuts sur le continent, ces services n'étant disponibles que dans une poignée de pays (par ex., en Afrique du Sud pour les banques, au Cabo Verde, aux Seychelles pour les services d'administration en ligne).

En dépit de nombreuses améliorations et du lancement de nouveaux systèmes ces dernières années, les pays africains et leurs résidents sont confrontés à plusieurs défis en matière d'identification. Parmi les domaines clés qui ont dû être renforcés figurent l'accessibilité des systèmes d'identification, leur capacité à soutenir efficacement la prestation de services et la mise en œuvre de garanties favorisant la confiance et la confidentialité des données.

Garantir l'accessibilité universelle des systèmes d'identification est un défi permanent. On estime qu'un milliard de personnes dans le monde n'ont pas de documents d'identité de base - et environ la moitié de cette population réside en Afrique[9]. L'Afrique abrite également 8 des 10 pays présentant les plus grands écarts entre les sexes en matière d'identification au niveau mondial et la couverture d'identification des adultes en Afrique subsaharienne est inférieure de près de 10 points de pourcentage chez les femmes par rapport aux hommes[10]. Les problèmes d'identification commencent dès la naissance : en Afrique, 100 millions d'enfants de moins de cinq ans n'ont pas été enregistrés à la naissance[11]. Les raisons de ces écarts de couverture sont multiples et comprennent : les coûts directs et (surtout) indirects élevés de l'inscription, y compris le coût des déplacements vers des sites d'enregistrement souvent éloignés ; des exigences documentaires et administratives complexes pour l'enregistrement ; et une demande limitée où les systèmes d'identification offrent une valeur limitée en termes de facilitation de l'accès aux services[12].

L'utilisation des technologies modernes a également accru la complexité et présente de nouveaux risques. Par exemple, toutes les solutions ne sont pas bien adaptées aux besoins et contextes locaux où la connectivité à Internet, l'accès à l'électricité ou la culture numérique des fonctionnaires ou de la population en général peuvent être limités. Le verrouillage des fournisseurs est une préoccupation commune, et est souvent associé à des coûts d'exploitation élevés insoutenables, à une

[9] Ensemble de données mondiales ID4D 2018 : https://id4d.worldbank.org/global-dataset
[10] https://documents1.worldbank.org/curated/en/727021583506631652/pdf/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-An-In-Depth-Look-at-the-2017-ID4D-Findex-Survey.pdf
[11] https://www.unicef.org/media/62981/file/Birth-registration-for-every-child-by-2030.pdf
[12] https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf

interopérabilité limitée du système d'identification et à de faibles niveaux de surveillance et de contrôle des données d'identité par les gouvernements et les particuliers. En outre, avec l'adoption accrue des technologies numériques dans l'identification et l'authentification, ainsi que le passage à des justificatifs numériques, les personnes dont la culture numérique et l'accès aux appareils connectés sont limités risquent d'être laissées pour compte.

Avec la numérisation des systèmes et du traitement des données, la nécessité de mettre en place des garanties efficaces pour protéger les données et la vie privée des personnes s'est également accrue. Des garanties inadéquates en matière de protection des données, de respect de la vie privée et de droits des utilisateurs - qu'elles soient juridiques, institutionnelles ou technologiques - peuvent rendre les systèmes d'identification vulnérables aux violations et laisser les données des personnes sans protection. De nombreux pays ont encore des progrès à faire pour mettre en place des systèmes d'identification sûrs et fiables : selon la CNUCED, seuls 28 pays d'Afrique (50 %) ont adopté une législation sur la protection des données et de la vie privée et 39 (70 %) ont mis en place une législation sur la cybercriminalité[13]. En outre, même lorsque de tels cadres existent, il peut être difficile de traduire efficacement les dispositions légales en contrôles institutionnels, opérationnels et techniques. À ce jour, seuls un petit nombre de pays stockent et gèrent leurs données selon les meilleures pratiques internationales pour se protéger contre le vol ou la perte involontaire de données[14].

Les systèmes d'identification numérique sont confrontés aux mêmes défis que le développement des écosystèmes numériques ; ces défis englobent notamment les questions de financement, car les cycles de financement, principalement ceux des donateurs qui sont basés sur des projets et limités dans le temps, sont déconnectés des cycles de développement technologique. En outre, la planification en vase clos et la prise de décision entre les groupes de parties prenantes limitent les possibilités de coordination entre eux, ce qui limite la réutilisation des solutions numériques et compromet leur applicabilité potentielle dans les programmes et les secteurs. Les lacunes en matière de culture numérique, à savoir le manque de capacités en matière de leadership dans le domaine des TIC et de sélection, de conception, de mise en œuvre, de mise à l'échelle et de maintenance des solutions TIC, sont souvent un problème pour les gouvernements et les praticiens du développement. Enfin, l'absence de financement pour la mise à l'échelle des solutions TIC est une autre grande préoccupation, dans la mesure où des fonds peuvent généralement être disponibles pour financer les premières étapes du cycle de vie du développement technologique, mais où les fonds disponibles pour la mise à l'échelle au niveau national sont limités (Cadre d'investissement numérique au service des ODD, UTI/DIAL, 2019).

1.3. **Autres initiatives favorisant la reconnaissance mutuelle et**

[13] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx
[14] https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf

l'interopérabilité des identifications numériques en Afrique

Un certain nombre d'initiatives existantes, complémentaires au Cadre, favorisent par ailleurs la reconnaissance mutuelle et l'interopérabilité des identifications numériques en Afrique. Elles comprennent, mais ne sont pas limitées à :

1.3.1. Stratégie de transformation numérique pour l'Afrique (2020-2030)

L'identité numérique est reconnue comme l'un des cinq thèmes transversaux de la stratégie, qui formule également dix recommandations politiques et propositions d'actions à travers deux thèmes : assurer l'inclusion, la sécurité, la confidentialité et la propriété des données, et soutenir l'interopérabilité et la neutralité. Bien que ces recommandations portent principalement sur le développement de systèmes nationaux d'identité numérique, une recommandation appelle à la création d'une «identité numérique ouverte et interopérable à l'échelle du continent, permettant la validation et l'authentification des personnes », tandis qu'une autre recommandation demande à la CUA, à la CEA et à d'autres partenaires de « collaborer à l'élaboration de normes continentales et régionales, notamment sur les protocoles d'authentification, les champs de données minimums, les protocoles de déduplication, les formats biométriques ainsi que d'autres formats, les réglementations types et d'autres normes ».

1.3.2. Initiative de la CEA sur l'identité numérique

La Commission économique des Nations Unies pour l'Afrique (CEA) a lancé une initiative sur l'identité numérique, le commerce numérique et l'économie numérique (DITE), faisant office de centre d'excellence, qui vise à harmoniser des normes connexes, à adopter des règlements pour garantir la sécurité, à augmenter les investissements et à développer les capacités et les compétences des acteurs clés[15]. Le Centre d'excellence numérique de la CEA soutient les travaux visant à établir un cadre continental africain d'identité numérique harmonisé, à définir et à façonner des politiques et des normes d'identité numérique, à assurer le développement des capacités des États membres, des communautés économiques régionales et de l'Union africaine. La CEA a produit un livre blanc sur un cadre pour l'interopérabilité numérique par l'établissement d'un cadre de confiance panafricain (PATF).

1.3.3. Alliance Smart Africa Trust (SATA)

Smart Africa est une initiative des chefs d'État africains visant à accélérer le développement socio-économique de l'Afrique en tirant parti des TIC. En 2020, le Bénin a préconisé d'un projet phare de Smart Africa visant à élaborer le schéma directeur d'identité numérique, soutenu par un groupe de travail comprenant le Rwanda, la Tunisie, l'Union africaine (UA), l'Union internationale des télécommunications (UIT), la Banque mondiale, le réseau Omidyar, la Commission économique des Nations unies pour l'Afrique (CEA), la GSM Association, le Forum économique mondial, la Gesellschaft für

[15] CEA, DITE pour l'Afrique, voir : https://www.uneca.org/dite-africahttps://www.uneca.org/dite-africa

Internationale Zusammenarbeit (GIZ) et plusieurs entreprises privées. Il a été adopté par le conseil d'administration de Smart Arica, qui comprend ses 32 États membres, l'UA et l'UIT. Le schéma directeur[16] propose SATA comme plateforme pour faciliter la reconnaissance mutuelle de confiance des identités numériques entre une série d'acteurs par le biais de mécanismes de certification fédérés. Des projets pilotes de SATA devraient avoir lieu au Bénin, au Rwanda, en Tunisie et dans d'autres États membres de Smart Africa. SATA servira de solution agile et adaptable pour permettre l'interopérabilité entre divers systèmes d'identité publics et privés sur le continent. Plus de détails seront disponibles sur sata.smartafrica.org

1.3.4. Projet d'identifications uniques pour l'intégrationrégionale et l'inclusion en Afrique de l'Ouest (WURI)

Le WURI constitue[17] un programme régional qui bénéficie d'un financement de la Banque mondiale pour accroître l'accès aux services dans les États membres de la CEDEAO participants en construisant des systèmes d'identification fondateurs qui sont accessibles à toutes les personnes sur le territoire du pays - sans considération de nationalité ou de statut juridique - et qui sont conçus dans une optique d'interopérabilité transfrontalière pour débloquer l'accès aux services sociaux, sanitaires, financiers et autres à travers les frontières. La Côte d'Ivoire, la Guinée et la Commission de la CEDEAO ont rejoint la phase 1 en 2018, et le Bénin, le Burkina Faso, le Niger et le Togo font partir de la phase 2 en 2020. Les principes clés du WURI comprennent l'enregistrement accessible à tous et inclusif, la minimisation des données et les références de base qui sont fournies à coût nul à la population.

1.3.5. Protocole du marché commun de la CAE

En vertu de l'article 8 du Protocole, les six États partenaires de la CAE se sont engagés à travailler progressivement à la mise en place « d'un système standard commun de délivrance de documents d'identification nationaux à leurs ressortissants »[18]. Cet engagement est étroitement lié à la réalisation d'autres objectifs du Protocole, notamment la libre circulation des marchandises (article 6), des personnes (article 7), de la main-d'œuvre/des travailleurs (article 10), des services (article 16) et des capitaux (article 24), ainsi que les droits d'établissement et de résidence (articles 13 et 14, respectivement). Les systèmes nationaux d'identification sont toutefois à des stades de développement différents. Néanmoins, dans le cadre de la géométrie variable et à l'initiative des projets d'intégration du corridor nord (NCIP), le Kenya, le Rwanda et l'Ouganda ont commencé en 2014 à reconnaître les cartes d'identité nationales des uns et des autres comme des documents de voyage valables. Dans le cadre du NCIP, il y a eu des discussions pour s'appuyer sur cette initiative pour des cas d'utilisation supplémentaires tels que les

[16] Smart Africa, Schéma directeur | Alliance Smart Africa - Identité numérique, octobre 2020, voir : https://smartafrica.org/knowledge/digital-id/.

[17] Banque Mondiale. Programme d'identification unique pour l'intégration régionale et l'inclusion en Afrique de l'Ouest (WURI). https://projects.worldbank.org/en/projects-operations/project-detail/P161329 ; https://projects.worldbank.org/en/projects-operations/project-detail/P169594

[18] https://www.eac.int/images/doc_image_png_NnlwzXikEvuHdytNzkKNVDMScreen%20Shot%202017-06-20%20at%20153445.png

services électroniques, mais elles ne se sont pas encore concrétisées. En 2018, la Banque mondiale et le secrétariat de la CAE ont réalisé une étude sur les possibilités de reconnaissance mutuelle des cartes d'identité nationales (NID) au sien de la CAE qui proposait quatre étapes.

1.4. La souveraineté numérique et des données

Avec 55 nations souveraines, l'Afrique compte en effet 55 entités juridiques à prendre en compte. La souveraineté numérique décrit un spectre de différents concepts techniques et réglementaires, allant de l'emplacement physique des serveurs à la construction de câbles sous-marins, en passant par les lois et pratiques relatives à la protection des données et à la taxation des marchés de données, qui permettent aux États de prendre leurs propres décisions sur les choix technologiques et leur réglementation.

Dans le but de garantir la souveraineté numérique et des données[19], les États membres de l'UA sont encouragés à :

1. mettre en place des systèmes de stockage sécurisés pour les données à caractère personnel (y compris les données sensibles) en concevant et en créant des centres de données nationaux qui devront permettre le contrôle des données par l'État et comprendre au minimum d'espace de stockage et de traitement dédiés exclusivement aux données à caractère personnel et sensibles. Il sera également nécessaire de mettre en place les garanties requises (techniques, en particulier) pour s'assurer que les données utilisées dans les échanges d'informations transfrontaliers ne comprennent en aucun cas des données à caractère personnel ou sensibles dont le traitement ou le stockage présenterait des risques graves pour les droits des personnes ou la souveraineté des États membres de l'UA.

2. renforcer les capacités et les infrastructures pour le développement des talents et des compétences africaines afin de relever les nouveaux défis et de renforcer la souveraineté numérique. Les États membres sont censés prendre l'initiative de faire progresser les compétences (y compris les compétences en matière de cyber-résilience) de tous les citoyens et résidents, et devraient donner aux gens les moyens de contrôler leurs données personnelles.

3. établir un partenariat basé sur le respect mutuel, une situation gagnant-gagnant sans compromettre la souveraineté et la propriété nationale et éviter les interférences étrangères qui pourraient affecter négativement la sécurité nationale, les intérêts économiques et les développements

[19] L'expression "souveraineté en matière de données" utilisée dans le présent Cadre a la signification suivante : les données à caractère personnel (y compris les données sensibles) liées aux systèmes d'identification numérique dans un État membre de l'UA doivent être collectées, stockées et traitées (i) dans des installations détenues ou contrôlées par l'État membre de l'UA et (ii) conformément au droit applicable de cet État,

numériques des États membres de l'UA.

Le Cadre sera guidé par les règles souveraines représentées par la ou les autorités d'enregistrement et de délivrance de l'identité de chaque État membre de l'UA, ainsi que par la structure de gouvernance, y compris la création d'une institution de coordination continentale de surveillance qui sera approuvée par les États membres de l'UA. En outre, les mécanismes de responsabilité, y compris le traitement des obligations en cas de faute, seront définis et approuvés par les États membres de l'UA. Le développement de la confiance à l'échelle du continent entre des États souverains dotés de systèmes d'identification numérique divergents est une tâche complexe mais réalisable, qui nécessite la collaboration de plusieurs parties prenantes. Afin de parvenir à l'interopérabilité pour l'échange d'informations sur l'identité légale dans les différents pays africains, les points communs entre les règles et normes nationales existantes doivent être reconnus, sur la base d'un ensemble minimal de critères qui permettront à la fois la souveraineté locale et une confiance suffisante dans l'approche de chacun.

Les États membres de l'UA doivent à cette fin renforcer et améliorer leurs cadres légaux et leurs capacités d'exécution, en particulier les capacités des autorités chargées de la protection des données à surveiller les transferts transfrontaliers de données et à faire appliquer les lois et règlements pertinents en cas de violation ou d'utilisation abusive.

Le Cadre proposé englobera les technologies de pointe et respectera les lois et réglementations des pays. Les gouvernements ne devraient pas être obligés d'utiliser des technologies spécifiques. L'utilisation de normes et de standards ouverts devrait garantir une grande diversité de choix technologiques par les États tout en facilitant l'appropriation et l'interopérabilité par les pays.

INTRODUCTION

En 2020, les États membres de l'Union africaine ont adopté la Stratégie de transformation numérique (STN) pour l'Afrique (2020-2030) avec la vision suivante :

> *Une société et une économie numériques intégrées et inclusives en Afrique qui améliorent la qualité de vie des citoyens africains, renforcent le secteur économique existant, permettent sa diversification et son développement, et assurent une appropriation continentale avec l'Afrique en tant que producteur et pas seulement consommateur dans l'économie mondiale.*

La réalisation de cette ambition - ainsi que celle de la ZLECAf - dépend du développement de systèmes d'identification numérique fondamentaux inclusifs et fiables qui permettent à tous les citoyens africains de prouver et de vérifier leur identité légale de manière fiable et sûre lors de transactions en personne et en ligne, et qui permettent aux prestataires de services des secteurs public et privé de reconnaître les pièces d'identité, quel que soit l'endroit d'Afrique où elles ont été émises. Il est important de noter que les systèmes d'identité numérique fondamentaux doivent être conçus de manière à renforcer

l'autonomie des personnes, notamment des populations défavorisées et marginalisées. Cela permettra à tous les citoyens africains de participer de manière significative à l'économie et à la société numériques, de débloquer l'accès aux services à l'intérieur des pays et au-delà des frontières, de promouvoir le commerce dans le cadre de la ZLECAf, de renforcer la confiance dans la société et l'économie numériques, et de réduire la fraude et le coût des transactions commerciales.

Il est important de noter que les systèmes d'identité numérique fondamentaux peuvent également soutenir le développement de « piles numériques »[20] plus larges avec des plateformes de paiement numérique et de partage de données fiables afin de créer des opportunités d'innovation et un large éventail de transactions sans présence, sans papier et sans argent liquide sur le continent. Cependant, cela nécessite également une atténuation complète des risques liés à l'exclusion, à la protection des données, à la cybersécurité et au verrouillage des technologies et des fournisseurs. C'est pour ces raisons que l'identité numérique est l'un des cinq thèmes transversaux de la STN, fournissant le mandat et la base du présent Cadre.

2.1. Vision, objectifs et cas d'utilisation indicatifs

La vision du *Cadre d'interopérabilité des systèmes d'identité numérique de* l'UA est que toutes les citoyens africains en Afrique peuvent accéder facilement et en toute sécurité aux services dont elles ont besoin, quand elles en ont besoin, auprès de fournisseurs des secteurs public et privé, ce qui encouragera une participation inclusive et significative dans l'économie et la société numériques au sens large et de permettre aux services de fonctionner avec une plus grande confiance et certitude.

1. Dans cette optique, le Cadre définit des exigences communes, des règles minimales, des normes, des mécanismes de gouvernance, ainsi qu'un alignement entre les cadres juridiques, avec les objectifs de :permettre aux citoyens africains de vérifier leur identité légale hors ligne et en ligne pour accéder aux services des secteurs public et privé dans tous les États membres de l'UA participants ;

2. donner aux citoyens africains le contrôle de leurs données personnelles, y compris la possibilité de ne divulguer que les attributs requis pour une transaction particulière ;

3. renforcer **la confiance et l'interopérabilité** entre les systèmes d'identification fondamentaux des États membres de l'UA.

Le Cadre n'appelle pas à la création d'un système continental unifié d'identification numérique mais fournit une base pour l'interopérabilité entre les systèmes d'identification

[20] Dans le contexte des technologies numériques, une « pile » constitue un ensemble de composants logiciels ou d'infrastructures indépendants qui fonctionnent ensemble pour permettre l'exécution d'un cas d'utilisation.

numérique existants des États membres de l'UA. qui prend en compte la souveraineté numérique des États membres de l'UA, les divergences dans la mise en œuvre de l'infrastructure numérique, la disponibilité des politiques et réglementations associées, les différents niveaux des systèmes d'identification et la vulnérabilité des populations pendant et après la mise en œuvre des systèmes d'identification numérique.Il est primordial que ce Cadre soit développé conformément aux meilleures pratiques et aux normes internationales[21] visant à protéger les données personnelles, à maintenir la cybersécurité et à sauvegarder les droits des personnes. Avec l'adoption de la Convention de Malabo sur la cybersécurité et la protection des données personnelles et le travail en cours pour développer un cadre continental de politique des données[22], l'Union africaine a pris une mesure importante pour établir un environnement numérique crédible pour les transactions en ligne via l'adoption d'un ensemble commun de règles pour régir le transfert transfrontalier des données personnelles sur le continent et l'alignement des cadres nationaux de protection des données et de cybersécurité.

Un cadre continental peut faciliter l'accès aux services dans tous les pays participants en permettant aux personnes et aux entreprises de vérifier les justificatifs d'identification et d'autres faits sans divulguer de données personnelles. Cela inclut la possibilité d'authentifier leur identité lorsqu'ils accèdent à des services en ligne (par ex., des services gouvernementaux) dans un autre pays avec leur identité numérique sans avoir besoin de s'inscrire aux solutions d'identité fondatrices locales reconnues par les prestataires de services étrangers. L'interopérabilité des identités numériques facilitent également le partage et le consentement pour des références vérifiables et des données fiables lors de la demande de services où la loi exige une telle vérification (par ex., preuve d'assurance, statut de vaccination), permettant aux gens de gagner du temps et de réduire la paperasserie.

Elle peut également renforcer l'intégrité et l'accessibilité des paiements transfrontaliers et des services financiers en Afrique, et créer des opportunités d'innovation. Les systèmes d'identification faibles et non fiables, l'absence d'harmonisation des règles créent des risques de blanchiment d'argent et de lutte contre le financement du terrorisme (AML/CFT),[23] qui entravent les échanges transfrontaliers, augmentent les coûts des services (par ex., les transferts de fonds) et freinent l'innovation. L'identité numérique peut faciliter l'identification et la vérification des clients lors de l'intégration, soutenir les processus de la connaissance du client et faciliter le suivi des transactions dans le but de détecter et de signaler les transactions suspectes. L'interopérabilité permettra non seulement aux migrants d'envoyer plus facilement de l'argent chez eux en allégeant la

[21] Il s'agit notamment de l'UIT-T X.1058, de l'ISO/IEC 29151, des principes et recommandations des Nations unies pour les systèmes de statistiques de l'état civil, des dix principes de l'identification pour le développement durable, des normes internationales sur la protection des données, du règlement général européen sur la protection des données, etc.

[22] Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, voir : https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

[23] Les risques AML/CFT font référence aux risques de blanchiment d'argent et de financement du terrorisme. Le FATF recommande aux gouvernements de mettre en place une approche multipartite intégrée pour comprendre les opportunités et les risques liés à l'identification numérique et pour élaborer des réglementations et des conseils afin d'atténuer ces risques.

vérification de la connaissance du client et la charge d'authentification, mais elle contribuera également à réduire les coûts, aidant ainsi l'Afrique à se rapprocher de la cible de l'ODD (10.c) de trois pour cent d'ici 2030.

Un Cadre continental peut également renforcer le commerce et le commerce électronique en augmentant la confiance dans les transactions commerciales électroniques et en facilitant les affaires et le commerce à travers l'Afrique. En 2020, le commerce intra-africain ne représentait approximativement que 16,6 % du PIB de l'Afrique[24]. La ZLECAf a été lancé en 2019 afin de débloquer de nouvelles opportunités pour les échanges commerciaux et le commerce électronique d'ici 2030. La reconnaissance transfrontalière des pièces d'identité numériques peut contribuer à renforcer les contrôles d'identité des acheteurs et des vendeurs, en particulier pour les biens soumis à restrictions vendus en ligne. Elle peut également permettre des signatures électroniques pour des transactions 100% en ligne et sans papier, ce qui permet aux entreprises et aux clients de gagner du temps et de renforcer la sécurité en réduisant les risques d'usurpation d'identité. Elle simplifie également le commerce transfrontalier en permettant aux entreprises de gérer numériquement leur interaction avec les pouvoirs publics, par exemple en déclarant des taxes, en participant à des procédures de passation de marchés, en demandant un numéro de TVA et en demandant des autorisations.

2.2. **Champ d'application**

Pour atteindre ces objectifs, le Cadre définira :

- Le type d'informations/données qui peuvent être partagées sous la forme d'un ensemble minimal de données pour les informations d'identité fondamentales[25] ;

- La manière de prouver qui a émis les données et qu'elles sont dignes de confiance ;

    - Établir un processus pour communiquer les sources autorisées fiables pour les données d'identité dans chaque État membre de l'UA ;

    - Déterminer la manière dont vérifier l'authenticité du renseignement numérique ;

- Les normes et processus qui décrivent comment les données sont partagées par les utilisateurs et vérifiées par d'autres dans un environnement hors ligne et en ligne.

---

[24] CNUCED, Rapport sur le développement économique en Afrique 2019 : Made in Africa : Des règles d'origine pour un commerce intra-africain renforcé, voir : https://unctad.org/press-material/facts-figures-0.

[25] Bien que le champ d'application de ce document se concentre sur les données d'identité, le cadre de confiance proposé peut être étendu par les États membres de l'UA pour représenter d'autres preuves et réalisations, comme les diplômes, les qualifications professionnelles, etc....

Ce document présente les fondements d'un cadre de confiance et d'interopérabilité des systèmes d'identification numérique sur le continent africain. Il définira les exigences minimales nécessaires pour assurer l'interopérabilité entre les systèmes d'identité numérique existants et futurs. L'interopérabilité désigne la capacité des différentes parties du Cadre - telles que les systèmes d'identité numérique et les systèmes des parties intéressées - à communiquer et à s'interfacer efficacement aux niveaux technique et sémantique. L'interopérabilité peut faciliter la reconnaissance mutuelle, ce qui représente une construction juridique, mais elle n'est pas une condition préalable et ne garantit pas la reconnaissance mutuelle. Le Cadre ne définit pas un système d'identité numérique unifié pour l'Afrique et ne traite pas des accords commerciaux et de responsabilité entre les États membres participants.

