PASAS

PLATEFORME D'ANALYSE, DE SUIVI ET D'APPRENTISSAGE AU SAHEL

PORTÉ PAR

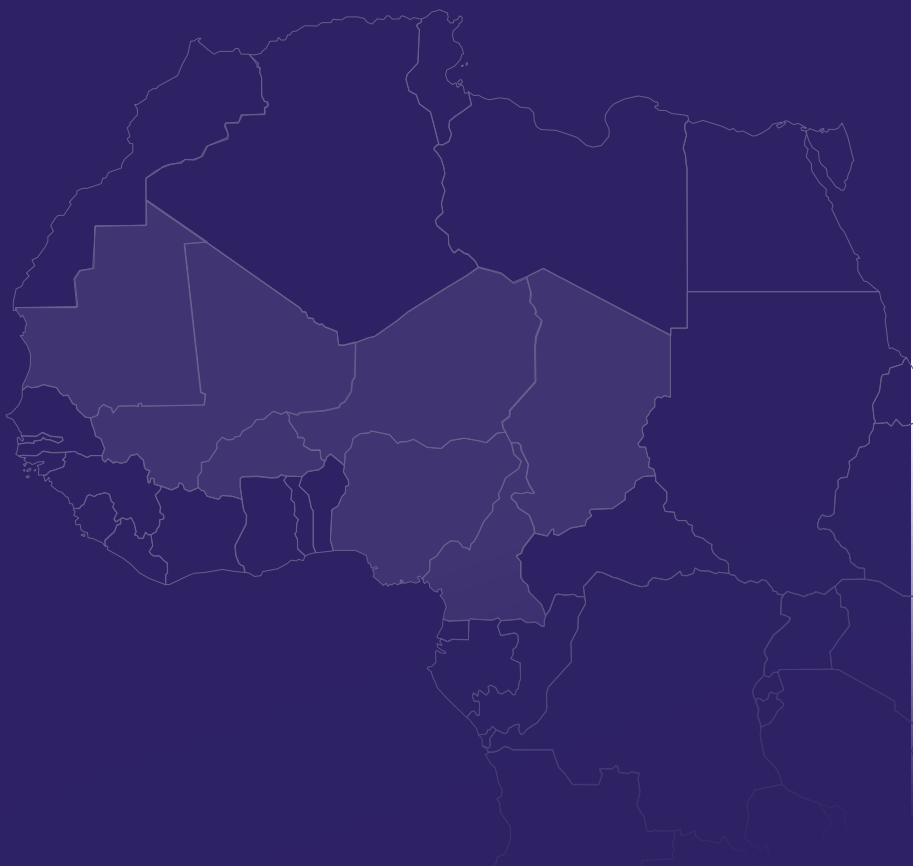
MINKA | AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT

Enjeux et défis de la souveraineté numérique de l'Afrique de l'Ouest en 2024 : du principe de souveraineté à une autonomie numérique stratégique, adaptative et résiliente

Julien Gavelle

17 septembre 2024

Public



IRD Institut de Recherche pour le Développement FRANCE | ICE FRANCE | UK International Development Partnership | Progress | Prosperity | ALLIANCE SAHEL

Merci de citer cet ouvrage comme suit :

(17 septembre 2024), Enjeux et défis de la souveraineté numérique de l'Afrique de l'ouest en 2024 : : du principe de souveraineté à une autonomie numérique stratégique, adaptative et résiliente, Plateforme d'Analyse du Suivi et d'Apprentissage au Sahel, Production Pasas. https://pasas-minka.fr

[Afrique de l'Ouest]

[Souveraineté, digital, sécurité, numérique]

