Centre for International
Governance Innovation

Note d'analyse No 185 — Juin 2024

La souveraineté numérique de l'Afrique : au-delà de la localisation des données

Folashadé Soulé

Points principaux

- Les États africains doivent veiller à ne pas confondre la souveraineté numérique avec la localisation des données, car ils risqueraient alors d'omettre les défis structurels qu'il faut aussi relever pour rendre la localisation des données viable.
- Vu l'impressionnant nombre de centres de données actuellement en voie de construction sur le continent, il faut davantage envisager l'équité numérique sous l'angle du partage des avantages des données, de l'évitement du colonialisme des données et de la promotion de la participation africaine au développement de l'infrastructure des données.
- Étant donné que la localisation des données gouvernementales sensibles, comme l'information électorale, est essentielle pour protéger la souveraineté numérique, il faut améliorer la capacité locale en matière de gouvernance de la technologie et des données. Des institutions africaines peuvent contribuer à susciter ce processus en développant de nouveaux modèles financiers et en renforçant la capacité de la gouvernance et de la cybersécurité numériques.

Introduction

La souveraineté numérique est une orientation et une position stratégique qui vise à réaffirmer l'autorité des acteurs étatiques sur le cyberespace, y compris sur le développement des technologies numériques. C'est pourquoi cette vision nécessite la reconnaissance des droits des pays individuels de développer et d'utiliser les instruments requis pour gouverner les cyberactivités au sein de leur territoire légal (Musoni et coll. 2023). L'approche de la souveraineté numérique d'un pays dépend aussi de ses intérêts économiques et politiques, de ses capacités technologiques, de ses priorités nationales et de sa politique numérique étrangère. Sur le plan international, on trouve plusieurs interprétations du concept de souveraineté numérique (ibid.) avec des variations d'un continent à l'autre.

La stratégie de l'Union européenne consiste à affirmer sa souveraineté numérique en établissant des normes légales mondiales et en faisant la promotion des technologies européennes. Le règlement général sur la protection des données (RGPD)[1] en est un exemple notable. Il fait partie de la stratégie européenne pour imposer des normes rigoureuses sur la gouvernance des données et étendre l'autorité de

1 Voir CE, *Règlement général sur la protection des données*, [2016] OJ, L 119/1, en ligne : <www.consilium.europa.eu/fr/policies/data-protection/data-protection-regulation/>.

À propos de l'auteur

Folashadé Soulé est agrégée supérieure du CIGI et associée de recherche principale du programme Global Economic Governance de la Blavatnik School of Government de l'Université d'Oxford. Elle est actuellement chercheuse invitée de l'Université du Ghana. Ses domaines de recherche portent sur les relations Afrique-Chine, l'étude du pouvoir dans les relations internationales de l'Afrique et la politique de la coopération Sud-Sud. Elle fait partie des chercheuses principales de la négociation des partenariats numériques de l'Afrique, un projet de recherche politique sur les relations de l'Afrique avec des partenaires en pleine ascension dans le secteur numérique. Dans le cadre de ce projet, elle dirige une série d'entrevues et de dialogues politiques avec de grands décideurs, des ministres et des acteurs civiques et privés africains qui servent à exposer la façon dont les acteurs africains édifient, négocient et gèrent les partenariats stratégiques dans le secteur numérique dans un contexte de rivalité géopolitique.

l'Union européenne sur le traitement des données, même au delà de ses frontières. En établissant ces normes, l'Union européenne encourage d'autres régions à adopter des lois similaires au RGPD.

Les États-Unis adoptent une approche de laissez-faire favorable à la circulation illimitée des données, qui avantage ses entreprises technologiques, qui contrôlent la plus grande part du marché mondial. Cependant, grâce à la CLOUD Act[2] (BSA 2021), les États-Unis maintiennent leur souveraineté en exigeant des entités américaines, quel que soit leur emplacement, qu'elles divulguent leurs données sur demande pour des motifs de sécurité nationale.