De nombreux pays africains disposent déjà de systèmes d'identification numérique bien établis et certains ont introduit des capacités d'authentification numérique. **Le Cadre fournit des exigences communes pour la communication des données et des processus d'identité fondamentaux qui seraient interopérables et acceptés dans d'autres États membres africains, tandis que les États membres conservent le plein contrôle et le choix pour la conception de leurs systèmes nationaux.**

Le Cadre complétera et s'appuiera sur, plutôt que de dupliquer, les activités associées au Protocole au Traité instituant la Communauté économique africaine relatif à la libre circulation des personnes, au droit de résidence et au droit d'établissement, et à la Conférence des ministres africains chargés de l'enregistrement des faits d'état civil et au Programme africain pour amélioration accélérée des systèmes CRVS (APAI-CRVS). La mise en œuvre du Cadre doit être étroitement coordonnée avec cette initiative et d'autres initiatives pertinentes, notamment pour étudier la migration en tant que cas d'utilisation supplémentaire des cartes d'identité numériques au moment opportun et pour veiller à ce que la couverture et la qualité des systèmes CRVS soient améliorées en tant que contribution importante aux systèmes d'identification numérique de base.

2.3. Cadre de confiance, confidentialité des données, interopérabilité et normes

Les systèmes d'identité doivent favoriser la confiance entre les différentes parties participantes, en veillant à ce que les droits légaux des utilisateurs individuels et des organismes d'exploitation soient respectés, et à ce que l'utilisation éthique des systèmes d'identité soit encouragée. Pour garantir cette confiance, il convient de définir un ensemble de règles auxquelles toutes les parties adhèrent et qu'elles respectent, à savoir un Cadre de confiance.

Si la technologie constitue un élément clé, les cadres de confiance se concentrent également sur les processus et les procédures. Un cadre de confiance solide doit définir clairement les :

- **Exigences commerciales** (par ex., portée, services fournis, exigences en

matière de participation) ;

- **Exigences techniques** (par ex., formats de données, interfaces, normes) ;

- **Exigences opérationnelles** (par ex., le fonctionnement de la preuve d'identité et de l'authentification, le support, les communications) ; et

- **Exigences juridiques** (par ex., niveaux de service, responsabilité, résolution des litiges, reconnaissance de la légalité des transactions électroniques dans les pays) pour le système d'identité.

Le Cadre est fondé sur l'interopérabilité. Pour faciliter l'interopérabilité, une entité doit pouvoir faire confiance à une autre entité en se basant non seulement sur l'intégrité des processus techniques (par ex., preuve cryptographique, etc.), mais aussi sur la provenance des données partagées (par ex., les processus de collecte et d'attribution d'un certain enregistrement à un individu).

L'interopérabilité n'exige pas que les systèmes d'identification fondamentaux soient uniformes, mais simplement que certaines normes communes et ouvertes soient respectées. En vertu de ce Cadre, chaque pays participant peut créer des systèmes d'identification fondamentaux adaptés aux besoins, aux traditions et à la législation locaux, à condition que certaines normes permettant l'interopérabilité soient respectées. Les normes ouvertes établissent des protocoles d'échange, des régimes d'essai, des mesures de qualité et des bonnes pratiques universellement compris et cohérents concernant la saisie, le stockage, la transmission et l'utilisation des données d'identité légale, ainsi que le format et les caractéristiques des justificatifs d'identité légale et des protocoles d'authentification.

Lors de l'examen de l'interopérabilité des justificatifs d'identité numérique et de l'authentification sur le continent, il sera important d'envisager des normes ouvertes pour les renseignements d'identité, la manière dont elles sont émises et la manière dont la confiance est communiquée entre les entités impliquées dans le Cadre de confiance. Ces renseignements, qui formeront la **base de l'identité numérique légale**, proviendront souvent de sources faisant autorité, telles que les agences gouvernementales. Un mécanisme d'authentification doit également être défini pour permettre aux détenteurs d'une identité numérique légale de partager ces renseignements avec les fournisseurs de services de manière appropriée, en veillant à ce que la divulgation des données soit binaire et que toute métadonnée soit masquée, et à ce que la vie privée et les droits des personnes soient protégés à tout moment.

Ce Cadre définira **la manière dont la confiance peut être établie dans ces renseignements vérifiables, et le fonctionnement des éléments de gouvernance et des normes pour les données**. La mise en œuvre technique de la solution peut être pilotée par le marché qui pourra s'appuyer sur le cadre de confiance pour développer des solutions innovantes d'identification numérique fondatrice. Le Cadre place la confidentialité, l'audit et la protection des données au premier plan et établit une

procédure transparente applicable à toutes les parties utilisatrices concernées sur la façon dont les données sont demandées, collectées, transmises et stockées et qui respecte des normes bien acceptées sur la procédure de partage des informations/données. L'importance de la tokenisation pour réduire les possibilités de collecte de données, de clonage et de fraude, en présentant au détenteur de l'identité la possibilité d'émettre des identités virtuelles, ce qui permet de protéger les identités réelles, est un aspect supplémentaire qui sera approfondi pour renforcer la confidentialité des données au niveau national/continental.

LE CADRE

Le Cadre d'interopérabilité des systèmes d'identification numérique de l'UA propose de définir, au niveau continental, une approche harmonisée permettant aux individus de partager avec les fournisseurs de services des preuves d'identité numérique[26] délivrées par des autorités de confiance, afin de prouver leur identité légale dans un environnement en ligne et hors ligne. Il s'agira de convenir d'une **norme commune pour représenter les preuves d'identité légale existantes délivrées par les États membres de l'UA dans un format numérique**[27]. L'authenticité de ces justificatifs d'identité[28] pourrait être vérifiée afin de garantir un niveau élevé de confiance et de sécurité.

Les systèmes nationaux d'identité fondamentaux ne sont soumis à aucune restriction quant à leur mode de fonctionnement ou aux types d'informations d'identification qu'ils utilisent pour authentifier les personnes ; chaque pays est souverain à cet égard. L'intention du Cadre est de créer les conditions de l'interopérabilité à l'échelle continentale en s'appuyant sur les systèmes existants là où ils existent et plutôt que de restreindre leur utilisation, d'étendre leur portée.

Les justificatifs d'identité numérique interopérable (IDC-ID) émises conformément au Cadre de l'UA prendront la forme d'un renseignement vérifiable qui viendra compléter les systèmes d'identification nationaux fondamentaux existants et les projets de coopération régionale, sans remplacer les systèmes d'identification numérique nationaux des États membres de l'UA. Les États membres de l'UA restent libres de choisir la manière dont ils souhaitent délivrer ce justificatif d'identité numérique. Elle peut être stockée dans un format purement numérique sur une application smartphone, un serveur en nuage, une carte à puce ou un lien vers la représentation numérique qui peut être établi à l'aide d'un code-barres à une ou deux dimensions sur un document papier (imprimé sur papier, carte plastique).

Le Cadre sera fondé sur le développement de systèmes d'identification interopérables, inclusifs et fiables, car ils constituent l'épine dorsale des sources de données faisant

[26] Les renseignements constituent un ensemble d'attributs concernant une personne concernée : par ex., le nom de famille, les données de naissance.

[27] Le cadre actuel se concentre sur la définition de renseignements vérifiables pour prouver des données d'identité, mais il pourrait être étendu pour partager des renseignements vérifiables sur des réalisations académiques, des qualifications professionnelles, etc...

[28] Un justificatif est composé d'un renseignement d'identité, de métadonnées sur l'émetteur et d'une preuve d'authenticité qui est généralement une signature numérique.

autorité sur l'identité légale des personnes et permettent ainsi à l'IDC-ID d'atteindre des niveaux d'assurance plus élevés. Les États membres de l'UA sont ainsi encouragés à renforcer leurs systèmes d'identification, ainsi que les principes d'identification pour le développement durable. Des solutions alternatives pour obtenir un IDC-ID pour les personnes qui sont actuellement exclues d'un système d'identification peuvent être envisagées.

Les normes relatives à une identité numérique légale interopérable pourraient être utilisées au niveau national ou soutenir des cas d'utilisation transfrontaliers. Par exemple, la norme pourrait être adoptée pour :

- Représenter les données d'identité numérique fondamentale au niveau national sur les justificatifs d'identité numérique nouvellement émises ou mises à jour ; ou,

- Représenter les données d'identité numérique fondamentale au niveau continental ou de la CER ;

- Être émise séparément en complément des systèmes d'identification numérique fondamentaux préexistants.

Les éléments d'interopérabilité, de confiance et d'inclusion définis dans ce cadre constituent une rampe de lancement pour un cadre continental plus complet et une infrastructure pour l'identification et l'authentification numériques sur le continent.

3.1. **Principes directeurs**

Les principes suivants guident la mise en œuvre de l'interopérabilité transfrontalière du cadre :

1. Transparence de la gouvernance et du fonctionnement.

2. Facilement accessible, rentable, financièrement et opérationnellement durable et largement utilisable.

3. Promotion du respect et la défense des droits de l'homme et de la liberté[29].

4. Assurance de l'intégrité technique, y compris une identité unique, sûre, évolutive et précise.

5. Garantie de la souveraineté des États membres et assurance que la souveraineté des données, notamment les données d'identité numérique, appartient à l'Afrique et reste sous son contrôle.

[29] Conformément à la Charte africaine (Banjul) des droits de l'homme et des peuples (adoptée le 27 juin 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entrée en vigueur le 21 octobre 1986)

6. Interopérabilité entre les États membres de l'UA.

7. Utilisation de normes ouvertes[30] et prévention du verrouillage des fournisseurs et des technologies.

8. Protection de la vie privée des données numériques et possibilité pour les personnes de contrôler leurs données personnelles, y compris la proportionnalité des données par la conception du système.

9. Protection de la confidentialité des données, de la sécurité et des droits grâce à un cadre juridique et réglementaire complet.

10. Définition de mandats et de responsabilités institutionnels clairs

Compte tenu du fait que le Cadre dépend de sources faisant autorité, comme les systèmes d'identification légaux, la qualité et la couverture de ces systèmes ont un impact sur sa mise en œuvre. L'exclusion de ces systèmes et d'autres défis tels que la faiblesse de la sécurité, par exemple, se traduiront par la même situation en termes de capacité à délivrer et à utiliser correctement les justificatifs d'identification.

Les États membres de l'UA doivent en conséquence s'acquitter de leur obligation de veiller à ce que toutes les personnes présentes sur leur territoire aient accès à une identification légale, conformément à la Convention relative aux droits de l'enfant et aux autres instruments juridiques internationaux et régionaux. En outre, ils sont également fortement encouragés à adhérer aux normes[31] et principes[32] internationaux pertinents existants et à veiller à ce que les sources d'autorité, et en particulier leurs systèmes d'identification légale, soient inclusifs, protègent les données et les droits des personnes, et soient conçus pour soutenir l'intégration économique et sociétale du continent.

3.2. **Modèle de mise en œuvre**

Le Cadre proposera une mise en œuvre en trois phases :

1. Adoption du Cadre de l'UA et soutien au cadre législatif favorable ;

---

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

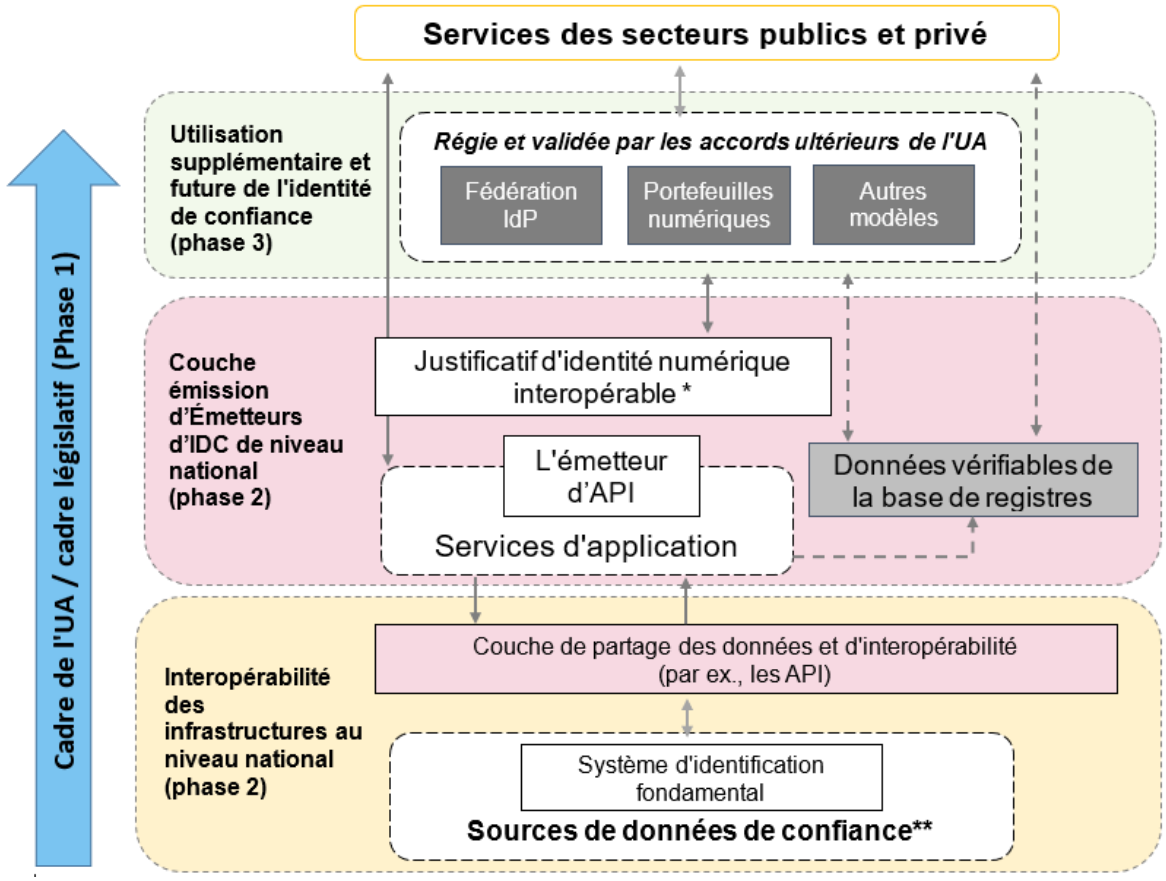
[31] Il s'agit notamment de la convention de Budapest sur la cybercriminalité, des principes et recommandations de la CEI, de l'ISO et de l'UIT-T pour les systèmes de statistiques de l'état civil, des normes internationales sur la protection des données (telles que le règlement général européen sur la protection des données et la convention 108+ du Conseil de l'Europe), des normes mondiales et régionales et des cadres de confiance pour l'identification.

[32] Par exemple, les dix principes d'identification pour le développement durable, qui ont été approuvés par 30 organisations internationales et régionales, dont des institutions africaines telles que la CEA, la BAD et Smart Africa, et adoptés par un certain nombre de pays africains (voir https://id4d.worldbank.org/principles), et les principes du développement numérique, qui ont été approuvés par plus de 200 organisations (voir https://digitalprinciples.org/).

2. Mise en œuvre du Cadre et adoption de spécifications techniques pour l'IDC-ID ;

3. La mise à l'échelle de la mise en œuvre du Cadre et fournit une infrastructure permettant des cas d'utilisation plus avancés tels que l'authentification à distance.

Figure 1 – Approche de la mise en œuvre du cadre par étapes



L'IDC-ID garantit que **l'autorité émettrice ne sait pas à quels services les individus accèdent avec leur ID** numérique, mais l'authenticité des justificatifs d'identité peut être vérifiée. Cela offre des garanties en termes de protection des données et de la vie privée et permet à l'individu de mieux contrôler l'utilisation de ses données.

* *Les détails de la mise en œuvre de la phase 2 seront discutés plus avant avec les États membres de l'UA.*

** *Les États membres décideront de ce que les sources de données fiables impliquent dans leurs systèmes d'identification fondamentaux.*

La couche infrastructure permettra des cas d'utilisation plus avancés et consistera à lier les justificatifs d'identité émises dans le format IDC-ID aux personnes réelles. Plusieurs

options techniques sont à la disposition des États membres de l'UA pour mettre en œuvre cette couche, qui pourrait être composée d'une fédération de fournisseurs d'identité offrant des mécanismes d'authentification aux détenteurs de l'IDC-ID ou le développement de solutions de portefeuilles d'identité numérique ou tout autre modèle permettant l'interopérabilité. Chacune de ces mises en œuvre peut offrir **une approche de minimisation des données et des services de divulgation sélective** pour des cas d'utilisation spécifiques, par exemple ne partager que les points de données pertinents d'une carte d'identité et d'un dossier de crédit pour obtenir un prêt, demander des prestations sociales ou de santé, obtenir une pension, demander des bourses d'études ou anonymiser l'ensemble de données minimum de l'IDC-ID (nom, date de naissance) en une preuve de majorité (+18 ans ou +21 ans ou une réponse oui/non).

3.2.1. **Composants de l'architecture**

Les sources de données fiables doivent répondre aux normes fixées par le cadre de l'UA en matière de qualité et d'intégrité des données. Dans de nombreux cas, ces normes seront remplies par un système d'identification fondamental (dont les sources de données fiables seront décidées par les États membres) qui peut fournir une preuve d'identité légale.

La figure 1 illustre l'extension de l'accès aux systèmes nationaux existants et aux sources de données fiables par le biais d'une couche de partage de données et d'interopérabilité fondée sur des normes et des protocoles permettant la délivrance d'IDC fiables. Les fournisseurs de services vérifient et récupèrent les données d'identité légale lors de la création justificatifs d'identité numérique fondamentale.

La couche d'émission d'IDC représente l'émission normalisée d'un justificatif d'identification basée sur une source de données fiable d'un système d'identification fondamental/national. Chaque émetteur de documents d'identité (au moins un par État membre participant) aura un certain nombre de fonctions clés (non limitées aux suivantes) :

- Une API de l'émetteur qui permet aux portefeuilles et autres systèmes de demander et de récupérer des justificatifs d'identification.

- Un registre de données vérifiables qui permet de vérifier les identifiants et de contrôler la révocation des justificatifs d'identification.

- Gestion des clés cryptographiques.

- Visibilité et vérifiabilité des justificatifs utilisées pour le détenteur d'IDC.

- Fourniture de métadonnées de justificatifs d'identification à côté de chaque IDC émis pour décrire la qualité, la provenance et le niveau de confiance associés à l'IDC émis.

3.2.2. Niveau national et exigences d'interopérabilité

Il n'est pas nécessaire de remanier les systèmes d'identité existants au niveau national pour réaliser l'interopérabilité au niveau continental. En revanche, des normes pour l'interopérabilité des données, l'interopérabilité technique via des API et des protocoles, et la représentation technique des justificatifs d'identification seront adoptées. La délivrance de ces identifications et leur création sont logiquement séparées des systèmes nationaux existants, mais seraient sous le contrôle d'agences nationales responsables.

La confiance technique, étayée par une cryptographie avancée, peut ne pas nécessiter une infrastructure à clé publique (ICP) continentale ou une autre infrastructure supranationale, mais résulterait plutôt de la préférence et/ou de la capacité des États membres de l'UA à utiliser une ICP nationale (le cas échéant) ou des alternatives légalement reconnues. Chaque État membre de l'UA continuera à exercer sa souveraineté nationale dans la conception des systèmes d'identité nationaux, y compris la manière dont ces systèmes interagissent avec le Cadre de l'UA.

3.2.3. Normes pour une participation des sources de données fiables

Des normes seront établies selon le Cadre de l'UA pour la qualité, la sécurité, la fiabilité et le niveau minimum d'assurance associé à chaque source de données fiable. Les systèmes des États membres devront fournir la preuve qu'ils ont atteint les exigences minimales de participation avant de pouvoir participer au Cadre de l'UA et de délivrer des justificatifs d'identification conformes à l'IDC. La nature de ces normes sera déterminée par un accord entre les États membres de l'UA.

3.3. Processus éprouvé- le Cadre de confiance

Le Cadre de confiance doit décrire des règles claires pour la participation des entités (par ex., les émetteurs, les détenteurs et les vérificateurs d'identité), le fonctionnement du cadre et les exigences techniques pour l'interopérabilité des informations d'identification fiables.

Toutes les entités pourront ainsi faire confiance aux informations d'identification partagées par les détenteurs d'identité sur la base de la confiance établie par l'autorité émettrice (pour l'information d'identification) et des processus que chaque entité a accepté de respecter dans le cadre de confiance.

Il est prévu que les sections clés suivantes soient rédigées par les États membres en tant que partie intégrante du cadre de confiance.

3.3.1. Rôles et responsabilités

Une définition claire de chaque entité (par ex., un émetteur de justificatifs d'identification), et des responsabilités qui lui incombent pour que la confiance soit maintenue, comme la gestion sûre et sécurisée des données et des services, et la notification des incidents.

Les rôles clés qui devraient être inclus dans le cadre de confiance seraient les suivants :

- **Les autorités de confiance** sont des sources de données faisant autorité en matière de preuve d'identité légale, approuvées par les États membres de l'UA.

- **Les émetteurs** sont des entités chargées de délivrer au titulaire la preuve d'identité légale dans le format numérique standardisé conformément au Cadre. Les autorités de confiance peuvent soit délivrer elles-mêmes les justificatifs d'identification, soit mandater une autre entité disposant de compétences plus adéquates (par ex., une agence TIC, le secteur privé).

- **Le détenteur** de l'IDC-ID est la personne qui possède une ou plusieurs justificatifs d'identification numériques. Le détenteur peut être, mais pas toujours, le sujet des attributs d'identité partagés via l'IDC.

- **Le vérificateur** est une partie intéressée (par ex., un fournisseur de services public ou privé) qui souhaite vérifier la déclaration d'identité d'un sujet donné.

- **Les fournisseurs d'identité, les fournisseurs de justificatifs d'identification et les fournisseurs de portefeuilles numériques** peuvent contribuer davantage à l'écosystème en fournissant un authentificateur pour lier l'identité du titulaire aux justificatifs d'identification et permettre ainsi des cas d'utilisation plus avancés nécessitant une authentification à distance.

- **Un organe de surveillance indépendant**, à mettre en place par les États membres, est susceptible d'être nécessaire pour garantir que les entités participantes respectent les règles établies par le cadre de confiance et définissent les outils et technologies minimaux nécessaires à la conformité. L'organe de surveillance devrait également être chargé de sensibiliser le continent aux compétences en matière de cyber-résilience afin de garantir la durabilité du cadre.

3.3.2. **Règles de participation**

Les règles de participation peuvent inclure des exigences légales, opérationnelles ou organisationnelles minimales requises pour une entité de confiance faisant autorité et fournissant un service dans le cadre de confiance. Par exemple, un émetteur peut être tenu d'avoir un accord officiel pour fonctionner (d'une source autorisée / agence gouvernementale).

Les services acceptant l'IDC-ID peuvent être invités à confirmer leur conformité aux exigences de base en matière de protection des données, de respect de la vie privée et de recours (pour les détenteurs d'identité).

Un protocole d'accord peut également être exigé pour garantir que toutes les entités opérationnelles acceptent les conditions du cadre de confiance.

3.3.3. **Gouvernance**

Des mécanismes de gouvernance, à approuver par les États membres de l'UA, seront nécessaires pour établir et maintenir les règles du cadre de confiance, approuver les modifications des exigences d'interopérabilité et déléguer la responsabilité de la conception et de l'élaboration des modifications du cadre à des sous-groupes de gouvernance, le cas échéant.

Un organe de surveillance indépendant, à établir par les États membres de l'UA, est susceptible d'être nécessaire pour garantir que les entités participantes restent conformes aux règles établies par le cadre de confiance. Cet organisme devrait également être chargé de veiller à ce que toutes les parties respectent formellement les normes et, en cas d'écart, fassent l'objet d'un audit ou soient amenées à rendre des comptes si nécessaire, par exemple en cas de violation de données.

La protection des personnes devrait être primordiale. L'organe de surveillance devrait être habilité à recevoir et à traiter les plaintes des titulaires d'IDC-ID victimes de mauvaises pratiques, de violations de données, d'usurpation d'identité ou d'autres incidents liés à l'identité numérique. Il devrait également être le point de convergence des mécanismes de recours, même s'il ne s'agit que d'un rôle de coordination, et devrait se faire le défenseur des individus et de leurs droits.

3.3.4. **Exigences d'interopérabilité**

3.3.4.1. **Niveau d'assurance**

Un moyen de communiquer le niveau de confiance accordé à un justificatif d'identification présenté par un titulaire à un vérificateur. Le Cadre doit définir les conditions dans lesquelles chaque niveau de confiance peut être atteint en fonction de la vérification de l'identité par une source faisant autorité, du processus de délivrance, et des moyens de détenir et de présenter un justificatif d'identification.

3.3.4.2. **Ensemble minimal de données**

La quantité minimale de données concernant l'identité d'un titulaire, telle qu'elle est fournie dans un justificatif d'identité, doit être suffisante pour permettre l'identification de la personne dans la majorité des transactions courantes, tout en respectant la nécessité

de minimiser les données. Les attributs contenus dans l'ensemble minimal de données peuvent être fournis par différentes entités de confiance.

L'organe directeur est libre de définir la manière dont des renseignements supplémentaires (ensembles de données) peuvent être incluses de manière facultative dans le cadre de confiance. Toute délivrance des justificatifs d'identification correspondantes doit être soumise aux mêmes conditions et règles que les émetteurs des justificatifs d'identité fondamentaux et ses exigences techniques.