SOMMAIRE

A l'instar des concepts de néolibéralisme[1], d'austérité[2] ou de résilience[3], la souveraineté numérique est un concept complexe aux enjeux multiples, dont l'ambiguïté fondamentale est également masquée par sa sur-mobilisation discursive sur le plan politique. Schématiquement, elle réside dans la tension entre, d'une part, la quête d'une indépendance numérique et, d'autre part, les dépendances inhérentes aux infrastructures et technologies mondiales. En outre, dans un contexte globalisé de plus en plus hétérogène et fragile, la mise en œuvre de véritables stratégies d'« autonomie partagée ou complémentaire » se complexifie davantage. En Afrique de L'Ouest notamment, des nationalismes s'expriment dans des répertoires et des processus de rupture en faveur d'une souveraineté défensive plus ou moins radicale, tout en s'engageant dans des régimes d'extraversion de plus en plus léonins et invasifs. Face à ces dynamiques, les aspects techniques de la souveraineté numérique, souvent négligés au profit d'approches plus politiques, doivent être appréhendés. La chaîne de valeur sur le plan technique de la souveraineté numérique englobe schématiquement le développement crucial des infrastructures numériques telles que les centres de données et la connectivité Internet, ainsi que la gestion locale des données incluant leur collecte, leur stockage sécurisé, leur protection technique et leur analyse. Parallèlement, l'innovation technologique joue un rôle central, soutenue par des initiatives visant à promouvoir les startups et à favoriser le développement de logiciels innovants. De plus, l'amélioration des compétences numériques par le biais de l'éducation et des formations professionnelles est essentielle pour renforcer cette infrastructure technique. Sur le plan politique, la mise en place de cadres juridiques et réglementaires robustes pour la protection des données, ainsi que pour la sécurité numérique, constitue une priorité. Enfin le respect des libertés collectives et individuelles favorise une prise en compte de ces dimensions. Face à l'étendue de ces sous-thèmes, ce policy brief ne se concentre que sur certains éléments clés, en particulier les problématiques qui apparaissent les plus immédiates, comme les questions de sécurité numérique qui affectent l'Afrique de l'Ouest de manière croissante ou les enjeux de l'IA : ceci à la lumière des enjeux nationaux et régionaux, dans un contexte géopolitique en évolution accélérée au niveau global, ajoutant des défis significatifs aux objectifs d'une souveraineté numérique durable.

I. Introduction

L'Afrique de l'Ouest se transforme grâce aux technologies numériques. Les investissements dans les infrastructures numériques (bien qu'en baisse en 2023[4]), la mise en

1 Harvey, David. Spaces of global capitalism: towards a theory of uneven geographical development. Verso, 2006

2 Blyth, Mark. Austerity: the history of a dangerous idea. Oxford university press, 2013

3 Chandler, David. Resilience: the governance of complexity. Routledge, 2014. Ces auteurs partagent une approche critique des concepts économiques et politiques qui, bien que complexes, sont souvent simplifiés et utilisés de manière rhétorique pour masquer les réalités et les inégalités sous-jacentes.

4 En 2023, les startups technologiques africaines ont levé 2,3 milliards de dollars, marquant une baisse de 54 % par rapport à l'année précédente. Cette diminution, la plus importante jamais enregistrée sur le continent, dépasse même la baisse observée lors de la crise de la COVID-19. Le nombre de tours de financement en actions a également chuté de 32 %. Cette tendance s'inscrit dans un contexte de ralentissement économique mondial, qui affecte l'écosystème africain avec un léger décalage, similaire à ce que l'on observe dans d'autres marchés émergents comme l'Amérique latine et l'Asie du Sud-Est. Malgré cette baisse, les niveaux de financement restent presque du double de ceux d'avant 2021, témoignant d'une croissance significative au cours des cinq dernières années. Au Nigeria, les préoccupations concernant la gouvernance des startups ont joué un rôle central, entraînant un ralentissement des investissements vers ces entreprises technologiques, à l'exception notable des fintechs

place de services publics en ligne, et le développement du secteur FinTech par exemple, contribuent à une amélioration notable de l'efficacité administrative et de l'inclusion financière. Toutefois elle demeure confrontée à des défis uniques en matière de souveraineté numérique[5], exacerbés par des contextes socio-économiques, politiques et technologiques qui complexifient davantage ses efforts pour rattraper son retard numérique. Tout d'abord, malgré une croissance de l'accessibilité des usagers[6], les investissements dans les infrastructures numériques demeurent souvent insuffisants, entretenant une faible couverture internet[7] et des disparités significatives entre les zones urbaines et rurales, et entre les pays. Ces limitations entravent l'accès équitable aux technologies numériques et ralentissent l'innovation ainsi que les dynamiques d'émulation régionale.