La Chine, en revanche, maintient un contrôle serré de ses activités nationales et internationales. Cette approche donne lieu à des règlements sur les données axés sur la surveillance et à des exigences rigoureuses concernant le transfert des données. Le gouvernement chinois a un accès privilégié à toutes les données issues de la Chine et exige des entreprises qu'elles transfèrent toute information critique à des serveurs étatiques. Les entreprises chinoises ont aussi l'obligation de permettre, sur demande de l'État, l'accès à leurs données pour des motifs de sécurité nationale.

Dans le cadre du projet de recherche politique sur la négociation des partenariats numériques de l'Afrique[3] hébergé à la Blavatnik School of Government de l'Université d'Oxford et appuyé par le Centre pour l'innovation dans la gouvernance internationale, ce mémoire vise à discuter d'approches de la souveraineté numérique en Afrique et des conséquences de cette souveraineté et des défis qui y sont attachés concernant la protection des données et la transformation numérique du continent.

2 Voir US, *Clarifying Lawful Overseas Use of Data Act*, Pub L No 115-141, 115 Cong (2018) (promulgué), en ligne : Congress.gov <www.congress.gov/bill/115th-congress/house-bill/4943>.

3 Voir www.geg.ox.ac.uk/negotiating-africas-digital-partnerships-interview-series.

Quelle est l'approche de la souveraineté numérique de l'Afrique?

En Afrique, une mauvaise interprétation courante consiste à tirer un parallèle entre la souveraineté numérique et la localisation des données. Certains acteurs, particulièrement des États, mais aussi des institutions financières régionales, pensent que les gouvernements africains peuvent exercer leur souveraineté numérique en ayant davantage de contrôle sur les données, l'infrastructure et toutes les activités de traitement des données qui ont lieu sur leur territoire, si l'infrastructure numérique et les centres de données nécessaires sont situés sur le continent africain et sont entre les mains d'entités africaines (par exemple, voir le Groupe de la Banque africaine de développement 2024). Les promoteurs de ce concept, qui comprennent certains gouvernements africains, cherchent, d'un côté, à mettre de l'avant l'État-nation comme le principal vecteur de la gouvernance du cyberespace, alors que, de l'autre côté, ils profitent des entreprises et des investissements privés pour promouvoir le développement numérique (Soulé 2023).

Ces initiatives de souveraineté économique comprennent des investissements substantiels visant à créer de nouveaux centres de données nationaux (de grands projets ont été lancés dans ce sens au Bénin, au Congo, en Côte d'Ivoire, dans la ville sénégalaise de Diamniadio, au Togo et dans d'autres parties de l'Afrique) et des points d'échange sur Internet. Bien que la localisation des données soit considérée comme un moyen d'assurer la souveraineté des données, elle demeure difficile à instaurer, principalement à cause des ressources financières et des capacités techniques requises pour déployer les centres de données nécessaires pour respecter cette condition. Un média nigérian a signalé en 2021 que 70 % des organismes gouvernementaux nigériens hébergeaient leurs données sur des serveurs infonuagiques situés outre-mer (Guardian Nigeria 2021). C'est pourquoi plusieurs États africains mettent la construction de leurs centres de données au cœur de leur ambition de souveraineté numérique, souvent en coopération avec des institutions financières internationales, comme la Banque mondiale, ou avec l'aide de prêts chinois.

Le développement accéléré des centres de données en Afrique : un nouveau capitalisme des données?

Face à cette accélération de la numérisation, plusieurs pays africains ont construit ou sont en train de construire des centres de données avec l'aide d'entreprises et d'investissements étrangers. Plusieurs gouvernements africains s'emploient aussi à obliger les entreprises à entreposer leurs données localement, bien que cette tactique ne mène pas nécessairement au développement numérique ou à une meilleure protection des données, car ces pays ont aussi des difficultés à offrir un approvisionnement fiable en électricité et une connectivité haute vitesse (programme Global Economic Governance 2023a).

L'explosion de la construction des centres de données en Afrique (environ 700 nouvelles installations durant les dix prochaines années, selon les estimations), qui montre bien la dépendance numérique de ce continent, représente ce que certains analystes appellent une phase de « capitalisme des données » (programme Global Economic Governance 2023d). Dans l'Union européenne, les données sont réglementées et protégées conformément au RGPD, mais, en Afrique, la protection des données est bien moins uniforme, et gouvernée par la Convention de l'Union africaine (UA) sur la cybersécurité et la protection des données personnelles (Convention de Malabo), le règlement complet sur la cybersécurité, que seuls quelques pays ont finalement ratifié (ibid.). Le manque de lois pour la protection régionale intégrale des données complique d'autant plus le problème.