3.3.5. Exigences techniques

3.3.5.1. Sécurité

Des exigences de sécurité de base doivent être définies pour chaque entité fournissant un service dans le cadre de l'infrastructure d'identité.

3.3.5.2. Preuve cryptographique

Les justificatifs d'identité seront vérifiés par l'inclusion d'une signature numérique créée par l'autorité émettrice. La vérification de la validité de la signature constitue une preuve cryptographique de la crédibilité de la déclaration faite par le titulaire du justificatif d'identification. Pour vérifier une signature numérique, une clé publique est nécessaire. La clé publique peut être fournie par une méthode décentralisée ou centralisée à déterminer dans le cadre de la confiance et de ses exigences techniques.

3.3.5.3. Format des justificatifs d'identité

Les spécifications techniques pour la création et la transmission des justificatifs d'identité doivent être définies en s'inspirant des normes existantes telles que les « Verifiable Credentials » (justificatifs vérifiables) du W3C, le cas échéant.

- Le justificatif numérique interopérable d'identité (IDC-ID) est un ensemble de renseignements d'identité légales (par ex., des attributs) et de relations faites par un émetteur qui peuvent être vérifiées de manière cryptographique. Il comprend plus particulièrement :
    - Des métadonnées de justificatif concernant le type de justificatif délivré, la date de délivrance, le nom de l'émetteur ;
    - Des informations sur le sujet du justificatif et le justificatif d'identité légal réel (par ex., la date de naissance) ;
    - Une preuve d'authenticité qui est généralement une signature numérique.

Le détenteur de l'IDC-ID est capable de générer des présentations vérifiables d'un ou plusieurs IDC-ID de manière à ce que l'authenticité du justificatif puisse toujours être vérifiée (par ex., une divulgation sélective).

3.4. Options d'authentification potentielles

Plusieurs approches architecturales peuvent être adoptées pour permettre au détenteur de l'IDC-ID d'être authentifié à un niveau d'assurance donné. Toutes les options suivantes peuvent coexister et être mises en œuvre à différents niveaux de coopération (par ex., entre des acteurs sectoriels spécifiques ou au niveau des CER).

En fonction de la disponibilité d'autres technologies dont les pratiques de mise en œuvre ont fait leurs preuves, d'autres options pourront être explorées.

3.4.1. Portefeuilles numériques personnels

Cette option consiste à fournir aux particuliers et aux entreprises un portefeuille numérique personnel contenant des attributs de preuve vérifiable d'identité légale qui peuvent être utilisés pour prouver l'identité d'une personne ou partager des faits spécifiques avec un fournisseur de services. Cette option d'architecture fait référence aux cas d'utilisation des Verifiable Credentials (justificatifs vérifiables) du W3C[33].

Figure 2 – Vue de l'option 1 - Portefeuilles numériques personnels

Processus d´authentification

1. La personne choisit **un fournisseur de portefeuille d'identité** pour stocker son IDC et un processus d'intégration est nécessaire.

[33] W3C, Verifiable Credentials Use cases, voir : https://www.w3.org/TR/vc-use-cases/.

2. La personne reçoit un identifiant vérifiable (par ex., ID, une preuve d'adresse) de la part des émetteurs faisant autorité et le stocke dans **un portefeuille numérique**.

3. En même temps que l'émission, la source émettrice enregistre une empreinte numérique du justificatif dans **une infrastructure à clé publique décentralisée en tenant compte de la vie privée des citoyens.**

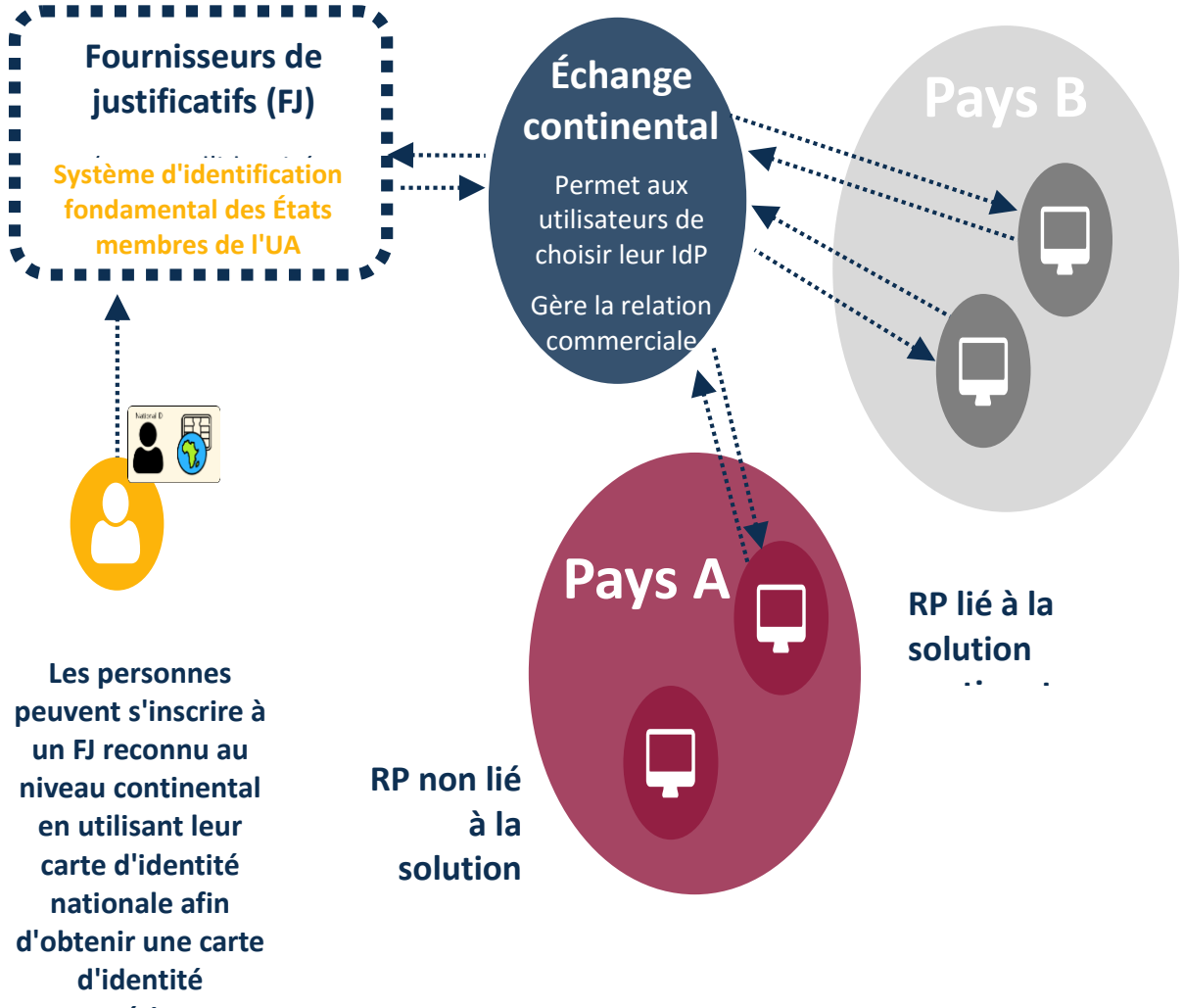
4. Les individus peuvent présenter à un fournisseur de services (par ex. une assurance) un justificatif de domicile en utilisant leur portefeuille (par code QR, Bluetooth, NFC).

5. Le fournisseur de services peut **vérifier** dans l'infrastructure à clé publique décentralisée que le justificatif est authentique et a été émis par une source reconnue.

3.4.2. **Option 2 - Fédération continentale d'identités numériques**

Dans le cadre de ce modèle, chaque résident africain pourrait s'inscrire auprès d'un fournisseur de justificatifs d'identité de niveau continental de son choix.

Figure 3 – Vue de l'option 2 - Fédération continentale d'identités numériques



*Les États membres décideront quelles sources de données fiables impliquent dans leurs systèmes d'identification fondamentaux.

Processus d´authentification

1. **Une fédération continentale de fournisseurs de justificatifs (FJ) d'identité est établie** : opérateurs de télécommunications, banques, gouvernements, etc… peuvent fournir des services d'authentification.

2. **Un échange continental** est créé, fournissant un point de contact unique pour tous les fournisseurs de justificatifs participants et les parties intéressée qui veulent authentifier des personnes.

3. Les personnes peuvent utiliser leur IDC délivré par une source faisant autorité (par ex., un système d'identification légal) pour **s'inscrire** auprès du fournisseur de justificatifs de leur choix. Le FJ peut vérifier l'authenticité de l'IDC.

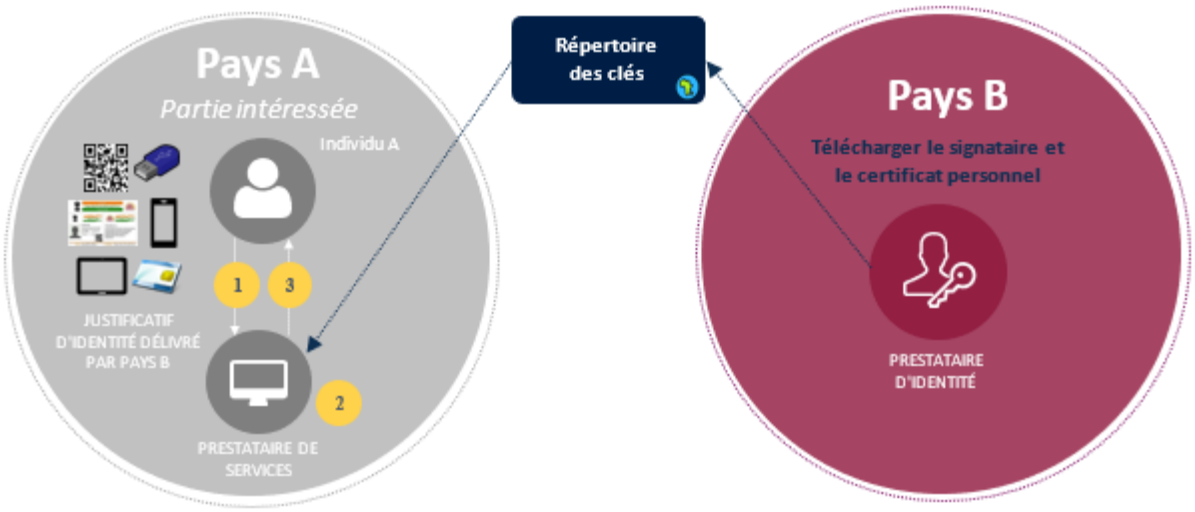
4. Si la vérification est réussie, le FJ délivre **un moyen d'authentification** au particulier.

5. La personne peut utiliser son moyen d'authentification pour **accéder aux services en ligne et en personne** qui sont connectés à l'échange continental.

3.4.3. **Option 3 - Justificatifs d'identité à signature numérique**

Ce modèle permet l'authentification en vérifiant les données d'identité légale signées numériquement sur un justificatif d'identité avec une clé publique, ainsi qu'un moyen supplémentaire de partager la photo du titulaire.

Figure 4 – Vue de l'option 3 - Justificatifs d'identité à signature numérique



Processus d´authentification

1. Les pays se mettent d'accord sur **une norme (par ex., un code QR)** et les sources émettrices signent de manière cryptographique les justificatifs (via une clé privée).

2. Les sources autorisées partagent leur clé publique dans **un répertoire de clés publiques** (RCP) dont la gouvernance sera approuvée par les États membres de l'UA et gérée au niveau continental.

3. Les pays créent un service distinct permettant de partager une copie de la photo du titulaire de l'IDC-ID accessible via une API sécurisée afin d'authentifier le titulaire. Pour travailler hors ligne, il est également possible pour un groupe de pays (par ex., les CER) de se mettre d'accord sur l'émission d'un justificatif physique contenant une photo du titulaire[34].

4. Les sources autorisées des pays délivrent **des formes normalisées** d'IDC aux personnes.

5. **Un logiciel de vérification** (application ou site web) est créé pour permettre aux fournisseurs de services de vérifier l'authenticité et l'intégrité de la signature sur l'IDC.

6. Les personnes peuvent utiliser leur IDC pour faire vérifier numériquement leur identité légale par des parties intéressées publiques ou privées dans leur pays ou à l'étranger et **accéder à des services**.

7. Chaque État membre sera tenu de conserver dans un espace de stockage

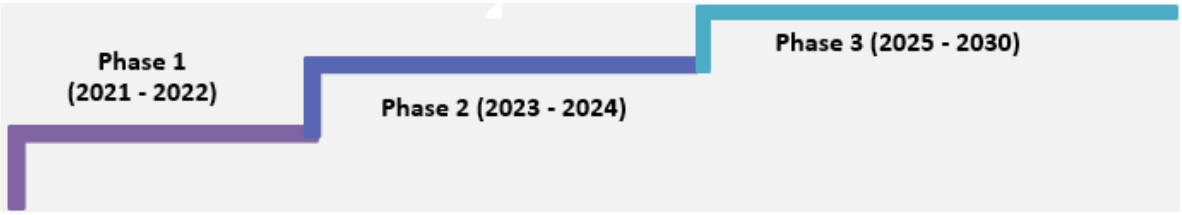
[34] La délivrance de justificatifs physiques a un coût supplémentaire. Les États membres participants devront discuter plus avant du financement de cette solution afin de ne pas créer d'obstacles à l'accès.

sécurisé, tel qu'un module matériel de sécurité (HSM), les clés privées, les certificats personnels et les algorithmes de hachage à utiliser pour le cryptage et la vérification de l'intégrité.

FEUILLE DE ROUTE DETAILLEE POUR LA MISE EN ŒUVRE

Pour accélérer la voie vers la réalisation des objectifs ambitieux de ce Cadre, les États membres de l'UA doivent intensifier leur collaboration pour affiner les détails du cadre technique et de référence, des normes et du processus communs.

La proposition consiste à diviser la mise en œuvre du Cadre en trois phases, comme le montre le schéma ci-dessous :



1. Adoption du Cadre et soutien au cadre législatif d'habilitation ;

2. Mise en œuvre du cadre et adoption de spécifications techniques pour l'IDC-ID ;

3. Mise à l'échelle du cadre pour fournir une infrastructure permettant des cas d'utilisation plus avancés tels que l'authentification à distance.

Pour chaque phase, des possibilités de consultation des États membres de l'UA, de la société civile et des parties prenantes de l'écosystème de l'identité seront prévues afin de garantir que le Cadre et sa mise en œuvre restent alignés sur les besoins des personnes et des contextes locaux. La documentation clé sera publiée et offrira une fenêtre de temps adéquate pour les contributions.

4.1. Phase 1 : Adoption du Cadre et environnement favorable

Présentation du projet de Cadre à la 4ème session ordinaire du CTS sur la Communication et les TIC pour adoption et entérinement par les organes délibérants.

Après l'approbation du présent document, les détails du cadre de confiance seront précisés, et les activités suivantes seront menées notamment :

- Sensibilisation ;

- Étude de faisabilité sur le paysage actuel du système d'identification numérique en Afrique ;

- Mise en place d'un cadre de consultation des acteurs de l'écosystème numérique visant à préserver l'intérêt de chaque acteur ;

- Mise en place d'instruments juridiques et réglementaires harmonisés.

- Définition des règles de participation.

- Mise en place des mécanismes de gouvernance et d'un forum pour partager les meilleures pratiques tout au long du processus de mise en œuvre ;

- Les dispositions juridiques qui devront être intégrées dans les environnements juridiques nationaux des États membres de l'UA afin de mettre en œuvre le Cadre, y compris les garanties appropriées en matière de cybersécurité et ainsi que la ratification de la Convention de Malabo sur la cybersécurité et la protection des données à caractère personnel ;L'adoption du cadre politique continental sur les données.

- La nomination de groupes d'experts par les États membres de l'UA pour définir l'interopérabilité et les exigences techniques.

- La mise en place de structures institutionnelles indépendantes au niveau national (autorités chargées de la protection des données, autorités de certification du contrôleur et équipes de réponse aux incidents informatiques(CIRT) ;

- Mettre en place des initiatives de renforcement des capacités ;.

- soutenir la mise en place d'une infrastructure numérique, y compris des centres de données aux niveaux national, régional et continental, nécessaire pour soutenir et maintenir l'opérationnalisation des systèmes d'identification numérique ; Mobilisation des ressources.

Afin d'assurer le succès du Cadre, une série de cas d'utilisation représentant les plus grandes opportunités pour le continent sera définie. Un groupe d'États membres de l'UA pourra ensuite collaborer pour tester et piloter des cas d'utilisation spécifiques, avec d'autres parties prenantes si nécessaire.

Une évaluation des principaux coûts et avantages du cadre proposé et des options d'authentification ultérieures devrait être réalisée afin de fournir une plus grande visibilité sur les besoins de financement pour éclairer la prise de décision des États membres de l'UA. En ce moment, on s'attend à ce que la conformité à une norme harmonisée pour représenter les informations d'identité engendre des coûts limités pour les États membres de l'UA, car elle pourrait être intégrée comme une exigence technique aux projets de numérisation existants de leurs systèmes d'identification fondamentaux. En revanche, la mise en place de l'infrastructure d'authentification devrait générer des coûts

supplémentaires et, selon les types de parties prenantes concernées, elle nécessite la définition de modèles économiques. Concernant cette phase, une analyse d'impact détaillée devra être réalisée afin de s'assurer que les options d'authentification proposées restent inclusives.

Les États membres de l'UA s'engagent également à :

- Élaborer et mettre en œuvre des cadres juridiques et réglementaires harmonisés qui renforcent la confiance dans les systèmes d'identification numérique fondamentaux ;Élaborer une législation et une réglementation harmonisées en matière de données personnelles qui renforcent les capacités des individus, tout en préservant la souveraineté des données ;

- Mettre en place l'infrastructure numérique, y compris l'infrastructure de données (centres de données nationaux), qui constitue la base de la mise en œuvre du système d'identification numérique.

- De ratifier la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel (si cela n'a pas encore été fait), d'accélérer son entrée en vigueur et de travailler à l'accélération de la mise en place d'autorités de protection des données chargées de la surveillance dans les pays participants ;Élaboration de la stratégie nationale de cybersécurité et mise en place d'équipes de réponse aux incidents informatiques (CIRT) afin d'atténuer les risques et les menaces liés aux cyberattaques, au vol de données et à la mauvaise manipulation d'informations sensibles ;

- Adopter le cadre de la politique continentale de l'UA en matière de données : qui demande que les systèmes d'identification numérique soient élaborés et mis en œuvre de manière cohérente, conformément à un cadre général de gouvernance des données garantissant que la combinaison et la réutilisation des données administratives publiques qu'impliquent les systèmes d'identification numérique s'effectuent avec des garanties appropriées. Ces politiques devraient donner aux individus les moyens d'agir et protéger la vie privée en ligne en tant que droit fondamental (y compris le choix et le contrôle de l'utilisateur, le consentement éclairé/manifeste, la souveraineté/la propriété des données, etc. ;)

- Lancer et/ou intensifier les efforts visant à renforcer les systèmes d'identification fondamentaux, afin de s'assurer qu'ils sont inclusifs et fiables, conformément aux normes et initiatives pertinentes telles que le Programme africain pour amélioration accélérée des systèmes d'enregistrement des faits d'état civil et des statistiques de l'état civil (APAI-CRVS) et *les principes d'identification pour le développement durable.*

Ces phases seront finalisées avec l'adoption de la version complète du Cadre par les États membres de l'UA.

4.2. Phase 2 : Mise en œuvre du Cadre et adoption des spécifications techniques de l'IDC-ID

La deuxième phase consistera à établir le cadre de confiance et les mécanismes de gouvernance et de coopération et à fournir **la spécification technique** pour la mise en place de l'IDC-ID qui inclura entre autres :

- Élaborer des normes et des règles minimales pour l'interopérabilité ;
- Profils d'attribution pour l'ensemble minimal de données (formats de données) et les métadonnées associées ;
- Présentation du format (par ex. codes à barres 2d, justificatifs vérifiables W3C)
- Niveau d'assurance (comme point de référence pour l'interopérabilité)
- Éléments de cryptographie pour la signature et le cryptage des données
- Protocoles de vérification pour les cas d'utilisation en ligne et hors ligne

Un exemple de mise en œuvre (application ou site web) pour la vérification de base de l'IDC-ID sera conçu par un groupe d'États membres de l'UA afin de tester l'interopérabilité des justificatifs d'identité et de prendre déjà en charge les preuves vérifiables de l'identité légale. La mise en œuvre permettra de garantir la confidentialité et la sécurité dès la conception.

Un accord sur la définition de **solutions alternatives pour obtenir un IDC-ID** pour les personnes qui sont actuellement exclues de tout système d'identification fondamental sera envisagé.

Une cartographie des autres initiatives de l'Union africaine en cours qui pourraient s'appuyer sur le cadre sera réalisée (par ex., le cadre continental africain des qualifications).

La phase 2 sera conclue par la mise en place d'un plan d'action clair pour la définition de l'infrastructure d'authentification dans le cadre de la phase 3.

4.3. Phase 3 : Développement de l'infrastructure pour permettre l'authentification à distance

La Phase 3 commencera à mettre en œuvre le cadre de confiance défini en phase 2.

La couche qui représente la délivrance de l'IDC-ID, pourra être achevée dans une deuxième phase par une infrastructure permettant des cas d'utilisation plus avancés tels

que l'authentification à distance. Cette couche d'authentification permettra aux individus de prouver leur identité numériquement en exerçant le contrôle d'un ou plusieurs facteurs d'authentification (par ex., un code biométrique ou PIN) liés à leur identité légale préalablement vérifiée, à savoir l'IDC-ID. Plusieurs options techniques sont à la disposition des États membres de l'UA pour mettre en œuvre cette couche, par exemple : la mise en place d'une fédération de fournisseurs d'identité fournissant des mécanismes d'authentification aux détenteurs de l'IDC-ID, ou le développement de solutions de portefeuille d'identité numérique ou tout autre modèle permettant l'interopérabilité. Chacune de ces mises en œuvre peut offrir une approche de minimisation des données et des services de divulgation sélective pour des cas d'utilisation spécifiques, tels que le partage des points de données pertinents d'une carte d'identité et d'un dossier de crédit pour l'obtention d'un prêt, la demande de prestations sociales ou de santé, l'obtention d'une pension, lorsque l'authentification est légalement requise ou l'anonymisation de l'ensemble minimal de données de l'IDC-ID (par ex., le nom, la date de naissance) dans une preuve de majorité (+18 ans ou +21 ans ou une réponse oui/non).

Les États membres de l'Union africaine pourront également trouver un accord supplémentaire sur la manière d'établir cette infrastructure de couche d'authentification et s'associer aux CER et à d'autres initiatives continentales qui étudient déjà la mise en place de solutions interopérables d'identification numérique pour accéder à des services à distance. En effet, les États membres et les organisations seront en mesure de tirer parti de la représentation commune, basée sur des normes, des informations relatives à l'identité dans un format numérique fiable et sécurisé et de créer des services supplémentaires sur cette base.

Les États membres de l'UA poursuivront leur collaboration pour renforcer le cadre de confiance et les mécanismes de gouvernance et de coopération faisant suite à l'accord sur les infrastructures supplémentaires, de la manière suivante :

- **Coordination avec d'autres initiatives** visant à établir l'interopérabilité au niveau continental (par ex., SATA et les CER).

- **Accord sur la meilleure option architecturale** (par ex. fédération, portefeuilles numériques, etc.) pour développer la fonction d'authentification à distance qui s'appuierait sur les justificatifs numériques interopérables (IDC-ID).

La phase 3 sera conclue par un plan d'action clair sur la mise en œuvre de la couche d'authentification selon l'option architecturale à convenir entre les États membres de l'UA et les institutions.

HYPOTHESES, DEFIS ET RISQUES MAJEURS

5.1. Hypothèses

Les États membres adopteront le cadre, collaboreront, s'engageront à mettre en œuvre et à prendre les réformes juridiques et réglementaires nécessaires et requises.

5.2. Défis généraux et mesures d'atténuation importantes proposées

Le tableau ci-dessous décrit les défis généraux et les mécanismes d'atténuation proposés.

5.3. Risques et mesures d'atténuation proposées

Le tableau ci-dessous décrit les risques et les mécanismes d'atténuation proposés.

#	Défis	Atténuations proposées
1.	Exclusion, faiblesse de la sécurité et érosion de la protection des données personnelles	Appliquer les principes définis dans le cadre (3.1) et renforcer les cadres juridiques et les infrastructures de sécurité et de protection des données dans les États membres de l'UA.
2	Réticence des États membres de l'UA à adopter et à mettre en œuvre le cadre.	Sensibiliser aux avantages du cadre d'interopérabilité aux niveaux national et continental et renforcer le système d'identification fondamental.
3	Manque de capacités techniques et financières des États membres de l'UA	Renforcer les capacités et promouvoir les échanges de connaissances entre pairs parmi les États membres de l'UA, et examiner la rentabilité des solutions technologiques à convenir dans le cadre des phases 2 et 3.
4	Centres de données inadéquats aux niveaux national/régional/continental	Construire des centres de données nationaux/régionaux/continentaux et promouvoir leur utilisation en Afrique.