Par ailleurs, les cadres juridiques et réglementaires relatifs à la cybersécurité et à la protection des données sont généralement insuffisants ou mal appliqués, compromettant la capacité des États à protéger leurs infrastructures numériques et leurs données. Cette situation est aggravée par une dépendance vis-à-vis des technologies et des infrastructures étrangères, ce qui remet en question certains des objectifs clés de la souveraineté numérique, allant jusqu'à mettre en péril à terme la souveraineté globale de la région elle-même. De plus, celle-ci est tout particulièrement vulnérable aux cyberattaques en raison de capacités limitées en cybersécurité et d'un faible niveau de sensibilisation et d'éducation du public, des entreprises et même des administrations publiques sur ces enjeux, ce qui génère une chaîne d'impacts sur la croissance et les efforts de transition vers davantage de gouvernance digitale. Le manque de professionnels qualifiés en technologies de l'information et en cybersécurité est un autre problème, exacerbé par des systèmes éducatifs souvent mal équipés pour offrir une formation adéquate en compétences numériques.

Le Ghana, le Sénégal et le Nigeria offrent des exemples pertinents pour aborder ces défis. Le Ghana se distingue par son adoption proactive des technologies blockchain, qui visent à moderniser et sécuriser ses infrastructures numériques[8]. Le Sénégal, en tant

qui continuent de croître (voir note 7). A noter aussi que 52 % des pays africains ayant enregistré une transaction étaient francophones (14 sur 27), contre 46 % l'année précédente. De plus, les pays francophones représentaient 68 % des financements en actions en dehors des quatre principaux marchés (Afrique du Sud, Nigeria, Kenya, Égypte), une augmentation notable par rapport aux 38 % de 2022. (Partech,2024, Africa Tech Venture Capital Report 2023, https://partech-admin.prod.unomena.io/media/documents/2023_Partech-Africa-Tech-VC-Report.pdf)

5 Voir annexe 1, Tableau des objectifs de l'Union Africaine pour la transformation numérique de l'Afrique (2020-2030).

6 A titre d'exemple en 2023, le Sénégal a atteint un taux de pénétration d'Internet de 108,31 %. Au Ghana, ce taux était d'environ 70 % en janvier 2024, en hausse par rapport au 68 % de 2023. Au Nigeria, la pénétration d'Internet était de 45,5 % au début de 2024, avec une croissance de 2,2 millions d'utilisateurs entre janvier 2023 et janvier 2024 par rapport à l'année précédente, montrant une augmentation rapide des utilisateurs. Voir https://datareportal.com/reports/digital-2024-nigeria; https://www.statista.com/statistics/1171435/internet-penetration-rate-ghana/; https://www.socialnetlink.org/2023/09/30/senegal-le-taux-de-penetration-de-linternet-estime-a-10831/.

7 Par ailleurs si l'accessibilité reste croissante, les répartitions socio-économiques et conditions d'accessibilité et de fiabilité, notamment en termes de cybersécurité, restent préoccupantes.

8 La blockchain est une technologie de stockage et de transmission d'informations qui est décentralisée, sécurisée et transparente. Elle fonctionne sans organe central de contrôle, permettant à un réseau d'utilisateurs de partager une base de données commune. Chaque transaction est enregistrée dans un "bloc" qui est lié aux précédents, formant une chaîne inaltérable. Cette décentralisation assure que toutes les transactions sont vérifiables et quasiment impossibles à modifier sans consensus. La blockchain est utilisée pour les cryptomonnaies comme Bitcoin, permettant des transactions financières sécurisées,

que leader francophone de la région, est en première ligne avec des initiatives telles que la eCFA, une crypto-monnaie nationale[9], illustrant une approche stratégique en matière d'innovation financière[10] ou plus récemment l'investissement dans les data center « neutres » . Enfin, le Nigeria, hub régional des fintechs[11], incarne un modèle de dynamisme économique et technologique. Ces pays jouent un rôle clé dans l'établissement de normes et de cadres juridiques régionaux pour soutenir le développement durable des technologies numériques[12]. Néanmoins, malgré leur indéniable avance-