Nombre de nations africaines manquent de lois solides sur la protection des données, ce qui soulève des craintes concernant la question de savoir si ces centres de données émergents peuvent être efficacement réglementés. Cette situation est tout particulièrement préoccupante, car plusieurs pays africains amorcent des projets nationaux sur l'ID numérique qui nécessitent la collecte, l'entreposage et le traitement des données sensibles

dans des centres de données. Bien que certains pays, comme le Ghana, fassent des progrès avec les systèmes d'ID numérique, il y a un manque général de collecte des données systématique et répandue sur tout le continent : en Afrique, des milliers de personnes n'ont toujours pas de dossier d'enregistrement civil (par exemple, un certificat de naissance) et, dans les endroits où ces types de dossiers existent, ils ne sont pas encore, pour la vaste majorité, numérisés (ibid.).

Un point important dont il faut tenir compte est la question de savoir qui sont les principaux bénéficiaires de ces centres de données. L'Afrique doit approcher avec prudence les discussions sur la place centrale des données, et remédier aux inégalités numériques pour assurer l'obtention, l'utilisation et les avantages réciproques et équitables de ces données. Ce processus sera favorisé par une augmentation des initiatives de construction et d'exploitation des centres de données africains. Cependant, bien que l'on prévoie une augmentation du nombre de centres de données sur le continent, les enjeux liés à la disponibilité et à la connectivité font de cette infrastructure numérique un défi de taille, sauf pour les grands investisseurs. Cette disparité soulève des questions sur la véritable souveraineté numérique et la vraie propriété locale des données en Afrique. Il semble qu'il y ait une mauvaise compréhension de la souveraineté numérique dans le contexte africain. Par exemple, il se peut que des dirigeants africains transmettent déjà des données nationales complètes à des entreprises internationales comme Google, susceptibles de financer des centres de données, sans tenir vraiment compte des conséquences pour la souveraineté et la sécurité des données. Cette pratique s'étend à des domaines comme l'infrastructure électorale, souvent gérée par des entreprises étrangères dont les données sont domiciliées hors de l'Afrique. Le problème critique, alors, est la question de savoir si ces centres de données sont construits pour réellement renforcer la capacité de l'Afrique ou pour servir des intérêts externes, une situation qui, selon des érudits, peut être considérée comme une forme de « colonialisme des données » (Coleman 2019). Tant qu'il n'y a pas une compréhension et une discussion plus globale de la signification de l'équité numérique pour l'Afrique, il sera compliqué d'atteindre la parité dans le paysage numérique mondial. Cette conversation est essentielle pour assurer que le développement de l'Afrique à l'ère numérique soit équitable et bénéfique pour les Africains.

Les risques auxquels sont confrontés les gouvernements africains qui se fient au modèle chinois de protection des données

Plusieurs pays africains ont aussi introduit des cadres de gouvernance des données qui ressemblent à ceux de la Chine. En 2021, le Sénégal a été, de façon remarquable, le premier pays africain à répliquer le modèle de gouvernance des données chinois, qui exige que tous les serveurs soient localisés au sein des frontières du pays (Olander 2021). L'État a transféré des données gouvernementales et des plateformes numériques qui étaient entreposées sur des serveurs à l'étranger dans des centres de données construits par Huawei au Sénégal. Ce centre de données a été financé par un prêt chinois. Selon le directeur de Sénégal Numérique, l'agence gouvernementale de développement numérique, « ce centre de données avant-gardiste permet au Sénégal de mieux contrôler sa destinée et de résoudre une fois pour toutes le problème de sa souveraineté numérique » (programme Global Economic Governance 2023b).