#	Risques	Atténuations proposées
1	Absence de définition correcte de la norme commune, manque de compréhension de la part des États membres de l'UA et incapacité à suivre et à adopter les normes communes.	Définition de normes et communication de celles-ci aux États membres de l'UA pendant la mise en œuvre et suivi régulier par un organisme panafricain fiable et habilité, soutenu et approuvé par tous les États membres de l'UA pour garantir le respect des normes. Discussions et ateliers ciblés avec les parties prenantes pour garantir une définition claire des normes pour la stratégie de mise en œuvre choisie.
2	Les faibles niveaux de confiance entre les autorités nationales, dont les capacités de mise en œuvre sont hétérogènes, entraînent une lente adoption du cadre à l'échelle continentale. En	Comparaison de la stratégie de mise en œuvre standardisée de l'État membre de l'UA avec des programmes nationaux d'identification fondamentaux similaires dans les États membres de l'UA. Le cadre devrait viser l'harmonisation et la reconnaissance mutuelle comme objectif à long terme, mais rester ouvert à l'élaboration de solutions souples et agiles, qui pourraient créer des mécanismes d'audit partagés entre les pays désireux

	outre, la réticence des États membres à accepter un organe de surveillance supranational ralentit la mise en œuvre du cadre de confiance.	d'établir la confiance entre eux tout en restant souverains - par la reconnaissance unilatérale des certificats de confiance émis.
3	La solution, les avantages et les options ne sont pas bien adaptés à l'environnement local ou l'information est mal diffusée et les personnes n'utilisent pas la solution, ce qui entraîne une faible adoption et, en fin de compte, des coûts élevés avec peu d'avantages.	Développer de solides structures de conception centrées sur l'utilisateur afin d'identifier des solutions faciles à utiliser et accessibles à tous ; Développer de solides mécanismes de diffusion dans les États membres de l'UA, qui intègrent tous les acteurs locaux partageant les mêmes idées.
4	Les États membres décideront de la technologie appropriée pendant la phase de mise en œuvre, mais s'ils optent pour la technologie ICP, absence d'institution de certification au niveau continental et manque de gouvernance adéquate des exigences cryptographiques pour la signature numérique qui s'avère être un obstacle à la mise en place du système d'interopérabilité.	Création d'un cadre juridique permettant l'établissement d'une institution de coordination au niveau continental, soutenue par une structure de gouvernance équitable tenant compte de la souveraineté de chaque État membre pour la mise en œuvre et la gestion des signatures numériques, leur émission, leur révocation, leur remplacement et leur mise à jour en temps voulu. Création d'une structure organisationnelle détaillée et dynamique pour permettre la gouvernance de l'infrastructure de signature numérique / ICP tout au long de la phase de mise en œuvre et d'opérationnelle
5	En raison de données incorrectes et incomplètes, la conception et la stratégie de mise en œuvre de certains composants d'interopérabilité tels que les signatures numériques peuvent être affectées. Un retard dans le partage des données et des informations pertinentes des citoyens ou des résidents pourrait également avoir un impact sur les délais du projet.	Réunions avec les agences gouvernementales pour la collecte de données relatives à la mise en œuvre des lacunes en matière d'information en tirant parti de l'expérience des experts par l'apprentissage entre pairs pour encourager la collaboration et l'appropriation régionale et continentale. Le suivi des délais et des étapes du projet pour éviter les retards. Il est également impératif d'avoir un calendrier de mise en œuvre détaillé et complet qui a été convenu par les États membres de l'UA et les principales parties prenantes.
6	Absence de lignes directrices clairement définies en matière de gestion du changement pour garantir que le cadre reste aligné sur les pratiques, les besoins et le	Mettre en place un processus de gestion du changement solide et bien défini dans le cadre de la gouvernance.

	développement technologique actuels :	
7	Les États membres décideront de la technologie appropriée pendant la phase de mise en œuvre, mais s'ils optent pour la technologie ICP, es agences de certification en Afrique peuvent ne pas parvenir à un consensus concernant la gestion de l'ICP au niveau du déploiement à l'échelle du continent. Deuxièmement, il n'y aura pas forcément de consensus sur la mise en place d'un échange de signatures numériques.	Si les États membres de l'UA peuvent soit créer une nouvelle institution de certification pour la gestion de l'ICP au niveau du continent, soit approuver un mécanisme permettant de réunir les agences existantes sur une plateforme commune.
8	L'absence d'un environnement juridique minimum favorable aux niveaux national et régional.	Les États membres de l'UA à accélérer la mise en œuvre des cadres juridiques et réglementaires harmonisés requis.

ANNEXE

6.1. **Définitions pratiques**

Attribut désigne une qualité ou une caractéristique nommée inhérente ou attribuée à quelqu'un ou quelque chose (adapté de NIST 800-63 :2017). Dans les systèmes d'identification, les attributs d'identité courants comprennent le nom, l'âge, le sexe, le lieu de naissance, l'adresse, les empreintes digitales, la photo, la signature, le numéro d'identité, etc.

Authentification désigne le processus qui permet d'établir la confiance dans le fait qu'une personne est bien celle qu'elle prétend être. L'authentification numérique implique généralement qu'une personne présente électroniquement un ou plusieurs « facteurs » pour « affirmer » son identité, c'est-à-dire pour prouver qu'elle est la même personne que celle à laquelle l'identité ou le justificatif a été initialement délivré. Ces facteurs peuvent inclure un élément que la personne connaît (par ex., un mot de passe ou un code PIN), possède (par ex., une carte d'identité, un jeton ou une carte SIM mobile) ou est (par ex., ses empreintes digitales) (adapté de NIST 800-63 :2017 et OWI 2017).

Autorisation désigne le processus qui consiste à déterminer quelles actions peuvent être réalisées ou quels services peuvent être accédés sur la base de l'identité affirmée et authentifiée (Nyst et al. 2016).

Source faisant autorité : la source faisant autorité en matière d'informations d'identité désigne un référentiel ou un système qui contient des attributs sur un individu et qui est considéré comme la source primaire ou la plus fiable pour ces informations. Dans le cas où deux ou plusieurs systèmes ont des données non concordantes ou contradictoires, les données de la source de données faisant autorité sont considérées comme les plus précises (FICAM, non daté).

Renseignements désigne qualification, réalisation, qualité ou élément d'information sur les antécédents d'un sujet, comme un nom, une pièce d'identité officielle, une adresse personnelle ou un diplôme universitaire. (Adapté du W3C)

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

Justificatif désigne un document, un objet ou une structure de données qui garantit l'identité d'une personne par une méthode de confiance et d'authentification. Les types courants de justificatifs d'identité comprennent, sans s'y limiter, les cartes d'identité, les certificats, les numéros, les mots de passe ou les cartes SIM. Dans le cas de ce cadre, le justificatif est une déclaration vérifiable appelée IDC-ID.

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

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

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

Personnes concernées désignent toute personne physique qui fait l'objet d'un traitement de données à caractère personnel.

Dignité numérique (dans le contexte de l'identification numérique) désigne le fait que l'identité humaine qui se cache derrière l'identification numérique bénéficie d'une certaine confidentialité et que ses données sont protégées.

Système d'identification numérique (ID) désigne un système d'identification qui utilise la technologie numérique tout au long du cycle de vie de l'identité, notamment pour la saisie, la validation, le stockage et le transfert des données, la gestion des justificatifs, ainsi que la vérification et l'authentification de l'identité (adapté du rapport de coopération public-privé ID4D).

Identité numérique désigne un ensemble d'attributs et/ou d'informations d'identification saisis et stockés électroniquement qui identifient une personne de manière unique (adapté de Harbitz & Kentala 2013 et du rapport ID4D Technology Landscape).

Signature numérique désigne une opération à clé asymétrique où la clé privée est utilisée pour signer numériquement les données et la clé publique est utilisée pour vérifier la signature. Les signatures numériques assurent une protection de l'authenticité, de l'intégrité et de la non-répudiation, mais pas de la confidentialité (NIST 800-63 :2017).

Système d'identification fondamental désigne un système d'identification créé principalement pour gérer les informations relatives à l'identité de la population générale et fournir des justificatifs qui servent de preuve d'identité afin d'accéder à des services publics et privés tels que l'éducation, les soins de santé, la protection sociale et les services financiers, etc. (adapté de Gelb & Clark 2013a et de diverses publications ID4D). Aux fins du présent Cadre, les États membres de l'UA décideront quelles sources de données fiables correspondent à leurs systèmes d'identification fondamentaux.

Systèmes d'identification fonctionnels désignent un système d'identification créé pour gérer l'identification, l'authentification et l'autorisation pour un service ou une transaction particulière, comme le vote, l'administration fiscale, les programmes et transferts sociaux, les services financiers, etc. Les justificatifs d'identité fonctionnels - tels que les cartes d'électeur, les dossiers de santé et d'assurance, les numéros d'identification fiscale, les cartes de rationnement, les permis de conduire, etc. - peuvent être communément acceptés comme preuve d'identité à des fins plus larges que leur objectif initial, en particulier lorsqu'il n'existe pas de système d'identification fondamental (adapté de Gelb & Clark 2013a et de diverses publications ID4D).

Harmonisation consiste à assurer l'uniformité des systèmes par l'utilisation de normes minimales pour faciliter l'interopérabilité et de cadres juridiques et de confiance (par ex., pour les niveaux d'assurance) pour fixer des règles et instaurer la confiance dans les systèmes respectifs.

ID désigne un justificatif d'identité ou un document d'identité dans certains domaines.

Système d'identification (ID) désigne les bases de données, les processus, la technologie, l'infrastructure, les justificatifs d'identité et les cadres juridiques associés à la saisie, à la gestion et à l'utilisation des données d'identité personnelles dans un but général ou spécifique (adapté des Principes d'identification).

Identification désigne le processus d'établissement, de détermination ou de reconnaissance de l'identité d'une personne. (Adapté de l'ISO/IEC 24760-1 : 2011 et de l'ITU-T X.1252)

Identité désigne les coordonnées sociales relatives qui distinguent un individu d'un autre. L'identité peut changer en fonction des acteurs ou du cadre dans lequel les individus se trouvent et n'est donc ni fixe ni absolue.

Fournisseur d'identité désigne une entité faisant autorité - par ex., une agence gouvernementale ou une entreprise privée - qui émet et gère les identités légales, les justificatifs d'identité et les processus d'authentification tout au long du cycle de vie de l'identité (document ID4D Public-Private Cooperation).

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

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

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

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

Protection de la vie privée et de la sécurité dès la conception désigne l'intégration proactive de mécanismes de protection de la vie privée et de sécurité dans la conception et le fonctionnement des produits et services, qu'il s'agisse de systèmes informatiques ou non, d'infrastructures en réseau ou de pratiques commerciales. Cela exige que la

gouvernance de la vie privée et de la sécurité soit prise en compte tout au long du processus de conception et du cycle de vie du produit.

Analyse d'impact sur la protection des données (AIPD) désigne un processus conçu pour identifier les risques découlant du traitement des données à caractère personnel et pour minimiser ces risques autant et aussi tôt que possible. Les analyses d'impact sur la protection des données sont des outils importants pour éliminer les risques et pour démontrer la conformité aux lois et règlements sur la protection des données.

Traitement de données à caractère personnel désigne toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou la combinaison et le verrouillage, le cryptage, l'effacement ou la destruction de données à caractère personnel.

Preuve d'identité légale désigne un justificatif, tel qu'un certificat de naissance, une carte d'identité ou un justificatif d'identité numérique, qui est reconnu comme une preuve d'identité légale en vertu du droit national et conformément aux normes et principes internationaux émergents (définition opérationnelle de l'identité légale du groupe d'experts en identité légale des Nations unies).

Partie intéressée (RP) désigne une entité qui s'appuie sur les justificatifs d'identité et les mécanismes d'authentification fournis par un système d'identification, généralement pour traiter une transaction ou accorder l'accès à des informations ou à un système (adapté de NIST 800-63 : 2017).

Cadre de confiance désigne les exigences commerciales, techniques, opérationnelles et juridiques du système d'identité afin de favoriser l'interopérabilité entre les différentes parties participantes.

Présentation vérifiable désigne une présentation inviolable (données dérivées d'un ou de plusieurs justificatifs vérifiables) codée de telle sorte que l'on puisse faire confiance à l'auteur des données après un processus de vérification cryptographique. Par exemple, les approches de divulgation sélective qui synthétisent les données et ne transmettent pas les informations d'identification vérifiables originales (adapté de W3C).

Vérification désigne le processus qui consiste à vérifier des attributs d'identité spécifiques ou à déterminer l'authenticité de justificatifs d'identité afin de faciliter l'autorisation d'un service particulier.

AFRICAN UNION **UNION AFRICAINE**

الاتحاد الأفريقي **UNIÃO AFRICANA**

P. O. Box 3243, Addis Ababa, Ethiopia Tel.: (251-11) 5182402 Fax: (251-11) 5182400
Website: www.au.int

Département de l'Infrastructure et de l'Énergie
Division de la société de l'information

Projet de Cadre stratégique continental en matière des données

Septembre 2021

6.2. **Résumé analytique**

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

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

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

La construction d'une économie des données nationale et régionale favorable nécessitera des niveaux de collaboration sans précédent entre les parties prenantes pour perturber les pressions économiques, politiques et stratégiques déjà ressenties par l'économie mondiale des données. En vue de garantir un accès équitable et sûr aux données pour l'innovation et la concurrence, les États membres devraient établir une approche juridique unifiée, claire et sans ambiguïté, qui offre une protection et des obligations sur tout le continent. Le cas échéant, les instruments et institutions

juridiques existants doivent être réexaminés pour s'assurer qu'ils ne sont pas en conflit les uns avec les autres et qu'ils offrent des niveaux complémentaires de protection et d'obligations.

Une stratégique globale en matière de données inclura nécessairement l'harmonisation entre les politiques et les lois sur la concurrence, le commerce et la fiscalité, tant au niveau national que régional. Ainsi, un écosystème de données optimisé pour l'Afrique permet d'équilibrer la mobilisation des recettes et la nécessité d'éviter les distorsions sur les marchés locaux et le système fiscal mondial. Les législations sur la propriété intellectuelle doivent également être révisées pour préciser qu'elles n'entravent généralement pas le flux de données ou la protection des données. En outre, les gouvernements doivent élaborer des politiques et des stratégies numériques transversales afin de coordonner les activités dans l'ensemble du secteur public et entre les secteurs public et privé pour atteindre les objectifs nationaux.

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

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

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

L'accès aux données est une condition préalable à la création de valeur, à l'esprit d'entreprise et à l'innovation. Lorsque les données sont de mauvaise qualité ou ne sont pas interopérables, elles limitent la capacité des entreprises et du secteur public à s'engager dans le partage et l'analyse qui peuvent apporter une valeur économique et sociale aux données. Ces cadres de traitement doivent s'aligner sur les principes suivants : consentement et légitimité, limitation de la collecte, spécification de la finalité, limitation de l'utilisation, qualité des données, garanties de sécurité, ouverture (qui inclut la notification des incidents, corrélation importante avec les impératifs de cybersécurité et de cybercriminalité), responsabilité et spécificité des données. Les modèles de sécurité doivent également être transversaux, en mettant l'accent sur le stockage et le traitement en nuage des données sensibles/propriétaires, la gestion des API et le soutien des marchés de données équitables.

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

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

Ainsi, comme il est souligné dans le cadre, la collaboration transversale doit être étayée par des mécanismes visant à stimuler la demande de données, ce qui implique

d'encourager les communautés de données innovantes et, du côté de l'offre, de garantir la qualité, l'interopérabilité et la pertinence des données dans les secteurs public et privé, ainsi que dans la société civile.

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

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

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

- coopèrent pour permettre aux données de circuler dans le continent tout en préservant les droits de l'homme, la protection des données, la sécurité et le partage équitable des bénéfices ;

- coopèrent pour créer les capacités nécessaires en matière de données afin de tirer parti des avantages des technologies et des services qui dépendent des données, notamment la capacité de gouverner les données de manière à ce qu'elles profitent aux pays et aux citoyens africains et favorisent le développement ;

- promeuvent une politique transversale des données et une réglementation souple pour appréhender l'émergence de nouveaux

modèles commerciaux dynamiques basés sur les données, qui puissent favoriser le commerce numérique intra-africain et l'entrepreneuriat basé sur les données ;

- créent des cadres intergouvernementaux pour faciliter la coordination des régulateurs autonomes de la concurrence, des diffèrent secteurs et des données afin de réglementer efficacement la société et l'économie numérique, formuler, mettre en œuvre et réviser la politique des données de manière dynamique, prospective et expérimentale ;

- Élaborer des législations nationales sur la protection des données à caractère personnel et des réglementations adéquates, notamment en ce qui concerne la gouvernance des données et les plateformes numériques, afin de garantir que la confiance est préservée dans l'environnement numérique.

- établir ou maintenir des autorités de protection des données indépendantes, efficaces et dotées de ressources suffisantes, renforcer la coopération avec les autorités de protection des données des membres de l'Union africaine et mettre en place des mécanismes au niveau continental pour élaborer et partager des pratiques réglementaires et soutenir le développement institutionnel afin de garantir un niveau élevé de protection des données à caractère personnel ;

- favorisent l'interopérabilité, le partage des données et la réactivité à la demande de données par la mise en place de normes de données ouvertes dans la création de données qui soient conformes aux principes généraux d'anonymat, de respect de la vie privée, de sécurité et à toute considération sectorielle relative aux données afin de faciliter l'accès des chercheurs, des innovateurs et des entrepreneurs africains aux données à caractère non personnel et à certaines catégories de données à caractère personnel ;

- favorisent la portabilité des données afin que les personnes concernées ne soient pas enfermées dans un seul fournisseur et, ainsi, encouragent la concurrence, le choix des consommateurs et permettent aux travailleurs indépendants de passer d'une plateforme à l'autre ;

- améliorent les infrastructures inégalement développées sur le continent en s’appuyant sur les actions régionaux des CER afin d’accéder à une couverture efficace des réseaux à large bande, un approvisionnement énergétique fiable, ainsi que des infrastructures et des systèmes numériques (données) fondateurs (IDE) (identité numérique (Digital ID), des paiements interopérables fiables, une infrastructure de cloud et de données et des systèmes de partage de données ouverts, pour le commerce numérique transfrontalier et le commerce électronique ;

- établissent un système national intégré de données pour permettre la création de valeur publique et privée basée sur les données, fonctionnant sur la base de cadres de gouvernance harmonisés qui facilitent le flux de données nécessaire à une économie de données dynamique, mais avec des garanties suffisantes pour être fiable, sûr et sécurisé ;

- administrent le système national intégré de données selon des principes d'accès, de disponibilité, d'ouverture (lorsque l'anonymat peut être préservé) d'interopérabilité, de sûreté, de sécurité, de qualité, d'intégrité et d'intégrité ;

- intègrent des codes ou des lignes directrices sur les données propres à un secteur ou à un spécialiste dans les régimes nationaux et continentaux de gouvernance des données ;

- ratifient la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel à le faire dès que possible, afin de servir d'étape fondamentale pour l'harmonisation du traitement des données ; et

- dans les négociations à venir sur les protocoles relatifs au commerce des services et au commerce électronique, ainsi que sur les protocoles relatifs à la concurrence et à la propriété intellectuelle, dans la zone de libre-échange continentale africaine, fournir des lignes directrices pour promouvoir l'accès aux données afin de soutenir l'innovation locale, l'esprit d'entreprise et à des fins pro-concurrentielles.

- donner la priorité aux partenariats qui respectent la neutralité politique et qui tiennent compte de la souveraineté individuelle et de la propriété nationale, afin d'éviter les interférences étrangères susceptibles de nuire à la sécurité nationale, aux intérêts économiques et aux développements numériques des États membres de l'UA

- promouvoir la recherche, le développement et l'innovation dans divers domaines basés sur les données, notamment l'analyse des données massives, l'intelligence artificielle, l'informatique quantique et la technologie Blockchain.

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

- faciliter la collaboration entre les différentes entités traitant des données sur le continent par la mise en place d'un cadre de consultation au sein de la communauté de l'écosystème numérique afin de préserver l'intérêt de chaque acteur.

- encourager et faciliter la circulation des données au sein des États membres de l'UA et entre eux en élaborant un mécanisme de circulation

transfrontalière des données qui tienne compte des différents niveaux de préparation au numérique, de la maturité des données ainsi que des environnements juridiques et réglementaires dans les pays ;

- faciliter la circulation des données entre les secteurs et au-delà des frontières en élaborant un cadre commun de catégorisation et de partage des données qui tient compte des grands types de données et les niveaux de confidentialité et de sécurité associés ;

- travailler en étroite collaboration avec les autorités nationales chargées de la protection des données personnelles des États membres de l'UA, avec le soutien du Réseau africain des autorités de protection des données personnelles (RAPDP), afin de mettre en place un mécanisme et un organe de coordination qui supervise le transfert des données personnelles au sein du continent et assure la conformité avec les lois et règles en matière de sécurité des données et des informations en vigueur dans les états membres de l'UA ..établir ou renforcer un mécanisme au sein de l'Union africaine pour centraliser et renforcer les engagements régionaux sur les normes de données.

- établir des mécanismes et des institutions ou habiliter ceux qui existent déjà, au sein de l'Union africaine, afin de renforcer les capacités et de fournir une assistance technique aux États membres de l'UA pour l'internalisation de ce cadre politique en matière de données ; et

- soutenir le développement d'une infrastructure de données régionale et continentale pour accueillir des technologies avancées axées sur les données (telles que le Big Data, l'apprentissage automatique et l'intelligence artificielle) et l'environnement propice et le mécanisme de partage des données nécessaires pour assurer la circulation à travers le continent ;

- Œuvrer à la construction d'un cyberespace sûr et résilient sur le continent, qui offre de nouvelles opportunités économiques, par l'élaboration d'une stratégie de cybersécurité de l'UA et la création de centres opérationnels de cybersécurité pour atténuer les risques et les menaces liés aux cyberattaques, aux violations de données et à l'utilisation abusive d'informations sensibles ;

- établir un Forum annuel d'innovation des données pour l'Afrique afin de sensibiliser les décideurs politiques au potentiel des données en tant que moteur d'une économie et d'une société numériques, de manière à faciliter les échanges entre les pays et à permettre le partage des connaissances sur la création de valeur et l'innovation en matière de données et les implications de l'utilisation des données sur la vie privée et la sécurité des personnes ;

- renforcer les liens avec d'autres régions et coordonner les positions communes de l'Afrique sur les négociations internationales liées aux

données afin de garantir l'égalité des chances dans l'économie numérique mondiale ;

- élaborer un plan de mise en œuvre qui tienne compte de la souveraineté numérique des États ainsi que des différents niveaux de développement, de la vulnérabilité des populations et de la numérisation au sein des États membres de l'UA, notamment des aspects liés au manque d'infrastructures TIC et à l'absence de politiques et de législations en matière de cybersécurité.

Table des matières

1. Introduction

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

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

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

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

L'optimisation des avantages d'une économie axée sur les données et la réduction des risques dépendent fortement de cadres politiques et réglementaires favorables qui renforcent la légitimité et la confiance du public dans la gestion des données. L'infrastructure de données qui permet un système de données intégré constitue un atout stratégique essentiel pour les pays, mais l'ampleur, l'étendue et la rapidité des changements induits par les technologies numériques axées sur les données rendent la réglementation complexe et gourmande en ressources. À mesure que les technologies émergentes deviennent plus essentielles dans l'économie des données, la diversité des parties prenantes et la pléthore de plateformes impliquées dans sa réglementation se développent également de manière spectaculaire, ce qui rend de plus en plus difficile pour les décideurs de rester impliqués et informés (Banque

africaine de développement, 2019). Les technologies avancées émergentes comme l'intelligence artificielle (IA) sont susceptibles de remettre de plus en plus en question l'efficacité des approches législatives traditionnellement disparates en matière d'élaboration des lois.

Les données sont de nature globale, ce qui signifie que, d'une part, les réglementations ont des implications transfrontalières et que, d'autre part, la préséance réglementaire est le plus souvent établie par les pays développés riches en données et à forte intensité de données. La pression du marché est également imposée par des entreprises en oligopole, notamment Facebook, Apple, Microsoft, Google et Amazon (ou FAGAM). La nature des données permet à ces entreprises qui opèrent sur les marchés numériques mondiaux axés sur les données de tirer parti de leur avantage concurrentiel en matière de données et d'algorithmes dans le monde entier. Ceci affecte à terme la concurrence locale et entrave la compétitivité mondiale des participants nationaux à l'économie des données. Par conséquent, il existe des questions de propriété intellectuelle et d'accès aux données, de commerce équitable, de concurrence et de droits des consommateurs qui ont un impact sur la politique en matière de données dans un contexte mondial et qui soulèvent la nécessité d'une gouvernance et d'une collaboration mondiales.

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

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

2. Mandat

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

Ce cadre politique en matière de données découle de la Stratégie de transformation numérique (STN) adoptée par l'Union africaine en 2020 pour transformer les sociétés

et les économies africaines d'une manière qui permette au continent et à ses États membres d'exploiter les technologies numériques pour une innovation locale qui améliorera les opportunités de vie, atténuera la pauvreté, réduira les inégalités facilitant la fourniture de biens et de services[35]. La concrétisation des objectifs de la STN est essentielle à la réalisation de l'Agenda 2063 de l'Union africaine, le cadre stratégique panafricain pour l'unité, l'autodétermination, la liberté, le progrès et la prospérité collective, et des objectifs de développement durable des Nations unies.