et pour les « contrats intelligents », qui s'exécutent automatiquement lorsqu'un ensemble de conditions est rempli (pour une explication didactique voir Drescher, Daniel, Blockchain Basics: A Non-Technical Introduction in 25 Steps. Apress, 2017, pp. 181-193). La transparence et la sécurité de la blockchain en font une technologie révolutionnaire dans divers domaines, de la finance à la logistique. Pour les gouvernements ouest-africains, l'intérêt réside prioritairement dans la possibilité d'améliorer la transparence des processus administratifs, de réduire la corruption et d'accroître l'efficacité des services publics, tout en renforçant la confiance des citoyens dans les institutions. Voir par exemple Blockchain Adoption in Africa: Trends in Market Activity and Policy Development," November 2023, background note prepared for the African AI and Blockchain Policy Forum, 15-16 November 2023, OECD, https://www.oecd.org/finance/blockchain/Blockchain-adoption-in-Africa-background-note.pdf.
L'article de David Mhlanga est par ailleurs une excellente introduction à ces enjeux : "The Pivotal Role of Blockchain Technology in Africa's Development: A Comprehensive Review," College of Business and Economics,

9Faute de place, cette note n'abordera pas la problématique des cryptomonnaies en Afrique de l'Ouest agrégeant pourtant ses propres enjeux au regard des questions de souveraineté. Pour un état des lieux éclairant, voir par exemple : ChainAnalysis, The 2023 Geography of Cryptocurrency Report: Everything You Need to Know About Regional Trends in Crypto Adoption, October 2023. https://www.chainalysis.com/blog/africa-cryptocurrency-adoption/; Agence Ecofin, "Afrique subsaharienne : les transactions en cryptomonnaies ont atteint 117,1 milliards entre juillet 2022 et juin 2023." https://www.agenceecofin.com/actualites/2909-112229-afrique-subsaharienne-les-transactions-en-cryptomonnaies-ont-atteint-117-1milliards-entre-juillet-2022-et-juin-2023; Henri Louis Vedie, L'émergence des cryptomonnaies en Afrique : réalité ou surévaluation ? Research Paper - N° 10/22 - Décembre 2022. À noter que les cryptomonnaies participe à générer des dynamiques positives associés à des problématiques complexes pour le développement dans le giron des Fintech (Ankun Liu, Orria Goni, et Aiaze Mitha, Cryptocurrency in Africa: Alternative Opportunities for Advancing the Sustainable Development Goals? UNDP, December 2022). Elles soulèvent de graves enjeux économiques, dont fiscaux, et même sécuritaires (ADF, Islamic State Group Uses Cryptocurrency to Fund Attacks in Africa, DAILY NEWS, 26 mars 2024).

10 https://african.business/2017/05/economy/senegal-creates-digital-currency-history

11 Le terme "fintech" est une abréviation de "financial technology", qui désigne l'ensemble des technologies et des innovations appliquées au secteur des services financiers. Il inclut des applications de paiements mobiles, des plateformes de financement participatif, des systèmes de gestion de patrimoine automatisés, des services bancaires en ligne, et bien plus encore. Les fintechs visent de manière générique à améliorer et à automatiser l'offre et l'utilisation des services financiers. Le Nigeria s'est affirmé comme un hub régional pour les fintechs en Afrique, en particulier au sein de l'écosystème technologique de Lagos, souvent surnommée la "Silicon Lagoon". Cette ascension repose sur divers facteurs, notamment une population jeune et dynamique, un taux de pénétration mobile élevé, et des innovations en matière de régulation financière. Voir Occasional paper no 76 - Fintech Evolution and Development in Nigeria, Central Bank of Nigeria,https://www.cbn.gov.ng/Out/2023/RSD/OCCASIONAL%20PAPER%20NO%2076%20-%20Fintech%20Evolution%20and%20Development%20in%20Nigeria.pdf). A noter que ce positionnement croissant est également associé à un investissement dans la recherche et l'analyse continue, favorisant des évolutions majeures dans ce secteur numérique stratégique.

12 Le Togo se hisse selon la société nPerf au top des performances en termes de connectivité mobile en Afrique de l'Ouest suivi du Bénin et du Sénégal : Baromètre des connexions Internet mobiles en Afrique de l'Ouest, (Mai 2024), tests effectués du 01/01/2023 - 31/12/2023, https://media.nperf.com/files/publications/BF/2024-05-02_Barometre_connexions_mobiles__Afrique-de-l-Ouest-2023.pdf. Afin d'éviter de reporter des données potentiellement biaisées par une logique sous-jacente commerciale ou de lobbying, nous avons limité l'utilisation de références produites par des

ment, ils font face à des défis significatifs comme la régulation, le financement, la sécurité numérique et les problématiques d'infrastructure, soulignant la nécessité de stratégies régionales adaptées.