Cependant, cet arrangement pose plusieurs problèmes. En effet, le danger qu'il y a à se fier aux technologies de surveillance chinoises pour assurer la souveraineté numérique des pays africains a été quelque peu dissimulé par la promotion chinoise de la souveraineté des données auprès de divers organismes mondiaux chargés d'élaborer des normes pour les technologies numériques (programme Global Economic Governance 2023f). Suite à des enquêtes, on a constaté que des données confidentielles était transférées chaque nuit du siège central de l'Union africaine édifié par la Chine à Addis Ababa, en Éthiopie, à Shanghai, en Chine, et devenaient ainsi accessibles au gouvernement chinois (Kadiri et Tilouine 2018). La Chine n'est de loin pas la seule puissance à utiliser l'Internet à des fins d'espionnage, car les services de renseignement des É.-U. ont eu accès aux données de millions de citoyens du monde, notamment en Afrique (BBC News 2014; *Le Monde* 2016).

De plus, bien que cette incitation à la souveraineté numérique et la priorité que cette souveraineté accorde à la localisation des données semblent habiliter les acteurs locaux, elles soulèvent aussi des questions sur les droits numériques et la capacité de la société civile de promouvoir ces droits et de combattre les abus des gouvernements locaux et les excès des entreprises privées (programme Global Economic Governance 2023e).

C'est pourquoi, bien que les centres de données et les infrastructures connexes puissent améliorer la qualité de la prestation des services aux utilisateurs finaux, il reste à voir si cette méthode contribue de façon substantielle à la souveraineté numérique. De nombreux services numériques, y compris ceux gérés par les gouvernements, sont encore hébergés sur des serveurs à l'extérieur du continent. Tant que les capacités technologiques endogènes demeurent sous développées, la souveraineté des données demeurera un objectif fugace (programme Global Economic Governance 2023f).

Selon Motolani Peltola à l'Université Tampere, « La soudaine hausse des efforts consentis par les gouvernements africains pour favoriser la souveraineté numérique et la propriété locale des données couvre des dimensions économiques, sociales et politiques. Le bien-fondé qui sous-tend l'adoption des exigences liées à la localisation des données comprend des facteurs dont il faut tenir compte pour la cybersécurité, la protection des données et de la vie privée des citoyens, le développement économique, l'exécution de la loi, la sécurité nationale et, de façon controversée, la censure et la surveillance gouvernementales. Bien que ces motivations soient vraies pour les pays africains, les motifs prédominants concernent souvent la protection des données et le développement économique. Par exemple, la politique sur la localisation des données du Nigéria est justifiée par l'aspiration de rétablir l'équilibre commercial négatif dans le secteur des technologies de l'information et des communications et de favoriser une économie numérique qui profite aux citoyens. De même, l'Afrique du Sud considère les données et les infrastructures numériques connexes comme des ressources nationales stratégiques » (programme Global Economic Governance 2023c).

Le double défi de l'entreposage des données et de la protection des données

Peltola explique, « Grâce à la mise en œuvre de règlements sur la localisation des données, certains gouvernements africains visent à atténuer le risque de la colonisation des données, à renforcer la souveraineté numérique et à faire en sorte que les économies locales en recueillent les profits. En Afrique, la prévalence des entreprises technologiques étrangères, qui ont accès à de précieuses données sur les utilisateurs, expose les gouvernements et les citoyens africains à des vulnérabilités concernant la sécurité nationale et la protection des données. L'hébergement local des données est considéré comme un moyen pour les gouvernements africains de maintenir le contrôle sur les données critiques et l'infrastructure des données, comme les centres de données, que certains pays considèrent comme une infrastructure d'information critique qu'il faut protéger comme un bien national stratégique dont découlent des profits socio-économiques » (ibid.).

La localisation complète des données est un objectif ambitieux, et peut-être inatteignable. Il n'en reste pas moins qu'il y a une tendance croissante vers la fragmentation d'Internet et la localisation des données, comme on le voit dans des pays comme le Sénégal. Actif dans le domaine de la cybersécurité, ce pays affiche manifestement sa souveraineté numérique : preuve en est sa ratification des conventions de Malabo et de Budapest (la deuxième convention étant aussi axée sur la cybersécurité). Le choix de la délocalisation des données du Sénégal, avec l'aide de la Chine, soulève d'importantes questions. L'incident de 2019, lorsque des serveurs des bureaux centraux de l'Union africaine construits par la Chine ont secrètement transmis, selon les dires, des données à la Chine, souligne la déconnexion potentielle entre les objectifs affirmés de ce genre d'initiatives et leurs résultats réels (programme Global Economic Governance 2023d).

