Edition 2025 de l'École africaine sur la gouvernance de l'Internet (AfriSIG) : Une perspective africaine sur la gouvernance des données à tous les niveaux

Présenté à l'examen du Groupe de travail sur la gouvernance des données de la Commission de la science et de la technique au service du développement (CSTD)

Version finalisée - 30 juin 2025

Préambule : À propos de ce document

Ce document a été élaboré par un groupe de personnes de différents secteurs et de groupes de parties prenantes à travers l'Afrique qui se sont réunis à Dar es Salaam, en Tanzanie, du 23 au 28 mai 2025 pour la 13e édition annuelle de l'École africaine sur la gouvernance de l'Internet (AfriSIG)[1]. Parmi les personnes qui ont contribué à ce texte figurent des responsables gouvernementaux, des journalistes, des analystes politiques, des défenseurs du numérique et des droits humains, des groupes de défense des droits des femmes, des organisateurs de forums nationaux et régionaux sur la gouvernance de l'internet, des régulateurs des télécommunications, des membres du parlement, des professionnels de la gouvernance des données et des membres de la communauté technique.

La structure du document s'inspire du texte sur la gouvernance des données du Pacte numérique mondial (2024). Le document comporte trois sections : la section A couvre les principes qui s'appliquent à la gouvernance des données. Cette section s'appuie sur le Cadre de politique de l'Union africaine sur les données de 2022, mais nous pensons qu'il a une pertinence universelle. La section B se penche sur l'interopérabilité entre les systèmes de gouvernance des données et la section C sur le partage des avantages des données. La section D propose des options pour des flux de données transfrontaliers sûrs, sécurisés et fiables.

Bien que les suggestions de ce document représentent une perspective africaine et s'adressent aux parties prenantes africaines, nous pensons qu'elles seront utiles au Groupe de travail de la CSTD sur la gouvernance des données.

Section A : Principes fondamentaux de la gouvernance des données

Le groupe approuve les principes du Cadre de politique des données de l'Union africaine (UA) accepté par le Conseil exécutif de l'UA en février 2022.[2] Ces principes s'alignent sur le droit international et visent à parvenir à une plus grande unité, solidarité et développement inclusif à travers le continent tout en protégeant les droits

1 AfriSIG est un projet conjoint de la Commission de l'Union africaine, de l'Association pour le progrès des communications et de la recherche ICT Africa - http://afrisig.org
2 https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf

de l'homme et des peuples tels qu'inscrits dans la Charte africaine des droits de l'homme et des peuples.[3] Il s'agit notamment de :

Coopération : échange de données et interopérabilité à l'appui d'un marché unique numérique robuste.

Intégration : Promouvoir les flux de données intra-africains avec une forte protection des données.

Équité et inclusivité : Assurer la réceptivité aux voix marginalisées.

Confiance, sécurité et responsabilité : créer des environnements de données sûrs, éthiques et sécurisés.

Souveraineté : Permettre aux pays africains de gérer et de gouverner eux-mêmes leurs données.

Exhaustif et tourné vers l'avenir : Encourager l'innovation, l'harmonisation et l'investissement.

Intégrité et justice : Garantir l'équité et les garanties juridiques dans tous les processus de données.

Le groupe AfriSIG propose également l'inclusion de cinq principes supplémentaires qui, selon lui, complètent les principes de l'AUDPF, à savoir :

Participation multipartite : Les systèmes et les politiques doivent intégrer intentionnellement les points de vue des différentes parties prenantes et, en particulier, refléter les besoins des groupes sous-représentés tels que les femmes, les jeunes, les personnes handicapées et les populations rurales.

Clarté réglementaire : Les cadres juridiques et réglementaires doivent être transparents, cohérents et applicables au-delà des secteurs et des frontières.

Justice des données : l'ensemble du cycle de vie des données (collecte, traitement, utilisation et gouvernance) doit promouvoir la justice, l'équité et l'inclusion. Les pratiques en matière de données peuvent renforcer ou perturber les asymétries de pouvoir existantes et doivent donc être conçues pour défendre la dignité, l'égalité et les droits de toutes les personnes. La justice des données exige une gouvernance participative, un accès équitable aux données et des mécanismes de réparation pour lutter contre les préjudices et l'exclusion.

Durabilité et justice environnementale : La durabilité et la justice environnementale exigent que les cadres de gouvernance des données mettent l'accent

3 https://au.int/en/treaties/african-charter-human-and-peoples-rights

sur l'infrastructure des données vertes, les pratiques d'économie circulaire et les politiques alignées sur le climat.