Par ailleurs, l'extraversion régionale de ces avancées est confrontée à des voisinages complexes sur le plan politique, et se révélant plus fortement vulnérables aux entrismes étrangers[13]. La Chine et la Russie prônent en effet une version restreinte et contrôlée de l'internet, fragilisant ainsi les opportunités d'application considérables[14] du digital en faveur du développement et de l'autonomie techno-politique des pays Ouest africains. La Chine par exemple propose des solutions techno-financières très attractives dans le cadre de la route de la soie digitale, mais dont les impacts à moyen et long terme sont à ce titre préoccupants. Le potentiel de construction d'un modèle digital autour d'une coopération et mutualisation transparente reste pourtant essentiel à la souveraineté et au développement global de la région. A court et moyen terme, tandis que les économies mondiales sont bousculées par des tensions géopolitiques accrues, la croissance numérique stimulée par une dynamique de coopération régionale innovante représente un des vecteurs centraux de résilience face, notamment, aux fluctuations des IDE[15] ou aux replis plausibles de l'APD suite aux récessions de crise subies par les pays donateurs [16].

II. Risques, impacts et enjeux de la souveraineté numérique en Afrique de l'Ouest

1. Cybermenaces : la cyber-résilience comme condition majeure de la souveraineté numérique

sociétés commerciales sans l'éviter systématiquement. Une attention particulière et une prudence méthodologique vis à vis des sources d'information sur ces thématiques devra s'accroitre dans les années à venir, tant la question de la souveraineté numérique devient également un enjeu géostratégique, y compris en termes de communication.

13 La création de l'Alliance des États du Sahel (AES) en septembre 2023 par le Burkina Faso, le Mali et le Niger est sans doute l'illustration la plus saisissante car elle représente un changement majeur dans la géopolitique de l'Afrique de l'Ouest. Cette initiative conduite suite à des coups d'État militaires successifs depuis 2020, a conduit ces pays à se retirer de la CEDEAO, perturbant à terme les efforts de régulation régionale. En conséquence, les tentatives pour harmoniser les régulations en matière de cybersécurité et de protection des données pourraient se retrouver fragmentées, compliquant l'attraction des investissements nécessaires au développement des infrastructures numériques. Alternativement, cela renforce le positionnement de sociétés chinoises telles qu'Huawei (https://traceinfos.fr/international-le-mali-et-huawei-signent-un-memorandum-dentente-pour-accelerer-le-projet-mali-numerique/) . Sur l'AES et ses enjeux voir notamment https://www.orfonline.org/expert-speak/the-alliance-of-sahel-states-a-regional-crisis-in-troubled-west-africa; https://www.africanresearchers.org/decoding-the-alliance-of-sahel-states-west-africas-geopolitical-shift-and-implications/.

14Se reporter à l'annexe 2 pour un échantillon. Tableau 2 : Souveraineté et opportunités numériques en Afrique de l'Ouest : enjeux et conditions de déploiement

15 Les flux d'IDE (investissements directs étrangers) vers l'Afrique ont diminué de 3 % en 2023, tandis que la valeur estimée des accords de financement de projets internationaux sur le continent a chuté de 50 % en 2023, après une baisse de 20 % en 2022. Cependant, certains secteurs tels que l'industrie chimique, l'électronique et les projets d'hydrogène vert ont montré une résilience notable. À noter également que les investissements intra-régionaux montrent une vive dynamique, y compris dans les secteurs digitech. Voir World Investment Report 2024: Investment Facilitation and Digital Government, UNCTAD, 2024.

16 L'APD (Aide Pour le Développement) semble en progrès relatif mais pourrait ne pas résister à de nouveaux chocs tandis que les impacts et évolutions de la guerre en Ukraine mettaient d'ores et déjà sous tension les pays donateurs fin 2022. Une crise majeure pourrait être à venir selon LOCDE. Global Outlook on Financing for Sustainable Development 2023: No Sustainability Without Equity, OECD, 2022.

Les cybermenaces ont des répercussions significatives sur les économies africaines, avec des pertes estimées à environ 10 % du PIB du continent en 2021 et une croissance de 70% des cyberattaques en 2023[17].