L'aspect pratique de la localisation complète des données en Afrique est aussi douteux. Les entreprises et l'infrastructure technologiques sont surtout étrangères, et les applications des données

ont souvent des dimensions internationales. De plus, comme la cybersécurité exige un degré de coopération internationale, des puissances externes peuvent tout de même obtenir des données en dépit des efforts de localisation. Cette réalité souligne l'importance d'examiner la dynamique des conventions et des traités internationaux sous l'angle d'une Afrique unifiée. Bien que l'ambition de pays comme le Sénégal concernant la localisation des données gouvernementales soit louable, on ne sait pas vraiment si cette approche est faisable dans toute l'Afrique. Une approche plus harmonisée de la protection des données, dans laquelle les pays africains définiraient ensemble leurs priorités et développeraient une compréhension plus approfondie de la gouvernance des données, serait plus adaptée (ibid.).

L'efficacité des stratégies utilisées pour que les gouvernements africains atteignent un consensus et agissent dans la sphère numérique est influencée par divers facteurs, dont certains sont humains, tandis que d'autres sont inhérents aux réalités de la région, comme l'instabilité et les conflits politiques. Ces facteurs détournent souvent la priorité des objectifs numériques. Par exemple, l'Union africaine a subi une cyberattaque significative en 2024, mais la réponse n'a pas été claire : elle reflétait le problème global de la priorité qu'on accorde aux conflits physiques par rapport aux menaces numériques. Contrairement à l'Union européenne, l'Union africaine n'a pas la même influence régionale et est reléguée au statut d'observateur des négociations sur la cybercriminalité. Cette limitation empêche l'Union africaine de parler au nom de ses États membres ou de les tenir responsables des problèmes numériques (ibid.).

Cette approche individualisée de la gouvernance dans les pays africains influe sur gouvernance cybernétique. Bien que l'Union africaine ait commencé à poursuivre une position africaine unifiée sur la cybersécurité, un document purement politique n'équivaut pas nécessairement à un consensus, comme en témoignent les retombées limitées de la Convention de Malabo.

Des réponses diverses au discours africain sur la propriété locale des données

Selon Peltola, « Les réponses d'acteurs étatiques étrangers, comme la Chine, les pays européens et les États-Unis, au discours qui entoure la localisation des données en Afrique reflètent selon toute vraisemblance leurs approches nationales de la souveraineté numérique, de la protection des données et des règlements. Tandis que l'Union européenne et l'Afrique ont en commun des craintes concernant la dominance des entreprises technologiques étrangères et leur utilisation des données des citoyens, il y a des disparités dans leurs approches de la souveraineté numérique. L'Union européenne se fait le promoteur d'une position libérale sur la souveraineté numérique en accordant la priorité au contrôle individuel des données et non pas à la supervision du gouvernement ou du secteur privé, ce qui contraste avec les tendances des pays africains d'afficher des éléments de modèles tant étatiques que libéraux dans leurs approches de la souveraineté des données à divers degrés » (programme Global Economic Governance 2023c).

« À l'inverse, » Peltola continue, « tant l'Union européenne que les États-Unis ont exprimé des craintes concernant le discours sur la propriété locale des données en Afrique, particulièrement en ce qui a trait aux conséquences de l'augmentation du contrôle gouvernemental sur les données afin de protéger les libertés civiles et la mauvaise utilisation potentielle des données par des gouvernements autoritaires. On craint aussi les risques que pose pour la sécurité nationale l'infrastructure numérique offerte par les entreprises étatiques chinoises. De plus, des questions entourent la compétitivité des entreprises technologiques européennes face au nombre croissant des règlements sur la localisation des données dans un secteur dominé par des entreprises technologiques chinoises et américaines. La complexité du paysage est d'autant plus exacerbée par les efforts de l'Union européenne de renforcer sa position dans la chaîne de valeur mondiale des données, de promouvoir la concurrence et de

négocier des ententes avec des pays africains concernant des clauses numériques » (ibid.).