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

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

Le présent Cadre stratégique en matière de données vise à renforcer et à harmoniser les cadres de gouvernance des données en Afrique et à créer ainsi un espace de données partagé et des normes qui régulent la production et l'utilisation croissantes des données sur le continent. Il s'agit de créer un environnement numérique sûr et fiable pour stimuler le développement d'une économie numérique inclusive et durable

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

qui favorise le commerce numérique intra-africain, conformément aux initiatives d'intégration économique régionale en cours dans le cadre de la ZLECAf.

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

2.1 Vision

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

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

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

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

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

2.2 Portée et objectifs

Compte tenu du fait que les données traversent désormais tous les aspects de notre vie quotidienne, mais dans des circonstances très différentes à travers le continent, **le Cadre fournit des orientations fondées sur des principes** aux États membres pour faciliter l'incorporation au niveau national du cadre stratégique continentale en matière de données de façon adaptée à leurs conditions et propose aussi un

instrument ou un mécanisme pour intégrer et coordonner les efforts continentaux. Le Cadre stratégique africain en matière de données vise à **renforcer les systèmes de données nationaux** pour une utilisation efficace des données en créant un environnement favorable qui **stimule l'innovation et l'esprit d'entreprise afin de favoriser le développement d'économies fondées sur la valeur des données** et qui facilite l'interopérabilité des systèmes et les flux de données transfrontaliers nécessaires à la réalisation du marché numérique unique africain. L'harmonisation des marchés africains offre la certitude réglementaire, l'ampleur et la portée nécessaires aux investissements requis pour la création de valeur publique et privée axée sur les données, avec les impacts distributifs et les multiplicateurs non économiques associés.

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

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

- Permettre aux États de coopérer sur les questions de gouvernance des données pour atteindre des objectifs communs liés au développement durable de leurs économies et de leurs sociétés ;

- Informer et soutenir l'internalisation de la stratégique continentale par les pays africains ;

- Veiller à ce que les données puissent circuler à travers les frontières aussi librement que possible, tout en favorisant une répartition équitable des bénéfices et en traitant les risques liés aux violations des droits de l'homme et aux autres intérêts légitimes des États, tels que la lutte contre le blanchiment d'argent, l'évasion fiscale, les jeux d'argent en ligne, la sécurité nationale.

- Favoriser et faciliter les flux de données transfrontaliers et en augmentant les opportunités commerciales tout en garantissant un niveau adéquat de données personnelles et de vie privée ;

- Établir des mécanismes de confiance collaboratifs pour permettre aux données de circuler aussi librement que possible entre les États membres, tout en préservant la souveraineté des États membres et leur capacité à réguler l'économie numérique.

- Encourager et faciliter les flux de données transfrontaliers et accroître les opportunités commerciales tout en garantissant un niveau adéquat de données à caractère personnel et de confidentialité ;

- Permettre aux États, au secteur privé, à la société civile et aux organisations intergouvernementales de coordonner leurs efforts sur les questions de données à travers le continent afin de réaliser un marché numérique unique et d'être plus compétitif dans l'économie mondiale ;

- Faire en sorte que les données puissent circuler à travers les frontières aussi librement que possible, tout en favorisant une répartition équitable des avantages et en traitant les risques liés aux droits de l'homme et à la sécurité nationale ;

- Permettre la compétitivité dans l'économie mondiale grâce à une coopération étroite et durable des États africains, du secteur privé et de la société civile par le biais d'opportunités de restructuration pour optimiser les avantages de la donnéification de l'économie et de la société.

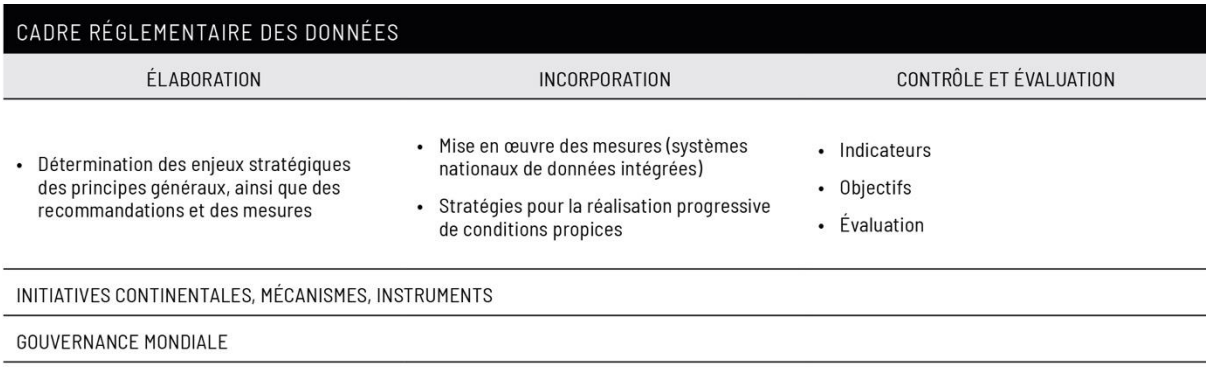
- Veiller à ce que les données soient utilisées d'une manière durable qui profite à la société dans son ensemble et ne porte pas atteinte à la vie privée, à la dignité et à la sécurité des personnes ;

- Veiller à ce que les données soient largement disponibles dans le cadre de protections appropriées pour une utilisation tant commerciale que non commerciale ; et

- Faciliter les moyens innovants de promouvoir les avantages publics en utilisant les données de manière nouvelle, ce qui permettrait aux données en Afrique de réaliser la valeur des données dans la prise de décision, la planification, le suivi et l'évaluation du secteur public.

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

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



3. La nécessité de repenser les stratégies de réglementation

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

3.1. Les données en tant que base d'un nouveau contrat social et d'une économie de l'innovation

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

Les données ne génèrent pas non plus automatiquement de la valeur. Au contraire, il existe différentes utilisations des données et différentes méthodes permettant de mesurer la valeur économique et sociale des données et des flux de données. (OCDE 2019) Au sens économique, c'est ce que les entreprises font qui conduit à la création de valeur à la fois en interne au sein de l'entreprise et en externe à travers le réseau étendu de données. Théoriquement, cette valeur peut être quantifiée en attribuant une valeur monétaire prenant en considération plusieurs variables de coûts et de revenus, comme la manière dont les organisations facturent les données générées par les utilisateurs, ou le rapprochement des coûts de gestion des données tels que la collecte, la maintenance et la publication des données. La

valorisation des données du point de vue des avantages socio-économiques - ou de la valeur des données non marchandes - intervient lorsqu'il existe des conditions fondamentales ou des catalyseurs qui permettent aux gouvernements de fournir des services publics plus efficaces, d'offrir une gestion efficace de l'environnement, et lorsque les citoyens vivent en meilleure santé et en sécurité économique grâce à l'exploitation des données (Banque mondiale, 2021). Un exemple de création de valeur des données publiques est l'utilisation des données pour informer les besoins d'allocation des ressources afin d'améliorer la prestation de services.

Ces caractéristiques des données ont été présentées ailleurs comme le potentiel des données à fournir la base d'un nouveau contrat social. (Banque mondiale 2021). Les orientations politiques qui découlent de cette approche mettent l'accent sur la nécessité de disposer de données ouvertes, de normes d'interopérabilité et d'initiatives de partage des données pour exploiter le potentiel des données en vue de stimuler le développement, d'assurer une meilleure répartition des avantages des données, d'encourager la confiance grâce à des garanties qui protègent les personnes contre les dommages liés à l'utilisation abusive des données, de créer et de maintenir un système de données national intégré qui permet le flux de données entre un large éventail d'utilisateurs d'une manière qui facilite l'utilisation et la réutilisation sûres des données.

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

Bien que les préjudices liés à la concentration des données et des informations et aux asymétries de pouvoir soient universels, leurs impacts sont inégaux, tant entre les pays qu'au sein de ceux-ci. La mise en place de politiques qui atténuent le risque différentiel pour différentes catégories de personnes, comme les enfants, ou pour des catégories de données dans différents secteurs, comme les données sur la santé, ou encore la garantie que la centralité croissante des données ne perpétue pas les injustices historiques et les inégalités structurelles, nécessiteront une réglementation beaucoup plus granulaire et adaptative. Si un cadre politique de préservation des droits en matière de données sera essentiel, les notions individualisées de vie privée, de liberté d'expression et d'accès à l'information (droits de première génération) dans les cadres normatifs actuels de protection des données ne suffiront pas à garantir des résultats plus équitables et plus justes. Les droits sociaux et économiques de deuxième génération sont également pertinents pour plusieurs domaines de la gouvernance des données en ce qui concerne la disponibilité, l'accessibilité, la facilité d'utilisation et l'intégrité des données qui

nécessitent une gouvernance des données pour avoir un impact sur l'inclusion équitable. Cela met en évidence la nécessité d'aller au-delà d'une réglementation de conformité négative et de passer à une réglementation positive qui créera un environnement permettant aux États et aux citoyens africains de participer efficacement à l'économie numérique. La création des conditions permettant l'accès nécessaire aux données tout en préservant les droits nécessitera le renforcement des capacités institutionnelles au sein de l'État et des capacités à réglementer de manière agile afin d'exploiter le potentiel des données visant à résoudre certains des problèmes les plus insolubles du continent.

Pour y parvenir, les décideurs politiques doivent équilibrer certaines des tensions liées à la valorisation des données afin de les optimiser à ces fins. La transformation des données en informations utiles pour guider la prise de décision s'articule autour de la chaîne de valeur des données, où les entreprises et certaines entités publiques disposent de cadres adéquats pour soutenir un écosystème de données cohérent. La création de valeur à partir des données peut renforcer les intérêts privés, comme l'amélioration de l'efficacité opérationnelle des entreprises, l'augmentation de leur clientèle et la création de produits et services innovants qui profitent aux activités commerciales et aux personnes concernées. Pour les gouvernements, la valeur publique des données est réalisée en s'assurant que les avantages socio-économiques des données permettent d'atteindre des objectifs socio-économiques plus larges. Bien que l'évaluation des données publiques et privées ait des intentions et des résultats différents, elles ne s'excluent pas mutuellement. De fait, la valeur marchande et la valeur non marchande ne devraient pas être corrélées au secteur privé et au secteur public. La valeur non marchande pourrait également être reliée à la recherche ou à la société civile. Le secteur public peut également créer une valeur marchande en ouvrant certains ensembles de données et en établissant des sources de revenus nouvelles. Il existe également des interactions innovantes entre les acteurs publics et privés qui peuvent améliorer l'écosystème global des données pour répondre aux besoins de développement socio-économique et améliorer le bien-être.

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

3.2. Nécessité d'une gouvernance des données - créer de la valeur, prévenir les préjudices

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

La politique en matière de gouvernance des données comporte ainsi certains mécanismes pratiques :

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

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

Ainsi, les priorités en matière de gouvernance deviennent :

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

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

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

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

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

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

4. Contexte

4.1. Vue d'ensemble des tendances en matière de politique et de législation régionales internationales

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

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

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

Le cadre de protection des données à caractère personnel de l'APEC, qui a été mis en œuvre par les États membres de l'APEC depuis 2005, se compose d'un ensemble

de principes visant à garantir la libre circulation des informations à l'appui du développement économique. Le cadre de l'APEC adopte une approche différente de la protection des données en alignant le mandat du cadre sur la promotion du commerce et de l'investissement, plutôt que sur la protection des droits de l'homme fondamentaux comme dans le RGPD de l'UE. L'un des points forts du cadre réside dans le fait qu'il souligne que les réglementations en matière de protection de la vie privée doivent prendre en considération l'importance des intérêts commerciaux et des entreprises, ainsi que les cultures et autres diversités des économies des États membres.

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

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

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

4.2. Contexte politique et législatif africain

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

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

Autres initiatives majeures sur le continent concernant la politique des données

L'initiative politique et réglementaire pour l'Afrique numérique (PRIDA). [3637]*Dans le cadre de la mise en œuvre de ce projet, la Commission de l'Union africaine a mis en place un groupe de travail d'experts qui a contribué à l'identification des indicateurs clés d'harmonisation et au développement d'un modèle et d'un outil de suivi et d'évaluation (S&E) sur la protection des données et la localisation qui sont prêts à être utilisés par les États membres de l'UA et les organisations régionales pour évaluer le degré d'harmonisation et d'alignement des lois et réglementations nationales.*

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

Les lois et protocoles régionaux sur la concurrence dans les communautés économiques régionales (CER) établies s'appliquent aux entreprises qui traitent des données, bien qu'elles ne fassent généralement pas explicitement référence aux données. Il s'agit notamment des règlements et des règles de concurrence du COMESA (2004), de la loi sur la concurrence de la CAE (2006), du protocole du marché commun de la CAE et du protocole relatif à la création d'une union douanière de la CAE, de l'acte additionnel de la CEDEAO relatif à « l'adoption des règles de concurrence communautaires et aux modalités de leur application dans l'espace de la CEDEAO », du protocole de la SADC sur le commerce (2006) et de la déclaration de la SADC sur la coopération régionale en matière de politique de concurrence et de consommation (2009). Ils abordent les pratiques anticoncurrentielles, y compris l'abus

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

de position dominante, ainsi que la structure du marché par la réglementation des fusions et acquisitions. Toutefois, les détails et les approches sont différents, ce qui pose des problèmes aux entreprises opérant dans plusieurs régions.

4.3. Analyse de la situation de l'économie des données en Afrique

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

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

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

• Nouvelles opportunités de travail pour les jeunes épris de technologie, afin d'améliorer l'entrepreneuriat local, le développement de contenu local et l'innovation.	l'intégrité, la sécurité, l'équité, les droits et l'éthique.

4.4. Les défis stratégiques qui se posent en matière de concrétisation des opportunités et d'atténuation des risques

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

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

Pour créer cet environnement favorable dans les États membres de l'Union africaine et dans la région, les points suivants, issus de l'analyse de la situation, peuvent avoir un impact sur la capacité des pays à répondre aux besoins d'une nouvelle économie des données.

La numérisation et la donneification touchent les secteurs public et privé, l'économie formelle et informelle, ainsi que les sphères sociales et culturelles, et nécessitent un changement par rapport aux politiques sectorielles traditionnelles. La politique en faveur de l'économie du numérique et des données

dont la société a besoin doit être transversale afin de coordonner les activités dans l'ensemble du secteur public et entre les secteurs public et privé pour atteindre les objectifs nationaux et régionaux. Il est en même temps important de tenir compte des politiques sectorielles spécifiques en matière de données afin d'optimiser et de préserver les diverses utilisations de différents types de données (par ex., les données relatives à la santé ou au climat). Au-delà de la constatation de ce principe, l'élaboration réelle des différentes politiques sectorielles qui devront être élaborées dépasse les attributions de ce cadre de haut niveau. Une réglementation efficace de marchés mondialisés de plus en plus complexes est essentielle pour que l'épine dorsale omniprésente et les services continus nécessaires au déploiement des services et applications de données puissent répondre aux divers besoins économiques et sociaux, améliorer la concurrence et favoriser l'innovation africaine. Comme dans tous les pays du monde, les décideurs politiques devront revoir et renouveler les arrangements institutionnels pour la gouvernance de l'économie des données. Des régulateurs spécialisés, tels que les régulateurs des données ou de l'information, sont nécessaires pour traiter les nouvelles questions de gouvernance des données, et les régulateurs nouveaux et établis devront s'engager dans des niveaux élevés de coordination nationale et régionale. Pour que le marché unique africain devienne opérationnel, l'harmonisation réglementaire est également essentielle à l'intégration des marchés, de même que des systèmes communs de paiement électronique, la facilitation du commerce transfrontalier et la normalisation de la fiscalité et des droits transfrontaliers. Les États africains devront se regrouper et élaborer des positions communes pour obtenir des résultats plus favorables dans les forums de gouvernance mondiale afin de mieux servir les intérêts africains.

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

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

La clarté et la sécurité juridiques à cet égard sont particulièrement importantes pour mettre en place une transformation numérique fiable et durable. Il est possible, par exemple, de fournir une certitude sur des questions telles que la propriété ou la garde des données et les droits qui y sont associés, tout en établissant un système complet de surveillance de l'accès, de l'acquisition, de l'analyse, du stockage et de la diffusion des données à caractère personnel et non personnel. L'harmonisation réglementaire est également essentielle pour l'intégration des marchés, avec des systèmes de paiement en ligne communs, la facilitation du commerce transfrontalier et la normalisation de la fiscalité et des droits transfrontaliers. Garantir la protection des consommateurs tout en permettant l'innovation est également essentiel au développement et à l'inclusion économique. En outre, comme les différentes approches juridiques servent des intérêts différents, les pays ont la possibilité de réinventer un système juridique harmonisé qui équilibre de manière adéquate les intérêts des entreprises et les droits numériques pertinents.

La création de systèmes de données nationaux intégrés et interopérables en réponse aux défis émergents améliore l'efficacité et permet une plus grande transparence et responsabilité. Un défi commun à tous les pays est que lorsque **les données sont de mauvaise qualité ou ne sont pas interopérables**, cela limite la capacité des entreprises et du secteur public à s'engager dans le partage et l'analyse qui peuvent apporter une valeur économique et sociale aux données. Des voies d'accès insuffisantes et un engagement limité en faveur de l'ouverture des données publiques, entre autres, font également obstacle à un environnement propice à une

économie des données solide. La fourniture de données de qualité nécessite de créer une demande de données dans tous les sites institutionnels (c'est-à-dire le secteur public, les institutions et les entreprises, etc.) L'extraction de la valeur des données nécessite non seulement un contrôle, mais aussi le développement de capacités analytiques et techniques dans les secteurs public, privé et autres.

Bien que plusieurs pays aient introduit des systèmes d'identification numérique, le **manque de systèmes d'identification numérique omniprésents et interopérables reste un défi social et économique majeur sur le continent**. Il s'agit d'un élément essentiel de l'organisation et du traitement des données relatives à certains attributs des personnes physiques, des entités juridiques et des biens. Ils permettent l'identification dans le but d'effectuer des transactions et d'interagir dans un écosystème de données de confiance. L'identité fondatrice et fonctionnelle facilite les services numériques, mais la couverture complète de l'identité fondatrice, en particulier, reste un défi à la fois social et économique. Les cadres régionaux émergents sur l'identité numérique commencent à s'attaquer directement à ce défi. Il existe des possibilités d'intégrer l'identité fonctionnelle décentralisée dans les cadres de protection des données. Ceux-ci peuvent fournir une identité fonctionnelle, tout en réduisant les risques associés aux données à caractère personnel.

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

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

En dépit de l'adoption de chartes continentales, de conventions et de lois types des communautés économiques régionales visant à harmoniser **la réponse de l'Afrique aux défis posés par la numérisation et l'intégration des données, leur ratification et leur mise en œuvre ont été variables**. Une adoption plus large des fondements numériques des initiatives continentales, telles que le ZLECAf, sera essentielle pour concrétiser les avantages d'une plus grande coopération économique. La

normalisation des règles relatives aux flux transfrontaliers est une condition préalable à la concrétisation des avantages attendus de la ZLECAf. Cela peut se faire en utilisant l'opérationnalisation de l'accord pour faciliter une meilleure interopérabilité transfrontalière des données et fournir une approche continentale harmonisée de l'économie numérique fondée sur les données. Cela peut être réalisé d'une manière qui soutient les avantages socio-économiques du commerce numérique et du commerce électronique, tout en garantissant que les informations sensibles restent sécurisées et que les réglementations pertinentes sur la protection des données à caractère personnel sont respectées.

En réponse aux précédentes vagues d'innovation technologique, économique, réglementaire et sociale, **les pays africains ont eu tendance à être des accepteurs de normes plutôt que des créateurs de normes**. Les organisations multilatérales, allant de l'OCDE à l'Organisation mondiale de la propriété intellectuelle et à l'Organisation mondiale du commerce, réagissent aux défis de la gouvernance mondiale des données. Bien que l'Afrique et les pays africains ne mènent pas, à quelques exceptions, de politiques numériques mondiales, mais la possibilité existe de changer cela. Les pressions commerciales multilatérales, plurilatérales et bilatérales visant à permettre la circulation des données avec peu de restrictions s'accompagnent de pressions visant à concéder des droits de propriété intellectuelle sur les données, de sorte que les pays africains sont confrontés à la perspective d'une exploitation et d'une appropriation des données. En l'absence d'une politique commune et d'un engagement en faveur de normes communes sur tout le continent, il est difficile pour la plupart des pays africains d'échapper aux courants de la dynamique mondiale en évolution rapide. Par conséquent, une action coordonnée par et pour l'Afrique est nécessaire pour libérer collectivement l'énorme potentiel de transformation des données afin de développer une économie numérique et une société moderne inclusive et durable en Afrique.

SMART AFRICA- Identité Numérique

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

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

Cas des communautés d'utilisateurs de l'innovation en matière de données

Les exemples typiquement cités de succès dans l'innovation en matière de données ouvertes sont l'émergence de pôles d'innovation particuliers dans la région, principalement dans les zones urbaines. Les pôles d'innovation, comme préconisé ailleurs, peuvent certainement être un site pour les succès sociaux et économiques des données ouvertes ; pourtant, il existe des exemples d'innovation en matière de données ouvertes qui peuvent se produire de manière plus organique simplement par la mise à disposition de données publiques ouvertes de qualité. Ces

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

5. Cadre stratégique en matière de données

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

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

Le Cadre fournit des orientations de haut niveau fondées sur des principes aux États membres pour les aider à élaborer une politique en matière de données adaptée à leur situation. Il recense les principes clés d'une gouvernance efficace des données et les stratégies à mettre en œuvre aux niveaux national, continental et international. Cela inclut des orientations sur les procédures et garanties institutionnelles, administratives et techniques appropriées qui doivent être mises en œuvre. L'objectif est de s'assurer que les écosystèmes de données nationaux et sous-régionaux sont

construits sur une infrastructure et des processus numériques fiables et interopérables qui font progresser un système de données continental harmonisé permettant d'assurer une croissance économique et un développement équitables et durables pour tous les peuples d'Afrique.

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

- Des incitations à investir efficacement dans les infrastructures de données numériques fondamentales et les systèmes numériques fondamentaux ;

- Des dispositions institutionnelles favorisant l'interaction optimale entre l'État, les marchés et les institutions de régulation pour permettre la création de valeur publique et privée ;

- Le renforcement des capacités numériques humaines et institutionnelles;

- La création de valeur à partir d'une utilisation responsable des données, la promotion d'une croissance équitable durable et le renforcement de la prospérité commune grâce à l'économie des données ;

- Une meilleure répartition des possibilités tant pour l'utilisation des services de données que pour la création de valeur axée sur les données au sein des pays et entre eux ; et

- Des environnements efficacement réglementés qui favorisent une concurrence équitable et les efficacités d'allocation des ressources qui produisent des résultats positifs en matière de bien-être des consommateurs.

5.1. Principes directeurs du Cadre

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

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

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

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

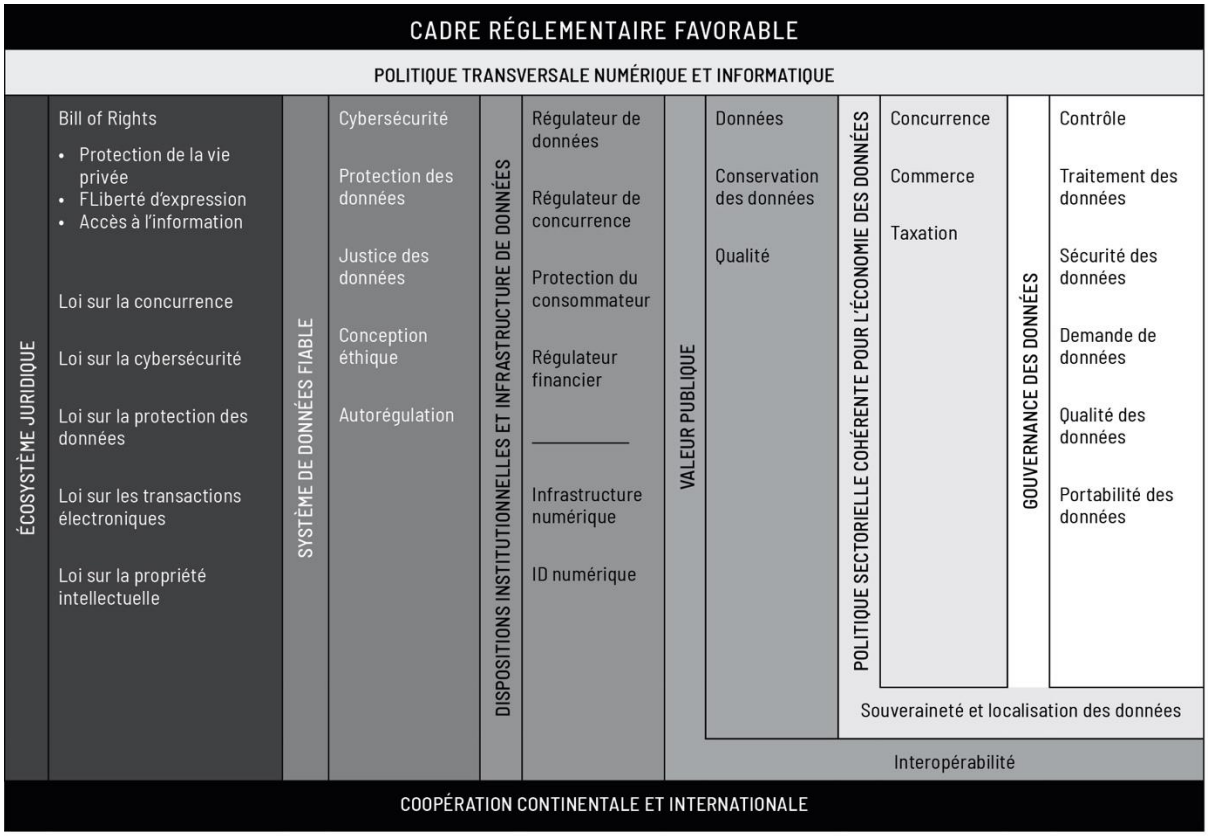
- **Équité et inclusivité** : pour la mise en œuvre du cadre, les États membres doivent veiller à ce qu'il soit inclusif et équitable, qu'il offre des opportunités et des avantages à tous les Africains et, ce faisant, qu'il cherche à redresser les inégalités nationales et mondiales en tenant compte des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

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

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

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

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



5.2. Définition et catégorisation des données

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

5.2.1. Données à caractère personnel et non personnel

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

Il existe de nombreuses façons de catégoriser les données affectant la politique et la réglementation de chaque catégorie, parmi les dimensions les plus importantes figurent l'intention publique ou privée et les méthodes de collecte traditionnelles ou nouvelles (UNCTAD, 2021; World Bank, 2021).