L'accès aux données comme outil de promotion des droits de la personne : L'accès équitable aux données, qui englobent les statistiques, les ensembles de données et les résultats de recherche, est essentiel pour favoriser une société juste, informée et inclusive à l'ère numérique et constitue une extension du droit d'accès à l'information.[4]

Section B : Interopérabilité des systèmes de données

Alors que le Cadre politique des données de l'UA et le Protocole sur le commerce numérique de la Zone de libre-échange continentale africaine (ZLECAf) soulignent la nécessité d'une gouvernance des données harmonisée, les environnements juridiques fragmentés restent un obstacle majeur. Les éléments suivants peuvent aider à résoudre ce problème :

Normes publiques communes : Les décideurs politiques devraient donner la priorité à l'adoption et à la mise en œuvre de normes de données publiques communes et internationalement reconnues afin d'améliorer l'interopérabilité des systèmes. Les normes d'interopérabilité doivent être adaptables et tenir compte de la diversité linguistique et de l'accessibilité pour les personnes handicapées. Ils doivent veiller à ce que les systèmes intersectoriels et transfrontaliers puissent interagir efficacement tout en préservant la confidentialité et la sécurité des données. Ces mécanismes devraient être complétés par des mécanismes de cryptage et d'authentification robustes pour protéger l'intégrité et la confidentialité des données.

La gestion des données, la participation des citoyens et l'inclusion de mécanismes de recours dans les cadres d'interopérabilité : cela favorisera la confiance du public et encouragera la conformité.

Renforcement des capacités : Les organismes régionaux impliqués dans l'harmonisation, tels que la CUA et les communautés économiques régionales (CER), ont besoin de capacités pour leur permettre de coordonner efficacement l'élaboration et l'adoption de normes conjointes, de mécanismes de responsabilisation et d'initiatives d'intégration numérique. La capacité est nécessaire au niveau des systèmes de

4 Extrait de la résolution de 2024 de la Commission africaine des droits de l'homme et des peuples sur « Promouvoir et exploiter l'accès aux données comme outil pour faire progresser les droits de l'homme et le développement durable à l'ère numérique. https://achpr.au.int/en/adopted-resolutions/620-data-access-tool-advancing-human-rights-and-sustainable-development CADHP/Rés.620 (LXXXI)

données, mais le renforcement des capacités humaines est une dimension encore plus importante de l'interopérabilité. Des capacités sont nécessaires au niveau des communautés qui génèrent des données, de la société civile et des défenseurs de la justice des données, des groupes d'éducation civique, des médias, des écoles et des universités - aux niveaux national, régional et international. Les parlementaires doivent également être en mesure de jouer efficacement leur rôle de surveillance. L'apprentissage par les pairs et l'assistance technique sont des moyens puissants de renforcer les capacités et devraient être encouragés et soutenus au sein des groupes de parties prenantes, mais aussi au niveau multipartite.

Partenariats : Les partenariats entre les gouvernements ainsi qu'entre le gouvernement et la société civile, le gouvernement et le secteur privé, ainsi que les collaborations multipartites devraient être encouragés pour soutenir le développement des capacités et faciliter l'interopérabilité.

Investir dans l'interopérabilité : les priorités d'investissement devraient inclure :

- Des centres de données régionaux partagés
- De l'infrastructure compatible IPv6
- Peering de bases de données et IXP neutres
- Des partenariats public-privé pour combler les lacunes en matière d'infrastructures
- Collaborations multipartites entre les gouvernements, les chercheurs, le secteur privé et la société civile.

Section C : Partage des avantages des données

La résolution de 2024 de la Commission africaine des droits de l'homme et des peuples (*CADHP/Rés.620 (LXXXI)*) affirme que l'accès aux données est une extension du droit à l'information. Il reconnaît le potentiel transformateur des données pour renforcer la démocratie, stimuler l'innovation, améliorer la participation du public et faire progresser l'élaboration de politiques fondées sur des données probantes, ce qui est essentiel pour atteindre les *objectifs de développement durable (ODD)* et l'*Agenda 2063 : L'Afrique que nous voulons.*

Pour garantir un large partage des avantages, la gouvernance des données doit être prise en compte :

Accessibilité, ouverture et données en tant que bien public : les données doivent être reconnues comme un bien public, en particulier lorsqu'elles permettent l'innovation et le développement inclusif dans des secteurs tels que la santé, l'éducation, la résilience climatique et les infrastructures publiques.

Les gouvernements devraient promouvoir des initiatives de données ouvertes qui permettent un accès sécurisé à des ensembles de données non personnelles et anonymisées pour la recherche et la défense de l'intérêt public, tout en maintenant de solides garanties de protection des données pour prévenir les abus et les préjudices.)

Divulgation maximale et données communes : Les données d'intérêt public détenues par des acteurs étatiques ou privés (lorsqu'il existe un intérêt public prépondérant) devraient être disponibles par défaut, limitées uniquement par des protections justifiables des droits de l'homme. Cela favorise une *communauté de données* au service de besoins collectifs.