Les secteurs privé et public sont tous deux touchés, avec des attaques visant les infrastructures critiques telles que les systèmes énergétiques, de transport et de santé, ainsi que les institutions gouvernementales et les entreprises privées. Les impacts opérationnels des cyberattaques sont également préoccupants, avec des interruptions de service pouvant compromettre la prestation de soins médicaux, perturber les transactions financières et compromettre la confiance des consommateurs dans les services en ligne. De plus, les cyberattaques entravent le développement socio-économique en détournant des ressources nécessaires et en créant un climat d'incertitude et de méfiance, ce qui peut dissuader les investisseurs et retarder les réformes nécessaires pour renforcer la sécurité et la résilience des systèmes.

Enfin, sur le plan de la sécurité nationale, les cyberattaques représentent une menace directe, avec la possibilité de voler des données sensibles, de perturber des opérations essentielles et d'éroder la confiance du public dans les institutions. Ces menaces soulignent la synchronisation des enjeux de cyber-résilience dans les objectifs de construction d'une souveraineté numérique effective.

2. Types de cybermenaces au Ghana, Nigeria et Sénégal

En examinant les cybermenaces et les enjeux de la souveraineté numérique en Afrique de l'Ouest, notamment à travers les cas du Ghana, du Nigeria et du Sénégal, plusieurs éléments émergent.

D'une part, les menaces sont diverses, allant des attaques classiques telles que le phishing[18] ou spear phishing[19] et les logiciels rançonneurs aux assauts sophistiqués comme

17 Julie Le Bolzer,En Afrique, la menace cyber enfle au rythme de la digitalisation," Les Échos, consulté le 26 juillet 2024, https://www.lesechos.fr/thema/articles/en-afrique-la-menace-cyber-enfle-au-rythme-de-la-digitalisation-2085287

18 Le phishing, ou hameçonnage, est une technique frauduleuse où des cybercriminels envoient des messages trompeurs, souvent par e-mail, pour inciter les destinataires à divulguer leurs informations personnelles. Ces messages semblent authentiques, mais ils visent à voler des identifiants de connexion, des données financières ou d'autres informations sensibles. Voir Whitty, M. T., & Doodson, J. (2020). The Real Online Threats to Real People: How Online Interactions Affect Our Offline Lives. Journal of Research in Crime and Delinquency, 57(3), 324-355; Kumaraguru, P., Rhee, Y., & Acquisti, A. (2017). Protecting people from phishing: The design and evaluation of an embedded training email system. International Journal of Human-Computer Studies, 98, 179-201.

19 Le spear phishing est une forme ciblée d'hameçonnage où les cyber-attaquants personnalisent leurs messages trompeurs pour des individus ou des organisations spécifiques. Contrairement aux e-mails d'hameçonnage traditionnels envoyés en masse, le spear phishing utilise des informations personnalisées pour paraître légitime, visant à inciter la victime à divulguer des informations sensibles ou à effectuer des actions malveillantes (voir Halevi, Tzipora & Memon, Nasir & Nov, Oded. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. SSRN Electronic Journal. Et plus spécifiquement les mécanismes socio-psychologiques du spear-phising dans Xu, Tianhao & Singh, Kuldeep & Rajivan, Prashanth. (2023). Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. Applied Ergonomics. 108.). De 2020 à 2022, une campagne nommée "DangerousSavanna" a ciblé les principales institutions financières des pays africains francophones tels que le Sénégal ou la Côte d'Ivoire en utilisant le spear phishing. Cette campagne utilisait des courriels en français contenant des pièces jointes malveillantes pour infecter les systèmes des entreprises visées. Les pirates ont également utilisé des domaines similaires pour imiter

les attaques par déni de service distribué (DDoS)[20]. D'autre part, les acteurs impliqués dans ces activités malveillantes varient, allant des hacktivistes aux cybercriminels organisés, en passant par les États-nations[21] et les cyberterroristes[22]. Ces menaces évolutives[23] ont des impacts multidimensionnels, allant des pertes financières directes à des conséquences sur le développement socio-économique, la stabilité politique et la sécurité nationale.