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

5.3. Facteurs permettant de créer de la valeur dans l'économie des données

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

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

Recommandations :

- Les États membres de l'Union africaine devraient promouvoir la recherche, le développement et l'innovation dans divers domaines liés aux données, notamment l'analyse des données massives, l'intelligence artificielle, l'informatique quantique et la Blockchain.

- Tous les groupes de parties prenantes, y compris les gouvernements, devraient renforcer leurs capacités d'analyse et de gestion des données afin de faciliter l'utilisation de données de qualité et de systèmes interopérables fiables. Cependant, il est important de se rappeler que dans de nombreux pays, le plus grand producteur et collecteur commun de données est l'État. Par conséquent, bon nombre des observations incluses dans la discussion sur la gouvernance des données ci-dessous ont une incidence particulière sur les actions des gouvernements.

5.3.1. Infrastructure de données fondamentale

5.3.3.1. Accès et utilisation du haut débit et des données

Définition des problématiques

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

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

Recommandation

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

Actions

Les États membres devront faire évoluer les politiques qui :

- Proscrire les frais prohibitifs de « droit de passage » des câbles à large bande et soutenir le partage des infrastructures ;
- Prévenir les pratiques anticoncurrentielles découlant d'une domination sur les marchés des infrastructures ;
- Investissent dans le Wi-Fi public et les technologies complémentaires ;
- Adopter des techniques innovantes d'utilisation du spectre, telles que l'attribution et l'accès dynamiques au spectre, et l'exploitation du dividende numérique (bandes de spectre accélérées par la migration de la radiodiffusion analogique vers le numérique) pour étendre l'accès au haut débit pour les zones rurales mal desservies ;
- Promouvoir la transition et l'adoption de l'IPv6, à mesure que les ressources de l'IPv4 s'épuisent au niveau mondial ;
- Investir dans des infrastructures nationales de dorsale et de connectivité transfrontalière, telles que les points d'interconnexion Internet (IXP), aux niveaux national et régional, afin de tirer parti de la bande passante internationale disponible, de réduire le coût d'accès à Internet et d'améliorer les vitesses d'accès aux données dans la région ;
- Tirer parti de modèles innovants pour le financement des infrastructures de données.

5.3.3.2. Infrastructure des données

Définition des problématiques

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

L'infrastructure de données de base fait référence à un large éventail de technologies qui facilitent l'utilisation intensive de données de qualité, y compris l'infrastructure matérielle et immatérielle. Il faudra combler les déficits actuels de l'infrastructure TIC "traditionnelle" en parallèle à la création d'une architecture destinée à soutenir l'intensification de la donnéification. Cela inclut également des ressources d'infrastructure telles que l'identification numérique pour permettre des transactions et une présence en ligne sécurisées. Le présent cadre se concentre sur trois aspects

de l'infrastructure des données qui nécessitent des considérations politiques se renforçant mutuellement et qui influencent également la gouvernance des données : les services en nuage, le big data et la plateformisation.

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

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

Services en nuage

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

L'interopérabilité de la fourniture de services en nuage est un facteur essentiel, car elle offre une certaine souplesse et permet aux utilisateurs de passer d'un fournisseur de services en nuage à un autre. Parmi les autres avantages de l'informatique en nuage, citons la réduction des dépenses liées à la consommation d'énergie ainsi que la diminution de la demande de gestion et de maintenance des systèmes en confiant la gestion des ressources informatiques à des tiers. En conséquence, les fonds peuvent être réaffectés à des activités orientées vers les clients et à une meilleure prestation des services publics. Toutefois, comme certains facteurs favorisent un environnement propice aux services en nuage, il faut prendre des dispositions pour

adopter les nouvelles technologies tout en s'attaquant aux problèmes structurels de la fracture numérique (capital humain, infrastructure, etc.). Ces processus doivent se renforcer mutuellement et être adaptés aux réalités économiques des États membres.

Big Data

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

Plateformisation

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

Le commerce numérique et les plateformes de commerce électronique étant de plus en plus à la base de l'activité mondiale et transfrontalière, l'intégration de domaines traditionnellement distincts de la réglementation et des priorités politiques est devenue de plus en plus importante et entrelacée au-delà des frontières géographiques. Toutefois, des politiques telles que la localisation des données ne seront pas plausibles sans les exigences structurelles et institutionnelles nécessaires à leur évolution et à leur mise en œuvre efficaces, en particulier en ce qui concerne les capacités numériques(Andreoni & Tregenna, 2020) [38]

Recommandations

L'utilisation des données comme outil de promotion des intérêts publics exigera des États qu'ils renforcent leurs infrastructures de données nationales et nécessitera un engagement solide des parties prenantes aux niveaux national, régional et mondial. L'élaboration de cadres politiques complets pour les données devrait s'accompagner

[38] Andreoni, A., & Tregenna, F. (2020). Escaping the middle-income technology trap: A comparative analysis of industrial policies in China, Brazil and South Africa. Structural Change and Economic Dynamics, 54, 324-340.

de stratégies de mise en œuvre dans les délais impartis pour les différents mandats nationaux afin de garantir la responsabilité et la transparence. Les États membres devraient hiérarchiser les ressources afin de s'assurer qu'il existe des incitations à accroître les investissements dans l'infrastructure numérique, les plateformes de données et les capacités logicielles pour exploiter le big data. Les investissements dans les infrastructures de données doivent soutenir le contrat social numérique. Les efforts des États pour améliorer l'interopérabilité, la qualité et l'administration publique des données doivent également compléter et améliorer les systèmes numériques publics tels que les identifications numériques, les paiements numériques et les flux de données ouverts, dans la mesure du possible.

Actions

- Au lieu de se concentrer sur l'investissement initial important pour remplacer les équipements TIC hérités qui se déprécient, les États membres devraient tirer parti des économies d'échelle et de gamme pour adopter des infrastructures qui soutiennent les avantages facilitateurs offerts par les services en nuage et d'autres nouvelles technologies qui soutiennent la création de valeur des données.

- Les politiques fiscales, commerciales (y compris en matière d'investissement et d'innovation) et de concurrence doivent être cohérentes, complémentaires et adaptées à l'économie numérique axée sur les données, notamment pour informer les stratégies de développement des infrastructures.

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

Gouvernance des données

- Créer des droits de portabilité des données - y compris pour les données non personnelles, afin que les clients des services en nuage puissent plus facilement changer de fournisseur.

- Développer des normes contractuelles pour les organisations publiques (qui peuvent être utilisées par les PME également), qui protègent leurs droits d'accès, de récupération, de suppression, etc. des données (y compris les données non personnelles, encore une fois) qui sont traitées par les fournisseurs de cloud computing.

- Développer des obligations de licences équitables, raisonnables et non discriminatoires (FRAND) pour les plateformes et les fournisseurs de cloud computing qui ont accès à des ensembles de données qui deviennent une ressource vitale pour entrer sur un marché.

5.3.3.3. ID numérique

Définition des problématiques

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

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

Recommandations

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

5.3.2. Créer des systèmes de données légitimes et dignes de confiance

Définition des problématiques

Pour créer un environnement de données fiable, les utilisateurs doivent faire confiance à l'ensemble du système politique et économique qui sous-tend l'économie des données. Parmi les aspects fondamentaux de ce système, citons la sauvegarde des droits de l'homme fondamentaux par le biais de l'État de droit, des dispositions institutionnelles et des réglementations établies par des processus consultatifs et transparents, et l'obligation pour les institutions chargées de superviser l'utilisation des données, ainsi que pour les producteurs de données publics et privés, de rendre

compte de l'utilisation des données publiques et à caractère personnel. L'inclusion et la diversité des personnes qui gèrent et supervisent les environnements de données, par exemple par le biais d'équipes mixtes, sont des critères importants pour instaurer la confiance. Plusieurs pays africains disposent déjà d'un grand nombre de ces aspects, le défi continental étant de s'assurer que tous les pays disposent de tous les aspects nécessaires et que ceux-ci sont adaptés de manière appropriée aux défis technologiques et économiques des données qui évoluent rapidement. Le cadre définit toutes les composantes essentielles des systèmes des données légitimes et dignes de confiance afin de permettre aux pays de comparer s'ils ont certains ou tous les composants entièrement en place.

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

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

5.3.3.4. Cybersécurité

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

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

5.3.3.5. Cybercriminalité

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

5.3.3.6. La protection des données

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

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

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

5.3.3.7. La justice en matière de données

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

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

Recommandations

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

Actions

- Protéger les droits de l'homme fondamentaux dans l’environnement numérique grâce à l'État de droit

- Veiller à ce que les dispositions institutionnelles et les réglementations ne soient établies que par des processus inclusifs, consultatifs et transparents ;

- Veiller à ce que les institutions chargées de superviser l'utilisation des données, ainsi que les producteurs de données publics et privés, soient responsables de l'utilisation des données publiques et personnelles.

- Renforcer la coopération avec les autres APD pour assurer une sauvegarde suffisante, une protection réciproque des données personnelles ainsi que des droits numériques individuels et collectifs sur tout le continent.

- Renforcer les accords d'assistance mutuelle légaux et les activités entre les États pour les enquêtes et les poursuites en matière de cybercriminalité.

- Veiller à ce que les institutions chargées de superviser l'utilisation des données personnelles soient habilitées à disposer de pouvoirs d'entrée et d'inspection aux fins de l'application des lois et règlements sur la protection de la vie privée et des données.

- S'assurer en outre que l'institution responsable de la surveillance de l'utilisation des données personnelles dispose des pouvoirs de correction suivants en ce qui concerne la correction de la violation des aspects de l'utilisation abusive et de l'abus des données personnelles :

    - Avertir un responsable du traitement ou un sous-traitant des données que les opérations de traitement prévues sont susceptibles d'enfreindre les dispositions des lois et réglementations applicables en matière de protection des données.

    - Réprimander un responsable du traitement ou un sous-traitant lorsque les opérations de traitement enfreignent les dispositions des lois et réglementations applicables en matière de protection des données.

    - Ordonner à un responsable du traitement de communiquer une violation de données personnelles aux personnes concernées.

    - Imposer une limitation temporaire ou définitive incluant une interdiction de traitement des données personnelles.

    - Ordonner la suspension des flux de données vers un destinataire dans un pays tiers ou vers une organisation internationale qui n'assure pas une protection adéquate similaire à celle du pays exportateur de données.

- Les institutions chargées de surveiller l'utilisation des données personnelles devraient être habilitées soit à assister, soit à demander l'indulgence d'un tribunal pour aider une personne ayant subi un préjudice matériel à la suite d'une violation de ses données personnelles

à recevoir une indemnisation d'un responsable du traitement ou d'un sous-traitant pour le dommage subi.

5.3.3.8. Éthique des données

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

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

L'éthique, quand on travaille avec la loi, il permet la mise en place de systèmes de données fiables en fournissant le type de détails pratiques et techniques qui soutiennent les lois, puisque les lois sont généralement d'application plus générale que les codes éthiques spécifiques, mais aussi parfois moins rapidement adaptables aux nouvelles technologies. L'éthique fonctionne de manière prospective, ce qui permet une conception éthique, tandis que les lois sont généralement promulguées et fonctionnent de manière rétrospective. Les codes de conduite éthiques devraient incarner les droits numériques et favoriser le respect du droit international et national.

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

Les traités relatifs aux droits de l'homme - en tant que produits de processus consensuels entre les représentants légitimes des citoyens - jouissent d'une plus grande légitimité que les codes d'éthique et sont juridiquement applicables lorsqu'ils sont promulgués au niveau national et par le biais de décisions régionales. Si ces traités manquent parfois de la spécificité nécessaire aux écosystèmes de données, les droits numériques, qui ont été formulés de diverses manières par la société civile, entre autres, et s'appuient sur le cadre des droits de l'homme, offrent le type de spécificité qui peut être utilisé. Bien que les organismes de défense des droits de l'homme et les arbitres existants aient la capacité requise pour développer des droits en réponse aux problèmes liés aux données, leurs mandats légaux ne les habilitent pas nécessairement à le faire.

Recommandations

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

Outre les recours juridiques réglementaires ou judiciaires disponibles dans un pays, il est également possible d'envisager d'habiliter les mécanismes des droits de l'homme existants au niveau national, régional et continental à statuer sur les utilisations des données.

Actions

- L'industrie des données et les communautés de recherche utilisant des données doivent formuler des codes de pratique, y compris les principes de responsabilité et d'éthique dès la conception, par le biais de processus incluant les personnes dont les données sont concernées ;

- Les États membres doivent exiger des cadres éthiques conformes aux droits dans les processus de passation de marchés publics ;

- Les États membres doivent inclure l'évaluation des codes d'éthique en matière de données dans les mandats des organismes de défense des droits de l'homme existants, tels que les commissions des droits de l'homme.

5.3.3. Dispositions institutionnelles pour la réglementation des systèmes adaptatifs complexes

Les points suivants sont des considérations essentielles pour aligner le contexte réglementaire dans un pays qui dispose des exigences d'une économie de données. La réglementation dans les économies de données exige des décisions réglementaires flexibles orientées vers l'avenir en cas d'incertitude. Ainsi, les régulateurs ont besoin à la fois du mandat et de la confiance pour réglementer de manière proactive. La réglementation adaptative complexe répond non seulement aux

défis de l'évolution rapide et de l'incertitude, mais encore à la complexité des écosystèmes de données qui alimente à une dynamique multifactorielle.

5.3.3.1. Renforcer les capacités des organismes de réglementation

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

5.3.3.2. Le passage d'une réglementation en vase clos

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

DOMAINE DE RÉGULATION	POINTS DE COLLABORATION POTENTIELLE AVEC L'AUTORITÉ DE RÉGULATION DES DONNÉES
Télécommunications	La disponibilité et la qualité de l'infrastructure de base pour permettre les services de données
Concurrence	La concentration, les fusions et les acquisitions, les pratiques anticoncurrentielles sur les marchés du numérique et des données, mais aussi l'effet de la tarification et de la structure du marché sur la sécurité
Protection du consommateur	Les dispositifs et services numériques, le commerce électronique
Commerce et industrie	La fiscalité numérique, le commerce électronique, les services numériques, les services financiers numériques
Finance	Le blockchain financier, la cybersécurité, l'inclusion financière, les services financiers mobiles, la confidentialité
Éducation	La protection des enfants en ligne, la connectivité des écoles, la disponibilité des données pour l'acquisition de compétences en matière de données

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

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

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

Encourager la coopération régionale et internationale sur les initiatives en matière de confidentialité des données et de cybersécurité afin de rationaliser les règles et pratiques disparates en matière de confidentialité des données et de cybersécurité dans des normes et des lois régionales ou mondiales communes et permettre la libre circulation des données et le commerce numérique (GSR 2021)].

5.3.3.3. Régulateur de données

La capacité des régulateurs sectoriels à être efficaces est déterminée, au moins dans une certaine mesure, par les dispositions institutionnelles et l'autonomie des régulateurs pour mettre en œuvre la politique. Les niveaux d'efficacité et d'innovation qui permettent l'évolution de l'écosystème dépendent de la disponibilité des aptitudes et des compétences des personnes et des institutions à chaque nœud de l'écosystème pour exploiter les avantages associés aux réseaux intégrés pour le développement économique et l'engagement social ou politique (Gillwald, Moyo et Stork 2012).

La mise en place d'un système de données intégré au niveau national et régional dépend aussi fortement de cadres réglementaires et politiques favorables qui facilitent l'obtention de données utiles, le renforcement des capacités humaines et techniques pour créer de la valeur à partir des données, l'encouragement du partage des données et de l'interopérabilité, et l'augmentation de la légitimité et de la confiance du public au sein de l'État pour gérer les données des citoyens de manière responsable. Pour créer les conditions qui permettent l'accès nécessaire aux données tout en préservant les droits, il faudra renforcer les capacités et les compétences institutionnelles afin d'optimiser le potentiel des données, et développer des mécanismes d'application.

5.3.3.4. 5.3.3.4 Concurrence

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

plateformes de données et aux nouveaux produits basés sur l'efficacité dynamique qui peuvent produire des produits complémentaires innovants (comme Whatsapp) qui améliorent le bien-être et le choix des consommateurs ou même les possibilités de concurrence locale sur leurs plateformes tout en étant dominants sur le marché mondial sous-jacent, (Facebook).

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

5.3.3.5. Protection des consommateurs

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

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

Recommandations

Les États membres de l'UA doivent disposer de réglementations adéquates, notamment en matière de gouvernance des données et de plateformes numériques, afin de garantir que la confiance est préservée dans l'environnement numérique. Les régulateurs des données devraient disposer des pouvoirs nécessaires pour faire

respecter les réglementations en matière de données, tels que les pouvoirs d'émettre des avertissements, de sanctionner les violations, d'accorder des compensations aux victimes de données, et de coopérer avec d'autres organismes, y compris les organismes d'exécution.

- Les Membres disposant de régulateurs de données devraient évaluer si les pouvoirs d'application existants sont suffisants.

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

5.3.4. Rééquilibrer l'écosystème juridique

Définition des problématiques

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

S'il est généralement admis que les données brutes ne sont protégées par aucun droit de propriété reconnu, des revendications ont été formulées sur les données en fonction des différents types de propriété intellectuelle : droits d'auteur, protection sui generis des bases de données, secrets commerciaux et brevets. Aucun de ces droits ne confère la propriété des données en tant que telles. La protection sui generis des bases de données est un droit propre à l'Union européenne, limité à l'Europe. Dans quelques pays de Common Law, le droit d'auteur a été étendu aux bases de données

et aux compilations de données, mais même ces pays ont des règles différentes, certains tribunaux étendant le droit d'auteur simplement pour l'effort de compilation, tandis que d'autres exigent de la créativité. Le droit d'auteur est destiné à récompenser les auteurs humains et son application aux bases de données compilées par des ordinateurs est indéterminée. Les litiges entre concurrents sur l'utilisation des bases de données standard de l'industrie chevauchent le droit d'auteur et le droit de la concurrence. Un jugement du tribunal sur (Discovery Ltd and Others c. Liberty Group Ltd ZAGPJHC 67, 2000) offre une solution qui respecte à la fois la protection des données et la concurrence : dans ces litiges, si les données sont de nature personnelle, elles sont la "propriété" de la personne concernée et les concurrents ne peuvent pas empêcher les autres d'accéder à ces informations. Alors que l'application des lois sur la propriété intellectuelle aux données est toujours en cours de résolution, les droits des personnes sur leurs données personnelles devraient être traités comme plus forts que toute revendication de propriété intellectuelle sur ces données, car la protection des données est si importante pour construire des économies des données.

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

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

Les États membres ont l'occasion de réinventer un système juridique harmonisé qui permette de concilier les intérêts divergents.

Recommandations

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

préciser qu'elles n'entravent généralement pas la circulation des données ou leur protection.

Actions

- Les contrats qui visent à renoncer aux droits numériques, à la protection des données à caractère personnel et qui entravent la concurrence devraient, en règle générale, être inapplicables. Cela peut être articulé dans la protection des données et la réglementation de la concurrence ;

- Les commissions nationales de réforme du droit ou des institutions juridiques expertes similaires devraient étudier et examiner comment harmoniser les différentes branches du droit, les régimes réglementaires et les organismes de contrôle qui traitent des données ;

- Les États membres devraient soutenir la mise à jour ou l'adoption de cadres et de réglementations en matière de droit de la concurrence qui prennent en compte les défis liés à l'analyse des questions de concurrence, à la conception de remèdes et à l'application de leurs pouvoirs pour préserver la concurrence sur les marchés axés sur les données, ainsi que le renforcement de la capacité des régulateurs de la concurrence à mettre en œuvre ces règles ;

- Les lois sur la propriété intellectuelle devraient être modifiées pour prévoir :

    - Que le droit d'auteur ne s'applique qu'aux bases de données et aux compilations de données d'auteurs humains qui font preuve d'originalité/créativité et que le droit d'auteur ne s'étend qu'à la sélection et à la disposition originales des données dans une base de données et non aux données elles-mêmes ;

    - Que tout droit d'auteur ou autre droit de propriété intellectuelle, y compris les secrets commerciaux, qui permet le contrôle des données ne s'applique pas aux données à caractère personnel ; et

    - Que tout droit d'auteur ou autre droit de propriété intellectuelle, y compris les secrets commerciaux, qui permet le contrôle des données est limité par les dispositions de la réglementation en matière de concurrence et des droits alternatifs qui offrent une protection aux innovations locales non envisagées dans les cadres actuels ;

    - Adaptation des régimes de DPI existants pour tirer parti des technologies de pointe, par exemple en permettant à l'IA d'utiliser des données.

5.3.3.6. Collaboration avec les processus de gouvernance régionaux et mondiaux

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

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

5.3.3.7. Une réglementation consultative et fondée sur des preuves

En vue d'exploiter l'expertise des parties prenantes, les réglementations devraient également être le résultat de processus consultatifs multipartites axés sur l'intérêt public. Elles devraient également être fondées sur des preuves et contextuelles. Des données administratives améliorées grâce à une meilleure collecte et analyse, et sur lesquelles les régulateurs peuvent prendre des décisions, amélioreraient considérablement la prise de décision au sein des organismes. Cela leur permettrait également d'offrir une plus grande certitude aux parties prenantes dans un cadre souple et adaptable, renforçant ainsi leur crédibilité (World Bank & ITU, 2020).

Recommandations

Lors de la création des dispositions institutionnelles, les États membres devraient clairement distinguer les rôles de l'État en tant que décideur politique et du régulateur, qui devrait être suffisamment indépendant de l'État et de l'industrie, afin de mettre en œuvre la politique dans l'intérêt du public et des fournisseurs de services et opérateurs de plateformes.

Les institutions de régulation doivent être établies sur la base des principes d'autonomie, de transparence et de responsabilité afin d'éviter l'emprise de l'État et des organismes de régulation. Les régulateurs devraient entreprendre des études d'impact réglementaire à un stade précoce de la réglementation afin de mettre en œuvre les meilleures approches qui concilient réglementation et croissance économique. Les régulateurs doivent publier les résultats de leurs efforts politiques et réglementaires afin d'améliorer les stratégies réglementaires dans tous les États, y compris les rapports sur la participation du public aux nouvelles réglementations. Les régulateurs doivent également être autofinancés ou financés par des crédits

parlementaires afin de garantir leur indépendance financière. Les décisions réglementaires doivent être fondées sur des données fiables et exploiter les connaissances du secteur privé et de la société civile par le biais de consultations publiques. Les régulateurs de la concurrence et du secteur doivent éviter une réglementation instrumentale de la concurrence, en adoptant des modèles d'efficacité dynamique plutôt que statique.

Actions

- Faire une distinction claire entre les rôles de l'État en tant que décideur politique et du régulateur, qui doit être suffisamment indépendant de l'État et de l'industrie, afin de mettre en œuvre la politique dans l'intérêt public ;

- Créer ou maintenir des organismes de concurrence pour faire face à la dominance sur le marché et à la concentration par le biais de fusions et d'acquisitions ;

- Mettre en œuvre des procédures claires de coresponsabilité entre les organismes sectoriels et les organismes de concurrence afin de garantir une réglementation coordonnée du secteur des infrastructures et des services numériques et d'éviter le "chalandage" ;

- Les régulateurs de données devraient collaborer au niveau régional et continental pour harmoniser leurs cadres, notamment à l'appui de la ZLECAf ; et

- Les personnes soumises aux décisions des organismes de réglementation devraient disposer de mécanismes clairs d'appel et de recours entendus par un organisme différent de l'organisme de réglementation, rendant les décisions conformes aux règles de justice naturelle et d'action administrative équitable.