Partage des données : Les pratiques de partage des données doivent être transparentes et respectueuses des droits, garantissant une utilisation non discriminatoire des données et des mesures de protection proactives contre les préjugés. Il faut envisager le recours à des ententes de partage de la valeur pour assurer la sécurité et l'échange équitable des données.

Partage équitable de la valeur : Le partage équitable des avantages devrait inclure une rémunération et une reconnaissance équitables pour les communautés et les individus qui génèrent ou contribuent à des données, en particulier ceux dont les expériences sont souvent exclues des systèmes numériques.

Assurez-vous que les communautés et les individus ont leur mot à dire sur la manière dont leurs données sont collectées, utilisées et supprimées afin de favoriser la confiance et l'intégrité des données.

Les communautés mal desservies doivent recevoir une compensation ou une reconnaissance pour leurs contributions aux données.

Des modèles de monétisation inclusifs sont nécessaires pour combler les lacunes régionales en matière de contenu et empêcher l'exploitation par des acteurs dominants (par exemple, les entreprises technologiques mondiales).

Les politiques transfrontalières en matière de données (par exemple, l'itinérance transparente des données) devraient soutenir la *Zone de libre-échange africaine* et le *marché unique numérique*, permettant une interopérabilité abordable.

Confidentialité et responsabilité : Des mesures de protection solides (consentement transparent, mécanismes de règlement des griefs et protocoles anti-préjugés) doivent accompagner l'accès aux données. Les cadres de gouvernance devraient inclure une surveillance publique, des systèmes de recours exécutoires (p. ex., le règlement des différends en ligne) et des règles claires pour la suppression des données.

Formation sur les données : Les ressources devraient être orientées vers des programmes communautaires et institutionnels de formation sur les données, en mettant l'accent sur l'autonomisation des femmes, des jeunes et des groupes marginalisés. Ces initiatives sont nécessaires pour promouvoir une participation équitable à l'économie numérique et garantir le consentement éclairé dans le partage des données. Donner la priorité à la formation sur les données pour les femmes, les jeunes et les groupes marginalisés par le biais de programmes communautaires/institutionnels et veiller à ce que les acteurs de la base, les médias, la société civile et les PME puissent participer aux initiatives d'économie des données.

Gouvernance inclusive : les parties prenantes doivent co-développer des modèles de gouvernance qui s'attaquent aux asymétries de pouvoir et répartissent équitablement la valeur économique/sociale des données.

Les communautés devraient avoir le pouvoir de décider de la collecte, de l'utilisation et de la suppression de leurs données.

Collaboration mondiale et régionale : la collaboration mondiale est aussi importante que la collaboration régionale, et la communauté et les organisations internationales doivent promouvoir de meilleurs systèmes de partage des avantages liés aux données.

Politiques fiscales équitables : Les politiques de fiscalité numérique doivent éviter de surcharger les innovateurs locaux tout en privilégiant la création de valeur locale et en veillant à ce que les opérateurs multinationaux paient des impôts suffisants proportionnellement aux bénéfices qu'ils tirent des données recueillies auprès des juridictions africaines.

Section D : Flux de données sûrs, sécurisés et fiables

Pour réaliser la transformation numérique, l'Afrique doit mettre en place des cadres solides qui facilitent des flux de données sûrs, sécurisés et fiables, tout en assurant la croissance économique et la protection des droits fondamentaux. La gouvernance

transfrontalière des données est essentielle à l'intégration de l'Afrique dans l'économie numérique mondiale tout en préservant la souveraineté, la sécurité et l'accès équitable. Les recommandations suivantes décrivent les principales mesures nécessaires pour parvenir à une gouvernance des données sécurisée et interopérable sur tout le continent.

Une approche fondée sur les droits de l'homme (HRBA) pour la gouvernance des données : L'approche de l'Afrique en matière de flux de données transfrontaliers doit être ancrée dans les principes des droits de l'homme, la gouvernance inclusive et l'accès équitable. Les mécanismes de gouvernance des données doivent être conçus pour faire respecter les droits individuels, favoriser la transparence et atténuer les risques liés à l'utilisation abusive, à la surveillance et à l'exploitation. La coopération numérique régionale doit être inclusive et fondée sur des considérations éthiques, et les cadres de protection des données doivent donner aux citoyens les moyens d'agir plutôt que de simplement servir les intérêts des entreprises ou de l'État.