Les États-Unis, qui adoptent une approche plus libérale de la souveraineté des données, se sont historiquement abstenus d'imposer des exigences fédérales ou générales concernant la localisation des données. La domination des entreprises technologiques américaines dans le monde entier et la promotion historique des É.-U. de la libre circulation transfrontalière des données reflètent un régime libéral sur la localisation des données assorti de restrictions limitées. Alors que les débats sur la localisation des données se poursuivent, il n'y a pas de consensus officiel entre les décideurs américains concernant les mandats nationaux, et les réponses en matière de politique étrangère doivent encore se matérialiser. Il n'en reste pas moins que les États-Unis sont principalement préoccupés par les retombées économiques des restrictions à la libre circulation transfrontalière des données sur les entreprises américaines, et craignent une approche autoritaire de la gouvernance des données issue de la domination croissante de la Chine dans l'établissement de l'infrastructure numérique en Afrique, qui suscite la tendance d'une augmentation de la localisation des données sur ce continent. Par exemple, l'Office of the US Trade Representative a exprimé des craintes concernant les mesures de la localisation des données au Nigeria et au Kenya qui, selon lui, discriminent les entreprises étrangères (qui entreposent et traitent des données dans le monde entier), et nuisent potentiellement au développement de l'économie numérique[4].

Selon Peltola, « La Chine, qui a adopté une vision étatique de la souveraineté numérique, centralise le rôle de l'État dans la gouvernance des données et le contrôle des données des citoyens. En imposant une approche rigoureuse de la localisation des données et l'hébergement des données dans l'État qui les a produites, la Chine a stimulé la croissance de ses entreprises nationales aux dépens de ses concurrents étrangers. En Afrique, la participation active de la Chine dans les infrastructures financières numériques, dont les centres de données, et la collaboration de ses entreprises technologiques avec les gouvernements dans la conception des stratégies économiques numériques nationales témoignent de sa détermination de façonner le paysage numérique conformément aux objectifs de sa route de la soie numérique » (ibid).

« Un fil conducteur de la réponse des acteurs étrangers, soit les États-Unis, la Chine et l'Union européenne, est un effort concerté pour stimuler la compétitivité de leurs entreprises technologiques sur le plan mondial, surtout dans le secteur technologique africain, qui recèle encore d'importantes occasions d'investissement. En dépit d'écarts dans les positions nationales sur la localisation des données, ces acteurs — les États-Unis (Karombo 2020), la Chine (conseil d'État, République populaire de Chine 2023) et l'Union européenne[5] — affichent un intérêt dans la capitalisation des occasions d'investissement facilitées par la tendance croissante à la localisation des données en Afrique » (ibid.).

Recommandations

La localisation des données gouvernementales, surtout des renseignements sensibles, comme les données électorales, à l'intérieur du pays est une étape cruciale vers la sauvegarde de la souveraineté numérique. Les pays africains doivent renforcer leur capacité dans les domaines de la gouvernance des données et de la technologie pour rendre cette ambition réaliste. Bien que l'aspiration de localiser les données ne soit pas tirée par les cheveux et soit bel et bien aussi celle d'autres pays, la transition vers un tel modèle en Afrique doit être soigneusement examinée pour équilibrer les ambitions et les réalités de la dépendance technologique et de la coopération internationale.

De plus, l'Union africaine doit accorder la priorité au financement et au renforcement des capacités de la gouvernance numérique et de la cybersécurité. Actuellement, comme nombre de pays africains dépendent du renforcement des capacités fourni par des États externes, il n'y a pas d'approche harmonisée. Cette situation est aggravée par la supériorité du donateur, qui fait que des pays externes dictent souvent les priorités numériques de l'Afrique.

4 Voir https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/march/fact-sheet-2019-national-trade-estimate.

5 Voir https://futurium.ec.europa.eu/en/Digital4Development/discussion/eu-au-data-flagship.

De plus, il sera crucial que davantage de pays africains développent et mettent en œuvre de solides règlements de protection des données et de la vie privée. Ces processus politiques doivent tenir compte des cadres continentaux de gouvernance des données comme le cadre de la politique sur les données de l'Union africaine, qui souligne l'importance de renforcer la détermination des intervenants à tous les niveaux pour veiller à ce que les données servent les intérêts du public, spécifiquement l'infonuagique, les services liés aux mégadonnées et la plateformisation. Cette approche sera essentielle pour favoriser l'efficacité du système, les améliorations de la prise de décisions et la facilitation d'un modèle africain de transfert transfrontalier des données qui favorise le commerce intracontinental au lieu de l'empêcher (Gehl Sampath et Tregenna 2022).