5.3.5. Création de valeur publique

Définition des problématiques

Disposer de données sans capacité humaine, sans contrôle suffisant ou sans incitation à la valeur ajoutée revient à ne pas en avoir. Ces contraintes s'appliquent à de nombreux pays africains. Il est également difficile de favoriser un secteur public axé sur les données. La valorisation des données dépend fortement des cadres réglementaires et politiques habilitants qui facilitent l'obtention de données utiles, le renforcement des capacités humaines, institutionnelles et techniques pour créer de la valeur à partir des données, l'encouragement du partage des données et de l'interopérabilité, et le renforcement de la légitimité et de la confiance du public au sein de l'État pour gérer les données des citoyens de manière responsable. En outre, l'infrastructure de données qui permet la mise en place d'un système de données intégré est un atout stratégique essentiel pour les pays. Le climat créé par l'interaction

des éléments de l'écosystème des données et la nature des relations et des processus non linéaires entre eux et en leur sein, déterminent les interventions visant à créer des incitations pour les investissements technologiques qui sont nécessaires pour stimuler la croissance de l'économie des données. Ces conditions sont façonnées par la structure du marché, la compétitivité des services qui en découlent et l'efficacité de la réglementation du marché.

5.3.3.8. Capacité du secteur public

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

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

5.3.3.9. Conservation des données publiques

Le secteur public est mandaté pour gérer les données clés du développement économique. Il s'agit notamment de données statistiques et d'indicateurs économiques utilisés pour l'établissement de rapports avec les institutions multilatérales, ainsi que de données administratives, telles que les identités numériques. Ces données sont souvent anonymisées et combinées avec d'autres données dans divers cas d'utilisation allant de l'hyperpersonnalisation commerciale, comme la solvabilité, à l'intérêt public pour les subventions sociales et la gestion des catastrophes.

Dans le secteur public, les données sont souvent utilisées pour améliorer le contrat social et atténuer les asymétries d'information dans l'élaboration des politiques, le suivi de l'impact des interventions et la prestation de services, notamment pour décider de l'affectation des ressources publiques. Les données publiques anonymisées peuvent

être combinées avec d'autres ensembles de données à des fins commerciales pour réduire les coûts d'entrée sur le marché, perturber les industries, améliorer l'efficacité et faciliter le développement d'innovations, de produits, d'informations et d'opportunités qui peuvent être disponibles en ligne, sans les limites des frontières géographiques et physiques. Toutefois, les institutions qui conservent les données publiques sont confrontées à divers défis qui sont examinés ci-dessous.

5.3.3.10. Garantir la qualité et la pertinence des données du secteur public

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

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

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

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

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

Actions

- Les organismes de réglementation du secteur et les responsables des données publiques doivent opérer dans le cadre de lignes directrices spécifiques sur la manière dont les évaluations de la qualité des données doivent être mises en œuvre, en fonction des cas d'utilisation communs, des algorithmes et du type de données utilisées, ces lignes directrices peuvent s'inspirer des meilleures pratiques mondiales (notamment la gouvernance des données et de l'IA), mais doivent être adaptées au contexte des cas d'utilisation des données africaines. En raison de l'échange, des combinaisons, du stockage stratégique et de la réaffectation, nécessaires pour créer une valeur des données. Une stratégie efficace de qualité des données dans l'ensemble du secteur public devrait être informée par les réalités techniques/pratiques/opérationnelles et devrait décrire les rôles, les responsabilités et les mandats des différentes entités gouvernementales dans la collecte et le maintien de données de haute qualité d'une manière qui protège les citoyens.

- Les États membres doivent participer aux efforts visant à établir et à adopter un cadre normatif pour des normes et des systèmes des données harmonisés visant à établir une interopérabilité nationale, régionale et internationale. Il peut s'agir d'interventions ciblées en matière de formation humaine, technique et institutionnelle, de projets

d'infrastructure sous-régionaux et de bacs à sable réglementaires des CER.

- Une approche continentale facilite les économies d'échelle pour inciter les investissements privés dans les infrastructures numériques fondamentales, y compris les technologies basées sur le cloud. L'harmonisation régionale des réglementations relatives à la gouvernance des données pourrait réduire davantage les coûts de mise en conformité et réduire l'incertitude et le risque opérationnel pour les investissements majeurs dans les infrastructures liées aux TIC.

- Les institutions publiques qui conservent les données devraient disposer de ressources adéquates afin de contribuer aux forums multilatéraux concernant les données et d'être les responsables de l'accès inclusif et de l'utilisation responsable des données guidés par les normes techniques et réglementaires appropriées de l'industrie, les standards et les meilleures pratiques- qui sous-tendent à la fois les caractéristiques informationnelles et économiques des données dans les industries prioritaires.

5.3.6. Des politiques sectorielles cohérentes pour valoriser les données

Définition des problématiques

Les politiques en matière de concurrence, de commerce et de fiscalité sont étroitement liées. Des économies de données locales compétitives, par exemple, peuvent accroître les services fondés sur les données et l'ouverture commerciale peut stimuler le commerce numérique international et les investissements directs étrangers (IDE) sur les économies de données nationales. Toutefois, cela peut également renforcer la domination des oligopoles mondiaux sur les écosystèmes de données nationaux, créant ainsi des tensions commerciales liées aux flux de données transfrontaliers.

Simultanément, les modèles commerciaux numériques axés sur les données peuvent miner la concurrence nationale et renforcer la concentration du marché, car les autorités fiscales ont du mal à quantifier, évaluer, établir et suivre les chaînes de valeur numériques en raison de caractéristiques telles que les vendeurs tiers et l'absence de présence physique comme base pour établir la responsabilité fiscale des entreprises dans le secteur axé sur les données.

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

5.3.3.11. Politique de concurrence

Définition des problématiques

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

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

5.3.3.12. Politique commerciale

Définition des problématiques

Les systèmes numériques ne fonctionnent plus dans le cadre de juridictions nationales clairement définies. Une réforme de la politique commerciale est nécessaire pour faire face à l'augmentation du commerce numérique et du commerce électronique. Les différentes influences géopolitiques, les dotations et les capacités institutionnelles et humaines sur le continent peuvent affecter les approches unilatérales du commerce numérique et les efforts d'harmonisation régionale. La stratégie transfrontalière en matière de données adoptée au niveau national nécessitera des capacités institutionnelles différentes, elle ne pourra être efficace que sur la base des dotations de l'écosystème de données existant, elle influencera la manière dont la valeur des données sera créée ou extraite au sein des pays africains et entre eux, et déterminera qui bénéficiera le plus du cycle de valeur des données au niveau national et régional.

Commerce des services, flux de données transfrontaliers et localisation

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

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

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

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

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

Trois approches stylisées pour régir les flux de données transfrontaliers

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

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

Commerce électronique

Les plateformes de commerce électronique permettent aux consommateurs de bénéficier d'une plus grande variété de choix à des prix plus compétitifs. Les stratégies visant à améliorer le commerce électronique ne peuvent pas être formulées isolément, car le commerce électronique est lié à une multitude d'autres questions, notamment l'identification numérique, la gouvernance des données, les droits de douane, les flux

de données transfrontaliers, la cybersécurité, l'interopérabilité des systèmes de paiement, la protection des consommateurs, la concurrence, la fiscalité et les normes, pour n'en citer que quelques-unes. En outre, pour améliorer l'adoption du commerce électronique, il faut tenir compte de facteurs tels que la pénétration de l'internet, la fiabilité des services postaux, l'utilisation des services de paiement (comptes bancaires ou argent mobile) et la sécurité des serveurs internet. Pour les États membres, une action collective par le biais d'une approche unifiée aura plus de chances de fournir de meilleurs résultats qui tiennent compte des contextes africains lorsqu'il s'agit de relever des défis qui se chevauchent et qui affectent différents mandats gouvernementaux sur les marchés des données dans les forums multilatéraux.

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

Recommandations

- Pour favoriser des marchés de données compétitifs, sûrs, dignes de confiance et accessibles, les responsables de la concurrence doivent trouver des moyens coordonnés et efficaces de réglementer la concentration des marchés de données tout en préservant les avantages qu'ils offrent dans le contexte des différents besoins de développement sur le continent. Cela inclut une réglementation ex ante des problèmes de concurrence avant qu'ils ne s'aggravent sur le marché.

- Les décideurs politiques en matière de fiscalité, de concurrence et de commerce devront renforcer les capacités humaines et techniques pour traiter les questions émergentes au-delà du mandat sectoriel traditionnel qui peuvent affecter les marchés de données ;

- Les États membres doivent promouvoir la prévisibilité et la convergence des régimes dans les domaines d'action complémentaires, de manière à ce qu'ils se renforcent mutuellement. Cela doit être fait pour naviguer dans l'émergence de nouveaux modèles commerciaux dynamiques axés sur les données qui peuvent favoriser le commerce numérique intra-africain et l'entrepreneuriat axé sur les données. Dans le même temps, les décideurs politiques devraient tenir compte des liens bidirectionnels entre les résultats économiques et la gouvernance des données et peser soigneusement les compromis.

- Les États membres devraient favoriser une approche régionale coordonnée, globale et harmonisée des défis de gouvernance mondiale associés à l'économie numérique mondiale axée sur les données, tels que:

    - La collaboration transfrontalière pour la mise en œuvre d'instruments de politique de la concurrence visant à lutter contre les comportements anticoncurrentiels sur les marchés numériques axés sur les données ;

    - L'encouragement de la portabilité des données par la réglementation et d'autres activités habilitantes ;

    - Les efforts de l'Organisation de coopération et de développement économiques (OCDE) pour prévenir l'évasion fiscale en ce qui concerne les entreprises axées sur les données ;

    - Les accords de l'Organisation mondiale du commerce (OMC) sur les services fondés sur les données et le commerce électronique ;

    - La mise en place d'une infrastructure régionale coordonnée de données de base et d'initiatives de développement de systèmes de données numériques ; renforcer les capacités humaines, techniques et institutionnelles pour soutenir l'interopérabilité des données, la création de valeur et la participation équitable aux économies de données ;

    - Le renforcement des capacités humaines, techniques et institutionnelles pour soutenir l'interopérabilité des données, la création de valeur et la participation équitable aux marchés des données ;

    - La contribution à l'harmonisation internationale des normes techniques, de l'éthique, de la gouvernance et des meilleures pratiques en matière de données, d'analyse des données massives et d'intelligence artificielle.

Actions

- Les États membres devraient encourager une réforme et une expérimentation dynamiques des politiques et des réglementations (par exemple, des bacs à sable réglementaires au niveau de l'industrie et des CER);

- Les décideurs politiques doivent tenir compte des liens bidirectionnels entre les résultats économiques et la gouvernance des données et peser soigneusement les compromis. Les différentes entités étatiques doivent s'efforcer d'établir des cadres de partage de données sûrs et responsables qui facilitent la demande de données, l'interopérabilité des

données, les flux de données transfrontaliers, les chaînes de valeur des données, ainsi que les normes et systèmes de données ouverts dans les secteurs prioritaires clés attribués par la STN;

- Pour que l'utilisation des données soit efficace, inclusive et innovante, il faudra une collaboration entre les institutions de régulation à travers différents mandats et une régulation coordonnée du marché (dans des domaines politiques interdépendants tels que les télécommunications, les finances, la concurrence, le commerce, la fiscalité et la réglementation des données);

- Les autorités de la concurrence ou les institutions connexes devront renforcer leurs capacités humaines et techniques pour traiter les problèmes de concurrence émergents, au-delà de la concentration du marché, qui peuvent affecter les marchés axés sur les données ;

- Les outils traditionnels de la concurrence, tels que les lignes directrices sur la définition des marchés, l'évaluation de la position dominante, les pratiques anticoncurrentielles (par exemple, l'abus de position dominante, les pratiques coordonnées et l'abus de puissance d'achat), les lignes directrices sur l'évaluation des fusions, ainsi que les théories du préjudice et la conception des remèdes, devront être adaptés pour intégrer le dynamisme des données et les caractéristiques des entreprises axées sur les données;

- Les signataires de la ZLECAf devront déterminer la manière dont le protocole sur le commerce électronique fonctionnera parallèlement aux lois et politiques existantes, et devra rendre compte et soutenir les objectifs des autres protocoles tels que la politique d'investissement, de propriété intellectuelle et de concurrence (à négocier en phase II) ; et

- Développer et renforcer les mécanisms de dialogue public-privé pour améliorer l'élaboration des politiques liées au commerce électronique.

5.3.3.13. Politique fiscale

Définition des problématiques

Une incohérence existe entre la taxation actuelle des bénéfices des plateformes mondiales et la manière dont la valeur est créée à partir des données dans le secteur de l'économie numérique. En Afrique, la plupart des pays sont principalement des marchés de données pour les plateformes mondiales, les utilisateurs contribuant de manière appréciable à la génération des bénéfices des plateformes, sans mécanisme plausible de captation de la valeur. Actuellement, le trafic de données en Afrique augmente à un taux annuel de 41% (CNUCED, 2019), ce qui implique une plus grande utilisation et adoption des services fournis par les plateformes numériques mondiales dans la région. Bien que les institutions multilatérales se soient engagées, principalement sous l'impulsion du Cadre inclusif de l'OCDE sur L'érosion de la base d'imposition et le transfert de bénéfices (BEPS) (bien qu'il ne soit pas totalement

inclusif pour l'Afrique puisque seuls 23 pays y participent), un consensus mondial n'a pas été atteint pour les différentes options proposées (Piliers 1 et 2) en matière de fiscalité numérique.

Plusieurs pays africains, réticents à retarder la taxation des services numériques ou non conscients des avantages pour leur pays des réformes internationales, mettent déjà en œuvre des mécanismes unilatéraux. Il s'agit notamment de taxes sur les services numériques et de prélèvements de péréquation fondés sur des données économiques significatives (données) afin de saisir une partie de la valeur des données en taxant certaines parties de l'économie numérique au sein de leurs juridictions. Ces mécanismes comprennent également l'extension de la taxation sectorielle sur l'industrie des télécommunications et la taxation des transactions d'argent mobile et de l'utilisation de certaines applications de communication over-the-top (OTT) dans la région, telles que WhatsApp, Facebook, Twitter, Skype et Instagram. Si ces taxes visent à augmenter les recettes publiques, leur impact négatif sur les consommateurs a ralenti l'accès et l'inclusion numériques (en raison du déplacement des coûts pour les consommateurs) et a restreint le droit à la liberté d'expression des citoyens. Du côté de l'offre, l'augmentation des taxes sur le secteur des télécommunications a un impact négatif sur les bénéfices des opérateurs du secteur résident (avec des implications négatives conséquentes pour les investissements en infrastructures dont le besoin est crucial au sein de la région aux ressources limitées), tandis que les OTT fondés sur les données sont largement non taxés localement (CTO 2020, ICTD 2020, RIA 2021, (CTO, 2020)).

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

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

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

Recommandations

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

Actions

- Les États membres doivent soutenir l'harmonisation du régime fiscal des biens et services numériques au niveau régional, et l'alignement au niveau mondial, qui atténueraient les risques liés au fait que les petits marchés des économies de données ne sont pas en mesure de générer une valeur significative et d'être compétitifs sur les marchés mondiaux pour contribuer à l'échelle et à la portée nécessaires à la création de valeur axée sur les données et à des bases fiscales généralement limitées.

- De manière complémentaire, un fonds de données publiques coalisé par les pays membres de l'UA pourrait être mis en place en collaboration avec le secteur privé pour construire l'infrastructure nécessaire à l'extraction de ces données de transaction, où les données peuvent être conservées dans le cadre d'un fonds commun de données régionales au-delà du seul domaine de la fiscalité.

- La facilitation d'un fonds de données publiques exigera des pays africains de numériser leurs systèmes d'administration fiscale pour permettre une évaluation et un recouvrement plus efficaces des taxes des plateformes numériques. Un système administratif fiscal numérique renforcera la capacité d'enregistrement des impôts, le partage des données de transaction avec les autorités fiscales nationales et l'échange d'informations sur les obligations fiscales auprès des

plateformes numériques à des fins de conformité, tout en réduisant les coûts opérationnels.

Les États membres devraient saisir l'occasion de la coordination de la taxation des services numériques pour un marché numérique unique pour exploiter de nouvelles sources de recettes fiscales qui pourraient leur permettre de supprimer les droits d'accises régressifs et fiscalement contre-productifs sur les réseaux sociaux et les services de données et, de réduire les distorsions tant sur le marché local que dans le système fiscal mondial.

5.4. Gouvernance des données

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

5.4.1. Contrôle des données

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

5.3.3.14. Souveraineté des données

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

favorise une approche dirigée par l'État qui met l'accent sur la sauvegarde de la sécurité nationale (Wright & Polatin-Reuben, 2014).

5.3.3.15. Localisation des données

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

Définition des problématiques

Alors que la localisation des données est souvent considérée comme une expression de la souveraineté des États, en tant qu'option politique possible, la localisation des données doit être évaluée sur une base coût-bénéfice. Ce choix politique peut présenter un défi pratique. Si la localisation des données est parfois motivée par la nécessité de protéger les personnes concernées, elle peut être appliquée à des données à caractère non personnel. C'est pourquoi il est essentiel que la localisation des données soit lue dans le contexte du contrôle, afin de souligner sur le plan politique l'importance des mécanismes de soutien qui peuvent faciliter l'acte de souveraineté. La localisation des données implique l'érection artificielle de barrières législatives aux flux de données, notamment par le biais d'exigences de résidence des données et de stockage local obligatoire des données (Cory, 2017). Des règles strictes de localisation des données exigeant le stockage de toutes les données localement, et pas seulement une copie, rendent ces données sensibles aux menaces de sécurité, notamment aux cyberattaques et à la surveillance étrangère.

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

Recommandations

- Les États membres doivent privilégier les partenariats politiquement neutres qui tiennent compte de leur souveraineté individuelle et de la propriété nationale afin d'éviter les ingérences étrangères susceptibles

d'affecter négativement la sécurité nationale, les intérêts économiques et les développements numériques des États membres de l'UA.

- Les États membres de l'UA ont le droit de formuler des règles relatives au numérique et aux données en fonction de leurs priorités et de leurs intérêts notamment pour protéger la sécurité des informations de l'État et de ses citoyens, et pour empêcher des tiers d'exploiter injustement les ressources et les marchés locaux.

- Des accords bilatéraux et multilatéraux doivent être établis pour exercer la souveraineté et le contrôle nationaux, et des voies de recours en cas d'infraction sont nécessaires.

- La localisation doit être évaluée au regard des préjudices potentiels pour les droits de l'homme.

- Les exigences en matière de localisation des données nécessitent une spécificité des données. Les solutions de localisation des données ont été fortement articulées au sein de silos de données sectoriels (verticaux) dans différentes juridictions ; par exemple, le Nigeria instituant certaines formes de localisation des données financières, l'Australie prescrivant des formes de localisation des données de santé, etc. Il s'agit d'un domaine dans lequel la spécificité est fortement requise, à la fois pour faciliter des flux plus larges dans la mesure où cela est propice à des impératifs politiques tels que la zone de libre-échange africaine, mais aussi pour la clarté qui peut aider à minimiser les coûts pour les entreprises et les innovateurs locaux et réduire les risques de conséquences involontaires.

- Le développement d'une infrastructure de données devrait être exploré en tant que mécanisme permettant d'exercer un contrôle, mais doit être contextualisé en tenant compte des impacts environnementaux, des infrastructures de sûreté et de sécurité, des coûts dupliqués pour les communautés de données locales et des coûts globaux.

- Les capacités du secteur public devraient être investies pour informer les initiatives nationales et efficaces de contrôle des données.

- Les droits des personnes concernées devraient être conçus et prévoir expressément un contrôle efficace des données personnelles. Les trusts et les gestions de données devraient être explorés comme une autre forme de contrôle efficace des données personnelles (et d'autres données).

Actions

- Les autorités chargées de la protection des données (DPA) doivent être pleinement habilitées, notamment en ce qui concerne la souveraineté des données ;

- Les APD sont encouragées à adopter des pratiques de coopération internationale et régionale en prenant note des différents stades de mise en œuvre et d'application dans les États membres ;

- L'évaluation des risques et l'engagement de plusieurs parties prenantes devraient être utilisés pour concevoir des solutions de localisation des données dans la politique par les rédacteurs, qui inclut la participation de la société civile ;La politique en matière d'infrastructure de données doit être alignée sur les impératifs de contrôle des données par les rédacteurs de la politique, mais doit tenir compte de la cybersécurité, de la protection des données personnelles, des risques environnementaux et du coût

- L'administration publique et la politique d'investissement devraient s'aligner sur les capacités de contrôle des données en priorité ;

- Le renforcement des capacités en matière de protection des données, de cybersécurité et de gouvernance des données institutionnelles dans les organismes concernés devrait être assuré par la politique et l'allocation des actifs.

Mécanismes permettant d'exercer un contrôle sur les données
Il existe des mécanismes permettant d'exercer un contrôle sur les données, comme les fiducies de données. Les fiducies de données et/ou les gestions de données sont des formes alternatives de solutions de gouvernance discrètes dans le contexte des données. Une fiducie légale est un instrument juridique utilisé pour gérer des biens, tant corporels qu'incorporels. Une fiducie permet à une personne de détenir des actifs (dont elle n'est pas propriétaire) au profit des bénéficiaires de la fiducie. La personne qui détient les actifs a été autorisée à le faire et doit aux bénéficiaires de ce fiducie une obligation fiduciaire d'agir de manière responsable dans la gestion de leurs actifs. Cette structure juridique traditionnelle a été posée comme un moyen de gérer des collections de données pour le compte de groupes et de faciliter le partage de données en masse dans des situations où les modèles de licence ou de données ouvertes risquent de ne pas être réalisables, comme un moyen de favoriser l'innovation en facilitant un accès équitable (Stalla-Bourdillon et al., 2019).
L'Open Data Institute définit les fiducies de données comme fournissant "...une gérance indépendante et fiduciaire des données" (Open Data Institute, 2018). L'ajout de l'élément fiduciaire à la définition (par opposition à la simple définition comme une forme de fiducie légale) a été fait car il s'agit d'un élément essentiel de responsabilité et d'obligation, qui constitue un fondement important du concept (Open Data Institute, 2020). En outre, elle peut inclure des solutions de protection de la vie privée par conception dans l'architecture de tout mécanisme conçu pour faciliter la confiance, donc dans la garantie de la vie privée en substance et en processus (Stalla-Bourdillon et al., 2019). Alors que les lois sur la protection des données peuvent créer des normes sur la façon dont les données d'une personne peuvent ou ne peuvent pas être traitées, en dehors du consentement ou du recours en cas de violation, les mécanismes permettant aux personnes d'agir sur leurs données sont limités - ainsi, les fiducies de données aident à faciliter la réalisation du contrôle des données. Les fiducies de données offrent aux personnes concernées un mécanisme par lequel elles peuvent fournir (ou "partager") leurs données, tout en leur retirant la responsabilité exclusive de "garantir" le respect de la protection des données par les acteurs des secteurs public et privé grâce à l'établissement d'une relation fiduciaire.

5.4.1. Traitement et protection des données

Définition des problématiques

Alors que les principes de contrôle des données permettent de délimiter et de définir les obligations relatives aux données à caractère personnel et non personnel, le traitement des données vise à définir les orientations politiques pour le traitement des données à caractère personnel, comme nous l'avons vu précédemment. La réglementation des données à caractère non personnel est déterminée par la catégorisation des données et les régimes d'accès spécifiques. Ces formes d'orientation sont importantes en tant que mécanisme permettant de réaliser la protection de la vie privée et des données. Le traitement des données à caractère personnel représente un élément essentiel de la gouvernance des données et de la création d'un environnement de confiance. L'instauration de la confiance est considérée comme un élément nécessaire à la promotion d'une économie numérique et de données saine. En restreignant les limitations de processus aux données à caractère personnel, ces contraintes ne doivent pas nécessairement entraver les flux de données pour le commerce numérique ; mais pour assurer cette absence d'entrave, il est nécessaire d'avoir des politiques de données cohérentes dans toute la région, reposant sur des principes communs, mais flexibles (Nations unies, 2017).

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

Les techniques de désidentification, y compris l'anonymisation et la pseudonymisation, peuvent faciliter certaines utilisations des données tout en

assurant une protection au moins partielle des données. La pseudonymisation peut être réalisée par l'utilisation d'un signifiant ou d'un masque qui ne peut être relié à une personne identifiable que par des données supplémentaires. Si l'anonymisation et la pseudonymisation peuvent permettre aux prestataires de services privés et au secteur public de faire un meilleur usage des données, elles dépendent de l'état actuel de la technologie et des mathématiques. Au fur et à mesure que de nouvelles approches mathématiques sont développées et que la puissance de traitement des ordinateurs augmente, des données considérées comme dépersonnalisées peuvent devenir identifiables. Bien que les réglementations en matière de protection des données exigent souvent la désidentification, ces techniques sont insuffisantes si les personnes concernées ne disposent pas de droits juridiques solides et si le régulateur n'a pas la capacité de faire respecter la protection des données.

Recommandations

- Il est nécessaire d'établir des APD qui soient indépendants, financés et efficaces. De plus, en tant que méthode pour garantir l'efficacité, les paramètres de responsabilité sont cruciaux pour aider une APD à avoir un champ d'action clair. Il faut établir des cadres de traitement légal des données qui prévoient des sanctions dissuasives claires pour assurer la conformité. Ils doivent couvrir tous les acteurs pertinents du traitement des données.