Instaurer la confiance et la sécurité grâce à la gouvernance et aux garanties techniques : un cadre réglementaire solide et harmonisé est essentiel pour favoriser la confiance dans les flux de données transfrontaliers. L'établissement et la mise en œuvre de lois nationales et régionales sur la protection des données qui s'alignent sur les normes africaines et mondiales, telles que la Convention de Malabo, le RGPD et les principes directeurs de l'OCDE, apporteront la clarté et la responsabilité indispensables. Une application efficace par des autorités de protection des données indépendantes et habilitées garantira la transparence et la conformité réglementaire.

D'un point de vue technique, l'Afrique doit intégrer les principes de l'architecture Zero Trust (ZTA),[5] en veillant à ce qu'aucune entité, qu'elle soit interne ou externe, ne soit automatiquement digne de confiance. Ce modèle applique une authentification rigoureuse, un contrôle d'accès granulaire basé sur le principe du moindre privilège et une micro-segmentation pour atténuer les menaces de sécurité. Des technologies d'amélioration de la confidentialité (PET) telles que le cryptage de bout en bout, les protocoles d'anonymisation, les centres de données sécurisés et les mesures de sécurité à plusieurs niveaux doivent être déployées pour protéger les données personnelles et biométriques sensibles.

En outre, l'Afrique devrait développer des cadres de confiance régionaux et des mécanismes de certification, permettant une reconnaissance mutuelle de la conformité

5 « Architecture Zero Trust (ZTA) » signifie qu'aucun utilisateur ou appareil n'est approuvé par défaut ; L'accès est basé sur la vérification de l'identité et un privilège minimal.

et des normes entre les juridictions. Ces cadres réduiront l'insécurité juridique, favoriseront l'interopérabilité et faciliteront la fluidité des transactions numériques.

Renforcement des structures de gouvernance et collaboration transfrontalière : Les États africains devraient intégrer l'AUDPF dans leur droit interne et établir des structures institutionnelles similaires pour assurer sa mise en œuvre au niveau national. Pour permettre un échange de données sans faille, il convient de promouvoir des protocoles techniques normalisés, garantissant la cohérence des formats de données, l'interopérabilité et l'infrastructure numérique.

Pour favoriser la coopération bilatérale et multilatérale, les communautés économiques régionales africaines devraient négocier des accords de partage de données transfrontaliers exécutoires qui intègrent les dispositions de cybersécurité des dispositions sur le commerce numérique de la ZLECAf, de l'AUDPF et de la Convention de Malabo. Cette action améliorera l'interopérabilité, renforcera la confiance entre les États et apportera une clarté juridique en matière de souveraineté des données.

En outre, des mécanismes de résolution des litiges doivent être mis en place pour lutter contre les violations et les abus, en veillant à ce que les flux de données transfrontaliers préservent la dignité des individus. Un système de recours public et de résolution des plaintes renforcera la confiance dans le cadre de gouvernance numérique de l'Afrique.

Renforcement des capacités, inclusion numérique et accès équitable : Pour que la gouvernance des données transfrontalières soit efficace, elle doit être inclusive et participative. Le partage fiable des données doit être ancré dans une gouvernance multipartite, en veillant à ce que les communautés marginalisées aient leur mot à dire dans les décisions concernant l'utilisation et le partage des données les concernant. L'inclusion numérique est essentielle pour garantir un accès équitable aux avantages de l'innovation axée sur les données, renforcer la confiance du public et atténuer les risques liés à la surveillance, à l'exploitation et à la discrimination.

La sécurité dépend de la collaboration : les pays africains doivent investir dans des infrastructures de cybersécurité et des programmes de renforcement des capacités numériques qui autonomisent les institutions et les individus à travers les gouvernements, la société civile et le secteur privé. En favorisant la culture numérique, les parties prenantes acquerront une compréhension des droits des données, du consentement éclairé, de la sensibilisation aux risques et du traitement éthique des

données, garantissant ainsi que l'écosystème de gouvernance des données de l'Afrique est transparent et responsable.

En outre, l'Afrique doit renforcer la maturité de ses capacités de cyberdéfense grâce à une coopération transfrontalière entre les centres d'opérations de sécurité (SOC), les équipes d'intervention d'urgence en matière de cybersécurité et de sécurité informatique (CSERT) et les centres d'analyse du partage d'informations (ISAC). Ces structures joueront un rôle central dans la réponse aux incidents, la surveillance de la sécurité des données et la protection contre les cybermenaces qui sapent la confiance dans la gouvernance numérique.

Normes publiques communes : Les cadres politiques doivent donner la priorité à des protocoles techniques normalisés pour assurer l'interopérabilité des systèmes et la portabilité des données. En mettant en œuvre ces mesures, l'Afrique peut construire un modèle de gouvernance des données qui soit inclusif, résilient et tourné vers l'avenir, permettant à la fois l'innovation et la protection des droits humains au sein d'un écosystème numérique sécurisé.

FIN