Des communautés économiques comme la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) jouent un rôle important, mais sont confrontées à des défis de gouvernance sous-régionaux. Même avec des directives comme la stratégie régionale sur la cybercriminalité et la cybersécurité de la CEDEAO, certaines incohérences, comme des interruptions d'Internet dans les États membres, révèlent des lacunes dans la mise en œuvre et l'adhésion.

Une autre stratégie pourrait faire intervenir des pays africains « champions », comme l'Égypte, le Ghana, Mauritanie, le Maroc et le Rwanda, qui ont fait preuve de leadership à propos d'enjeux spécifiques sur la gouvernance numérique en dirigeant et en orientant d'autres intervenants vers des objectifs collectifs spécifiques. Cette approche s'est déjà révélée prometteuse sur le continent, comme en témoignent, par exemple, les progrès obtenus dans le cadre la Convention de Malabo. En mars 2022, le Togo a réussi à rallier des chefs d'États africains sélectionnés pour adopter la Déclaration de Lomé sur la cybersécurité et la lutte contre la cybercriminalité, par laquelle les signataires se sont engagés à signer et à ratifier la Convention de Malabo. La convention est finalement entrée en vigueur en juin 2023 après que le minimum requis de 15 États membres de l'UA l'aient ratifiée. Les prochaines étapes peuvent faire intervenir l'utilisation de cette dynamique comme plateforme pour diriger le développement d'une approche harmonisée et adapter la convention aux besoins locaux ou régionaux.

Si elle est mise en œuvre de façon responsable et transparente, la stratégie sur la transformation numérique de l'Union africaine pourrait constituer un cadre solide pour l'évolution numérique du continent. En assurant la transparence et la reddition de comptes dans la mise en œuvre de cette stratégie, il serait possible de définir plus efficacement le paysage de la gouvernance numérique de l'Afrique.

Ouvrages cités

BBC News. 2014. « Edward Snowden: Leaks that exposed US spy programme. » BBC News, le 17 janvier. www.bbc.com/news/world-us-canada-23123964.

BSA. 2021. « What Is the CLOUD Act? » www.bsa.org/files/policy-filings/09012021whatiscloudact.pdf.

Coleman, Danielle. 2019. « Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws. » *Michigan Journal of Race and Law* 24 (2): 417–39. https://doi.org/10.36643/mjrl.24.2.digital.

Conseil d'État, République populaire de Chine 2023. « China to strengthen digital cooperation with African countries. » Le 20 octobre. https://english.www.gov.cn/news/202310/20/content_WS653213d0c6d0868f4e8e0799.html.

Gehl Sampath, Padmashree et Fiona Tregenna, eds. 2022. *Digital Sovereignty: African Perspectives.* Johannesburg, Afrique du Sud: Chaire de recherche en développement industriel de l'Afrique du Sud DSI/NRF. https://doi.org/10.5281/ZENODO.5851685.

Groupe de la Banque africaine de développement. 2024. « Congo : le nouveau datacenter financé par la Banque africaine de développement va consacrer la souveraineté numérique du pays et de la sous-région. » Actualités et événements, le 17 mai. www.afdb.org/fr/news-and-events/congo-le-nouveau-datacenter-finance-par-la-banque-africaine-de-developpement-va-consacrer-la-souverainete-numerique-du-pays-et-de-la-sous-region-70845.

———. 2023b. Cheikh Bakhoum, Sénégal Numérique : « Les rivalités géopolitiques dans le numérique peuvent favoriser une concurrence positive au profit des pays africains. » Entrevue sur la négociation des partenariats numériques de l'Afrique. www.geg.ox.ac.uk/content/cheikh-bakhoum-senegal-numerique-les-rivalites-geopolitiques-dans-le-numerique-peuvent.