- L'évaluation des risques liés aux données à caractère personnel doit être obligatoire lors du déploiement du développement technologique des données à caractère personnel.

- Un sous-principe important, qui doit être mis en action avec des cadres de traitement des données pour les acteurs publics et privés, est celui de la minimisation. La minimisation de la collecte des données à caractère personnel est l'un des mécanismes les plus efficaces pour atténuer les risques et les préjudices des personnes concernées.

- Il convient d'explorer les codes de conduite pour promouvoir les données et les besoins spécifiques du secteur. Ces codes, approuvés par l'APD concernée, peuvent fournir une expertise sectorielle et industrielle dans la gestion des risques et préjudices réels qui peuvent être associés au traitement, et garantir les meilleures pratiques dans la gestion de ces préjudices. Ils peuvent également contribuer à l'examen des exceptions sectorielles qui peuvent être nécessaires pour qu'une économie des données constructive puisse prospérer, tout en s'inscrivant dans un programme de développement durable plus large, par exemple en facilitant la recherche (dans le domaine de la santé ou dans d'autres domaines du développement social).

Actions

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

- Les APD devraient être établies de toute urgence parallèlement aux législations nationales sur la protection des données à caractère personnel.

5.4.2. Accès aux données et interopérabilité

Définition des problématiques

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

Recommandations

- Les normes de données ouvertes devraient être prioritaires dans la création et la maintenance des données publiques. La création des données selon ces normes n'exclut pas la mise en place de mécanismes de contrôle ou de limitation de l'accès dans des catégories des données définies à des fins impératives. La portabilité des données doit être soutenue. La portabilité des données peut être une forme de droit de la personne concernée, défini comme le droit de la personne concernée d'obtenir les données qu'un responsable du traitement détient sur elle, dans un format structuré, couramment utilisé et lisible par machine, et de les réutiliser à ses propres fins. La portabilité peut être facilitée par une politique de portabilité des données dans le secteur public, et par

l'établissement de droits spécifiques de portabilité des données dans les contextes de consommation. Les partenariats de données (y compris les options telles que les banques de données) doivent être privilégiés en tant que mécanismes permettant de faire progresser les données ouvertes de qualité et préservant la vie privée.

- Pour tenter de faciliter la spécificité, la catégorisation des données peut être une méthode permettant d'assurer la cohésion des cadres de traitement des données au sein des allocations relatives au traitement, et des principes de sécurité. La catégorisation à laquelle il est fait référence dans ce cas n'est pas telle que les typologies sectorielles considérées de manière plus large, mais plutôt comme un mécanisme spécifique pour réaliser des formes particulières de risques qui s'alignent sur les types de données et d'informations, et pourraient inclure des catégories sensibles (comme les données des enfants), des classifications de sécurité pertinentes, par rapport aux formes de données déjà dans le domaine public.

- Les restrictions sur le traitement doivent être clairement articulées et limitées, afin de ne pas interférer avec le traitement à faible risque qui pourrait être de plus en plus essentiel à la formation de l'IA par le traitement de données à grande échelle.

Actions

- Les États membres devraient mettre en place une politique d'ouverture des données qui fixe des normes ouvertes pour la production et le traitement des données, de sorte que lorsque la décision d'ouvrir les données est prise, les coûts élevés pour s'assurer qu'elles sont utilisables et manipulables soient évités. Les lois sectorielles et les codes de conduite des APD devraient être examinés pour garantir un accès légal aux données, conjointement avec la politique en matière de données ;

- Les APD devraient avoir une double fonction d'accès à l'information et de protection de la vie privée ;

- Des initiatives multisectorielles d'ouverture des données devraient être mises en œuvre sur des secteurs de données prioritaires comme la santé, la recherche et la planification.

5.4.3. Sécurité des données

Définition des problématiques

La sécurité des données comprend l'ensemble des politiques, normes, règlements, législations et pratiques visant à protéger la confidentialité, l'intégrité et la disponibilité des données contre les accès non autorisés, la corruption ou le vol, tout au long du cycle de vie des données. Ces principes fondamentaux de la sécurité des données

définissent également les trois principaux domaines de responsabilité de la sécurité de l'information. Le concept de sécurité des données englobe de nombreux aspects, de la sécurité physique du matériel des centres de données et des dispositifs de stockage aux contrôles d'accès administratifs, en passant par la sécurité logique des réseaux, des logiciels et des applications. Il inclut également les procédures et politiques organisationnelles.

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

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

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

Recommandations

- **Les États membres devraient élaborer des politiques nationales de cybersécurité ainsi que les mesures juridiques et techniques nécessaires pour soutenir la confiance dans leur espace numérique.**

- Les États membres sont encouragés à coopérer au niveau régional pour élaborer des normes de cybersécurité à respecter dans les secteurs public et privé afin d'accroître la croissance économique régionale.

- Les politiques en matière de données devraient s'aligner sur les politiques de cybersécurité et de cybercriminalité, et la législation traitant de la cybercriminalité devrait respecter les droits de l'homme.

- Un régime de sanctions commun pour les cyberattaques devrait être établi.

Actions

- Les États membres, qui n'ont pas encore entrepris des mesures de cybersecurité, devraient immédiatement élaborer des plans de cybersécurité et les rationaliser au sein des structures de gouvernance publiques afin de promouvoir la solidité et de réduire les vulnérabilités.

- Les institutions de cybersécurité telles que les équipes de réponse aux incidents de sécurité informatique (CSIRT) devraient être intégrées dans l'élaboration des politiques en matière de données.

- Les rôles de traitement des données en tant que forme de protection de la sécurité devraient être spécifiés en matière de politique par les décideurs.

- Le renforcement des capacités en matière de protection des données, de cybersécurité et de gouvernance institutionnelle des données dans les organismes concernés devrait être assuré par le biais des politiques et de l'allocation des ressources, et pourrait être soutenu par les APD.

5.4.4. Flux de données transfrontaliers

Une question de plus en plus importante concernant le commerce international et régional est le transfert transfrontalier de données à caractère personnel et autres (Deloitte, 2016). Dans le contexte africain, les cadres internationaux et régionaux qui facilitent les transactions transfrontalières et le flux de données à caractère personnel entre les pays sont essentiels pour la création de marchés communs et notamment pour la réalisation de l'Accord de libre-échange africain. Le transfert transfrontalier de données à caractère personnel, en particulier, est façonné par l'approche de la souveraineté des données qu'un pays souhaite poursuivre, qui renvoie au principe

juridique selon lequel les informations (généralement sous forme électronique) sont réglementées ou régies par le régime juridique du pays dans lequel ces données résident. Comme indiqué, ce concept est remis en question par la réalité moderne des mouvements de données. Il convient toutefois de reconnaître les critiques du prétendu récit des "flux de données" et l'étendue de ses avantages pour les dividendes numériques dans le développement (Gurumurthy et al., 2017), ainsi que le fait que des quantités importantes de flux de données se produisent en fait horizontalement au sein des entreprises, plutôt qu'entre elles.

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

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

Recommandations

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

transfrontaliers, et identifier l'entité et les personnes africaines habilitées à gérer ce système.

Actions

- Les APD devraient établir des normes minimales pour le transfert de données ;

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

5.4.5. Demande des données

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

Recommandations

- Les communautés de données devraient être considérées comme prioritaires dans la politique d'innovation. Ces communautés nécessitent des incitations et un soutien de la politique nationale, y compris la promotion active des pôles de données et d'autres formes d'innovation communautaire qui peuvent contribuer à engendrer des compétences et des cultures de données ;

- Les dispositions réglementaires relatives à la gestion des données devraient prévoir des bacs à sable réglementaires pour encourager le développement local des données.

Actions

- Les communautés de données devraient être intégrées dans les processus d'élaboration des politiques de données par les décideurs politiques ;

- Les communautés de données devraient être associées à la mise en place d'initiatives de données publiques ouvertes par les responsables ministériels de la mise en œuvre ; et

- Les universités devraient être incluses en tant qu'acteurs politiques pertinents pour aider à établir la "base de connaissances" dans laquelle l'économie locale des données peut puiser des connaissances scientifiques et technologiques suffisantes.

5.4.6. Gouvernance des données pour les secteurs et les catégories spéciales des données

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

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

Recommandations

- Les états membres devraient éviter les régimes de données spéciaux qui ne sont pas intégrés aux régimes de données nationaux et qui n'intègrent pas les principes de bonne gouvernance des données.

- Les mécanismes et les politiques de gouvernance devraient permettre le développement d'une gouvernance des données par catégorie et par secteur pour les données relatives aux enfants, les données relatives à la santé et d'autres types de données sensibles ou de données spécifiques à un secteur qui justifient un traitement distinct par le biais de processus conformes aux principes du cadre.

5.5. Gouvernance internationale et régionale

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

Certaines initiatives internationales et continentales servent d'étape fondatrice pour précipiter la mise en œuvre.

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

Recommandations :

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

- Faciliter la collaboration entre les différentes entités traitant des données à travers le continent par la mise en place d'un cadre de consultation au sein de la communauté de l'écosystème numérique afin de préserver l'intérêt de chaque acteur.

- Renforcer les liens avec les autres régions et coordonner les positions communes de l'Afrique sur les négociations internationales liées aux données afin de garantir l'égalité des chances dans l'économie numérique mondiale.

- Soutenir le développement d'infrastructures de données régionales et continentales pour accueillir des technologies avancées axées sur les données (telles que les données massives, l'apprentissage automatique et l'intelligence artificielle) ainsi que l'environnement favorable et le mécanisme de partage des données nécessaires pour assurer la circulation à travers le continent ;

5.5.1. Normes des données continentales

Pour faciliter la coopération transfrontalière, il est important de parvenir à un consensus sur les normes de données, ce qui fait partie intégrante de la promotion de l'interopérabilité. Ces formes de consensus multipartites devraient faire référence au

travail effectué par l'Organisation internationale de normalisation et à d'autres formes de consensus international obtenues dans des contextes sectoriels spécifiques. Toutefois, si la normalisation internationale est importante pour la compétitivité, il convient de noter que ces normes internationales peuvent ne pas être suffisantes pour les besoins de la région. Ceci est démontré, par exemple, dans les défis linguistiques rencontrés dans le contexte des données spatiales ou géographiques.

Recommandations

- Le consensus sur les normes de données devrait faire référence aux travaux de l'Organisation internationale de normalisation, entre autres forums pertinents ;

- Les normes doivent toutefois être établies avec des réflexions spécifiques sur les facteurs contextuels ayant un impact sur le continent.

Actions

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

5.5.2. Portail de données ouvertes et autres initiatives

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

5.5.3. Instruments continentaux

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

5.3.3.16. Mécanisme de flux de données transfrontalier

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

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

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

Accord de libre-échange continental africain

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

Recommandations

- Encourager et faciliter les flux de données au sein des États membres de l'UA et entre eux en élaborant un mécanisme de flux de données transfrontaliers qui tienne compte du contexte africain, à savoir les différents niveaux de préparation au numérique, la maturité des données ainsi que les environnements juridiques et réglementaires.

- Faciliter la circulation des données entre les secteurs et au-delà des frontières en élaborant un cadre commun de catégorisation et de partage des données qui tienne compte des grands types de données et de leurs différents niveaux de confidentialité et de sécurité.

- Travailler en étroite collaboration avec les autorités nationales chargées de la protection des données personnelles des États membres de l'UA, avec le soutien du Réseau africain des autorités (RAPDP), afin d'établir un mécanisme et un organe de coordination qui supervisent le transfert des données personnelles au sein du continent et assure la conformité avec les lois et règles en matière de sécurité des données et des informations en vigueur dans les états membres de l'UA . . ;

- Permettre le partage des données et l'amélioration de l'interopérabilité entre les États membres de l'UA et d'autres mécanismes de l'UA, notamment le mécanisme de coopération policière de l'Union africaine (AFRIPOL).

- Œuvrer à la création d'un cyberespace sûr et résilient sur le continent, qui offre de nouvelles opportunités économiques, par l'élaboration d'une stratégie de cybersécurité de l'UA et la création de centres opérationnels de cybersécurité afin d'atténuer les risques et les menaces liés aux cyberattaques, aux violations de données et à l'utilisation abusive d'informations sensibles.

- Mettre en place des mécanismes et des institutions, ou renforcer ceux qui existent déjà, au sein de l'Union africaine, afin de renforcer les capacités et de fournir une assistance technique aux États membres de l'Union africaine en vue de l'incorporation au niveau national de ce cadre politique en matière de données.

- Il est recommandé que les négociations de la ZLECAf sur le chapitre de la concurrence établisse des normes minimales pour garantir que les données à caractère non personnel putativement exclusives soient accessibles aux innovateurs, aux entrepreneurs et aux autres acteurs de la chaîne de valeur afin d'encourager la concurrence sur le continent.

- Les membres de la ZLECAf devraient envisager d'inclure des dispositions dans le chapitre de la concurrence qui obligent les autorités de la concurrence examinant les questions de structure du marché à prendre également en compte les effets de la structure du marché sur la sécurité et la vie privée. Il est important d'éviter la concentration des courtiers en données ou des plates-formes à l'échelle nationale et régionale, car cela crée un risque de défaillance unique ou de quelques points de défaillance aux conséquences considérables.

- Les membres du ZLECAf devraient également envisager d'inclure des dispositions dans le chapitre de la propriété intellectuelle de la ZLECAf qui clarifient le statut des données par rapport à la propriété intellectuelle, en particulier :

  - Que si le droit d'auteur est étendu aux bases de données et aux compilations de données, qu'il ne s'applique que lorsque les bases de données et les compilations sont créées par des auteurs humains et présentent une originalité et que le droit d'auteur ne s'étend qu'à la reproduction de la sélection et de la disposition originales des données dans la base de données et non aux données elles-mêmes ;

  - Que tout droit d'auteur ou autre droit de propriété intellectuelle, y compris les secrets commerciaux, qui permet le contrôle des données ne s'applique pas aux données à caractère personnel ; et

  - Que tout droit d'auteur ou autre droit de propriété intellectuelle, y compris les secrets commerciaux, qui permet le contrôle des données est limité par les dispositions de la réglementation sur la concurrence.

Actions

- Les États membres doivent ratifier la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel et élaborer des protocoles supplémentaires, le cas échéant, pour refléter

les changements intervenus depuis la rédaction initiale ; Établir, ou habiliter, un mécanisme au sein de la CUA pour centraliser les engagements régionaux sur les normes de données ;

- Une fois adopté, des alignements avec le processus de la ZLECAf devraient immédiatement être explorés;

- Inclure les questions liées aux données dans les négociations sur les chapitres de la concurrence et de la propriété intellectuelle de la ZLECAf et

- S'accorder sur des critères communs et cohérents pour évaluer l'adéquation des niveaux de protection des données à caractère personnel sur le continent afin de faciliter et de permettre le transfert transfrontalier des données et de normaliser la protection.

5.5.4. Institutions et associations continentales et régionales

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

Communautés économiques et de développements régionaux

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

Arbitres en matière de droits de l'homme

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

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

Réseau africain des régulateurs de données

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

Associations d'autorités de régulation des TIC

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

Associations sectorielles

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

Forum africain de la concurrence

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

Recommandations

- Renforcer la coopération réglementaire et le partage des connaissances entre les pays et régions d'Afrique en renforçant les capacités au Réseau africain des autorités de protection des données et des Associations régionales des régulateurs des TIC.

- Les mécanismes d'arbitrage continentaux et régionaux existants devraient être explicitement habilités à traiter les questions relatives aux données qui sont impliquées dans les droits numériques et les droits sur les données, ainsi que les litiges transfrontaliers sur les données.

- Les autorités fiscales africaines devraient collaborer par le biais du Forum africain de l'administration fiscale (ATAF) pour élaborer une position africaine afin de représenter plus efficacement l'intérêt commun

dans le processus de réforme de la fiscalité internationale, comme l'érosion de la base de l'impôt et le transfert de bénéfices (BEPS).

- Mettre en place un Forum annuel d'innovation des données pour l'Afrique qui servira de plateforme pour des discussions multipartites, facilitera les échanges entre les Pays et sensibilisera les décideurs politiques sur le potentiel des données comme moteur de l'économie numérique actuelle.

5.6. Cadre de mise en œuvre

5.6.1. Cadre de mise en œuvre par étapes

Il convient de noter que si les domaines d'activité ci-dessous sont identifiés par phases, leur réalisation n'est pas strictement linéaire. En particulier, les phases 2 et 3 sont considérées comme des processus simultanés, qui peuvent se dérouler parallèlement aux activités d'incorporation au niveau national. Le cadre de mise en œuvre doit être lu conjointement avec la cartographie des parties prenantes décrite au point 11.2.

	Activité	Description	Principal Acteur
PHASE 1 : ADOPTION DU CADRE			
A	Les États membres adoptent le cadre stratégique		États membres
B	Conception du cadre de suivi	Mise en place d'un cadre de suivi de haut niveau	CUA
C	Établir ou habiliter un mécanisme au sein de l'UA pour centraliser les engagements régionaux en matière de données.	Les activités doivent inclure un soutien à la mise en œuvre, la coordination sur les normes de données et d'autres domaines spécifiques énoncés dans les recommandations nécessitant une collaboration régionale	CUA
PHASE 2 : APPROPRIATION			
A	Évaluer le cadre continental	Assurer l'alignement sur les instruments continentaux.	CUA, CER, AUDA-NEPAD Smart Africa.
B	Engagement des structures continentales	Engager les structures associées sur les domaines potentiels de collaboration dans la mise en œuvre du cadre.	CUA
C	Évaluation des cadres internationaux	En se concentrant sur les principes, explorer l'alignement avec les cadres des structures internationales.	CUA
D	Mobilisation des structures internationales		CUA, États membres de l'UA
PHASE 3 : SOUTIEN CONTINENTAL AUX ÉTATS MEMBRES POUR REMPLIR LES CONDITIONS PREALABLES			

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

5.6.2. Cartographie des parties prenantes

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

DESCRIPTION	SOUS-TYPES	Objectif
INTERNATIONAL		
Nations Unies	Union Internationale des Télécommunications, Département de la sûreté et de la sécurité des Nations Unies	Alignement de la politique de développement
Organisations multilatérales	Organisation de coopération et de développement économiques, Banque mondiale	Alignement de la politique économique

Structures de gouvernance de l'Internet	Forum sur la gouvernance de l'Internet, Groupe de travail sur l'ingénierie Internet, Internet Corporation for Assigned Names and Numbers (ICANN)	Alignement des politiques numérique et Internet
Normes internationales	Organisation internationale de normalisation	Alignement des normes en matière de des données
Organisations multilatérales (sectorielles)	Organisation mondiale de la santé, Organisation mondiale du commerce	Alignement des composantes sectorielles de la politique
RÉGIONAL		
Communautés économiques régionales	CEDEAO, SADC, CAE, CEEAC, COMESA, IGAD, CEN-SAD, UMA,	Alignement des politiques économiques et du développement
Structures de gouvernance de l'Internet	AFRINIC, IGF Africain	Alignement des politiques numérique et Internet
Réseau communautaire (régulateurs)	Réseau Africain des autorités de protection des données, autres associations de régulateurs, Forum de l'administration fiscale africaine	Alignement des politiques intersectorielles et transfrontalières
Communauté régionale (sectorielle)	Banque africaine de développement	Alignement des composantes sectorielles de la politique en matière de données
NATIONAL		
Départements nationaux	Télécommunications, Justice, Coopération internationale	, Alignement des politiques en matière de donnes
agences statistiques		Habilitation
Autorités de régulation	Protection des données, Réglementation des TIC, règlementation de la concurrence	Mise en œuvre
Au niveau de l'entreprise	Comités de gouvernance des données	Habilitation, engagement multipartite

7. RECOMMANDATIONS :

Suite à l'approbation du cadre de la politique continentale des données par les organes de l'UA, la Commission de l'UA, en collaboration avec les institutions régionales et les parties prenantes concernées, élaborera un plan d'action pour guider la mise en œuvre du cadre qui prend en compte la souveraineté numérique des États ainsi que les différents niveaux de développement, la vulnérabilité des populations et la numérisation au sein des États membres de l'UA, notamment les aspects liés au manque d'infrastructures TIC et l'absence de politiques et de législations en matière de cybersécurité. Le plan d'action (à court, moyen et long terme) identifiera les rôles

et les responsabilités et mettra l'accent sur les priorités clés et les actions immédiates tant au niveau régional qu'au niveau continental, ce qui va de pair avec les niveaux de maturité des données des États membres de l'UA.

Références

Banque africaine de développement. (2019). Rapport annuel 2019 | Banque africaine de développement - Construire aujourd'hui, une meilleure Afrique demain. https://www.afdb.org/en/documents/annual-report-2019

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

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

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

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

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

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

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

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

Gillwald, A., & Mothobi, O. (2019). After Access 2018: A Demand-Side View of Mobile Internet From 10 African Countries (After Access 2018: A Demand-Side View of Mobile Internet from 10 African Countries After Access: Paper No. 7 (2018); Policy

Paper Series No. 5). Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf

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

Information Society. (2018). Personal Data Protection Guidelines for Africa. A joint initiative of the

Internet Society and the Commission of the African Union. https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

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

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

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

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

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

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

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

Nicholas, G., & Weinberg, M. (2019). Data Portability and Platform Competition: Is User Data Exported From Facebook Actually Useful to Competitors? | NYU School of Law. New York University School of Law.

https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition

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

Open Data Charter. (2015). Open Data Charter Principles. Open Data Charter. https://opendatacharter.net/principles/

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

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

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

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

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

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

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

Stork, C., & Gillwald, A. (2012). South Africa's mobile termination rate debate: What the evidence tells us (Policy Brief No. 2; South Africa). Research ICT Africa.

https://researchictafrica.net/publications/Country_Specific_Policy_Briefs/South_Africa_Mobile_Termination_Rate_Debate_-_What_the_Evidence_Tells_Us.pdf

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

CNUCED. (2021). Rapport sur l'économie numérique 2021 : Flux de données transfrontières et développement : Pour qui les données circulent [publication des Nations Unies].

Nations Unies. (2017). En regardant vers l'avenir, l'ONU va examiner comment l'intelligence artificielle pourrait aider à atteindre la croissance économique et à réduire les inégalités-Développement durable des Nations Unies. https://www.un.org/sustainabledevelopment/blog/2017/10/looking-to-future-un-to-consider-how-artificial-intelligence-could-help-achieve-economic-growth-and-reduce-inequavan der Spuy, A. (2021, February 23). How do we protect children's rights in a digital environment only available to some? African Post. https://researchictafrica.net/2021/02/23/how-do-we-protect-childrens-rights-in-a-digital-environment-only-available-to-some/

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

Wook, M., Hasbullah, N. A., Zainudin, N. M., Jabar, Z. Z. A., Ramli, S., Razali, N. A. M., & Yusop, N. M. M. (2021). Exploring big data traits and data quality dimensions for big data analytics application using partial least squares structural equation modelling. Journal of Big Data, 8(1), 49. https://doi.org/10.1186/s40537-021-00439-5lities/.

Banque mondiale. (2021). Des données pour des vies meilleures. Banque mondiale. doi:10.1596/978-1-4648-1600-0

Banque mondiale et UIT. (2020). La Banque mondiale et l'Union internationale des télécommunications lancent un manuel sur la réglementation numérique [Texte/HTML]. Banque mondiale. https://www.worldbank.org/en/news/feature/2020/09/08/the-world-bank-and-international-telecommunication-union-launch-handbook-on-digital-regulation

Forum économique mondial. (2016). Indice de préparation aux réseaux. Rapport mondial sur les technologies de l'information 2016. http://wef.ch/29cCKbU

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

8. ANNEXE - DEFINITIONS PRATIQUES

9. **L'ANONYMISATION** DESIGNE LA SUPPRESSION DES IDENTIFIANTS PERSONNELS DIRECTS ET INDIRECTS DES DONNEES.

Le terme "**continental**" désigne l'Afrique dans le présent cadre.

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

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

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

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

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

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

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

Les services en nuage désignent les applications grand public (c'est-à-dire les médias sociaux et le courrier électronique proposés sur Internet), dans lesquelles les

données ne se trouvent pas sur les appareils des individus mais sont stockées à distance dans un centre de données. Les exemples incluent Facebook, YouTube et Gmail.

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

La capacité numérique désigne le terme utilisé pour décrire les compétences, l'alphabétisation, les normes sociales et les attitudes dont les individus et les organisations ont besoin pour prospérer, pour vivre, apprendre et travailler dans une société et une économie numériques.

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

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

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

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

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

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

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

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

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

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

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

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

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

Le respect de la vie privée et la sécurité dès la conception consistent à intégrer de manière proactive des mécanismes de respect de la vie privée et de sécurité dans la conception et le fonctionnement des produits et services, qu'il s'agisse de systèmes informatiques ou non, d'infrastructures en réseau ou de pratiques commerciales. Cela

exige que la gouvernance de la vie privée et de la sécurité soit prise en compte tout au long du processus d'ingénierie et du cycle de vie du produit.

La pseudonymisation désigne le traitement des données de manière à ce qu'elles ne puissent être associées à un individu sans informations supplémentaires.
Aux fins du présent cadre, le terme "**Régional**" désigne les cinq régions d'Afrique reconnues par l'Union africaine.

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

2022-01-20

Report of the 4th Ordinary Session of the STC on Communication and ICT (STC-CICT), 25-27 October 2021

African Union

DCMP