———. 2023c. Motolani Peltola : « La recherche de la souveraineté numérique et de la propriété locale des données a des implications pour le développement des capacités locales. » Entrevue sur la négociation des partenariats numériques de l'Afrique. www.geg.ox.ac.uk/content/motolani-agbebi-peltola-la-recherche-de-la-souverainete-numerique-et-de-la-propriete-locale.

———. 2023d. Nnenna Ifeanyi-Ajufo : « L'état actuel de la cybersécurité en Afrique est la tendance à la cyber-militarisation de la cybergouvernance. » Entrevue sur la négociation des partenariats numériques de l'Afrique. www.geg.ox.ac.uk/content/nnenna-ifeanyi-ajufo-letat-actuel-de-la-cybersecurite-en-afrique-est-la-tendance-la-cyber.

———. 2023e. Teki Akuetteh, Africa Digital Rights Hub : « La société civile a le pouvoir de tenir les gouvernements responsables de l'application des droits numériques. » Entrevue sur la négociation des partenariats numériques de l'Afrique. www.geg.ox.ac.uk/content/teki-akuetteh-africa-digital-rights-hub-la-societe-civile-le-pouvoir-de-tenir-les.

———. 2023f. Tin Hinane El Kadi : « Les négociations collectives aideraient à maximiser les gains avec des entreprises technologiques. » Entrevue sur la négociation des partenariats numériques de l'Afrique. www.geg.ox.ac.uk/content/tin-hinane-el-kadi-les-negociations-collectives-aideraient-maximiser-les-gains-avec-des.

Guardian Nigeria. 2021. « [TRADUCTION] 70 % des agences gouvernementales hébergent des données à l'étranger en dépit d'une infrastructure locale de 220 millions de dollars. » *The Guardian* (Nigeria), le 4 juin. https://guardian.ng/technology/70-of-govt-agencies-host-dataabroad-despite-220m-local-infrastructure/.

Kadiri, Ghalia et Joan Tilouine. 2018. « À Addis-Abeba, le siège de l'Union africaine espionné par Pékin. » *Le Monde*, le 26 janvier. www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

Karombo, Tawanda. 2020. « The US development corp is betting $300 million on Africa's rising demand for data storage. » *Quartz*, le 11 décembre. https://qz.com/africa/1945156/us-dfc-bets-300m-on-africas-demand-for-data-storage-centers.

Le Monde. 2016. « Révélation Snowden : l'Afrique et les télécoms sous surveillance massive. » *Le Monde*, le 8 décembre. www.lemonde.fr/pixels/article/2016/12/08/revelations-snowden-les-elites-africaines-et-les-techniciens-des-telecommunications-surveilles-par-les-americains-et-les-britanniques_5045480_4408996.html.

Musoni, Melody, Poorva Karkare, Chloe Teevan et Ennatu Domingo. 2023. « Global approaches to digital sovereignty: Competing definitions and contrasting policy. » ECDPM Discussion Paper No 344. Mai. https://ecdpm.org/work/global-approaches-digital-sovereignty-competing-definitions-and-contrasting-policy.

Olander, Eric. 2021. « The Powerful Symbolism of The Huawei-Built Data Center Deal in Senegal. » Le projet Afrique-Chine, 24 juin. https://chinaglobalsouth.com/analysis/the-powerful-symbolism-of-the-huawei-data-center-deal-in-senegal/.

Programme Global Economic Governance. 2023a. Bulelani Jili : « Les décideurs africains doivent envisager le développement numérique, les flux de données et la gouvernance des données comme des éléments qui se renforcent mutuellement. » Entrevue sur la négociation des partenariats numériques de l'Afrique. www.geg.ox.ac.uk/content/bulelani-jili-les-decideurs-africains-doivent-envisager-le-developpement-numerique-les-flux.

Soulé, Folashadé. 2023. *La navigation des partenariats numériques de l'Afrique dans un contexte de rivalité mondiale*. Mémoire No 180 du CIGI. Waterloo, ON : CIGI. www.cigionline.org/publications/navigating-africas-digital-partnerships-in-a-context-of-global-rivalry/.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Credits

Directeur général de l'économie numérique (jusqu'en fevrier 2024) Robert Fay
Directrice, gestionnaire de programmes Dianna English
Gestionnaire de programmes Jenny Thiel
Réviseure Susan Bubak
Conception graphique Sami Choudhary

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org