Le cyberactivisme[24] en Afrique de l'Ouest est devenu un outil puissant pour la mobilisation sociale, la dénonciation de la corruption et l'appel à des réformes politiques. Des mouvements tels que #EndSARS au Nigeria démontrent la capacité des campagnes en ligne à attirer l'attention internationale et galvaniser un soutien massif. Cependant, cette forme d'activisme soulève des questions cruciales de souveraineté numérique et ses interprétations au regard des libertés publiques notamment, là où les États cherchent à contrôler et réguler l'espace numérique pour préserver la stabilité et la sécurité nationale. Les gouvernements de la région voient souvent le cyber-activisme comme une menace à leur contrôle de l'information, ce qui conduit à l'adoption de cadres législatifs destinés à lutter contre la cyber-criminalité mais de plus en

d'autres institutions financières ('DangerousSavanna' hackers targeted financial institutions in Africa For Two Years, Infosecurity Magazine, 7 septembre 2022).

20 Les attaques par déni de service distribué (DDoS) sont des cyberattaques où des multiples systèmes informatiques ciblent simultanément un seul système, surchargeant ses capacités et le rendant inaccessible à ses utilisateurs. Voir Hayes, M., & Akam, N. (2017). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA) (pp. 1-8) ; Dohaji, Mazen. "DDoS Attacks On The Rise In Africa." CIO Africa, 1 septembre 2023.

21 Voir section 1.3

22 Le cyber terrorisme désigne l'utilisation de technologies informatiques et de réseaux, notamment l'internet, pour mener des attaques visant à provoquer des perturbations, des dommages ou de la peur dans des objectifs politiques, idéologiques ou religieux. En 2016, le secteur pétrolier et gazier nigérian a subi des cyberattaques sophistiquées, perturbant la production et la distribution de pétrole et de gaz, entraînant des pertes financières importantes et compromettant des informations sensibles. Voir Achunike, Victor U., & Egbuna, Fidelis C. (2020). Synopsis of Cyber-attacks Incidents and Impacts on Oil and Gas Critical Infrastructures: A Nigerian Perspective. International Journal of Advances in Engineering and Management (IJAEM), 2(3), 335-343. En 2019, durant les élections générales, des hackers ont tenté de manipuler les résultats en infiltrant les systèmes de la Commission électorale nationale indépendante (INEC), soulevant des préoccupations majeures sur l'intégrité électorale. Les institutions financières nigérianes ont également été ciblées par des attaques par déni de service distribué (DDoS) et des campagnes de phishing, perturbant les services bancaires en ligne et menaçant la sécurité des transactions financières.

23 Par exemple les rançongiciels, qui représentent une menace majeure en ciblant régulièrement les infrastructures critiques. Leur impact est également exacerbé par l'émergence de nouveaux modèles organisationnels parmi les cybercriminels, tels que les programmes d'affiliation et les plateformes de rançongiciels en tant que service. Ces programmes permettent une professionnalisation et une rationalisation des opérations, augmentant ainsi l'efficacité et l'impact des attaques. L'évolution des tactiques cybercriminelles montre également une adaptation rapide aux failles humaines et technologiques. L'hameçonnage par courriel reste par exemple un vecteur d'attaque majeur, exploité par les criminels pour diverses cyberinfractions, y compris les rançongiciels et les escroqueries en ligne (Kshetri, N. 2019. Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), voir également le rapport d'Interpol sur la cybersécurité en Afrique de 2024.

24 Le cyberactivisme inclut des pétitions en ligne, le hashtag activism, la dénonciation de comportements répréhensibles (exposition de comportements répréhensibles ou de documents secrets par des plateformes comme WikiLeaks) et le hacktivisme, combinant hacking et activisme pour des actions directes.

plus restrictifs ou sur-interprétés, au risque de s'approcher des modèles russes ou chinois[25], quand ces modèles ne sont pas ouvertement appliqués[26]. Des lois comme le *Cybercrimes Act* de 2015 au Nigeria et le Code des Communications Électroniques de 2018 au Sénégal, bien qu'initialement destinées à prévenir les cyber-crimes, sont souvent critiquées pour restreindre la liberté d'expression et cibler les activistes en ligne ou les journalistes[27], ce qui n'éteint pas nécessairement toute contestation mais peut en retour stimuler sa radicalisation. Ainsi, le groupe de hackers *Mysterious Team* a rendu plusieurs sites web gouvernementaux sénégalais inaccessibles en mai 2023 *via* des attaques par déni de service (DDoS). Ils ont revendiqué ces attaques sur Twitter avec le hashtag #FreeSenegal, dénonçant alors la répression politique.
Quelle que soit la légitimité des motivations politiques de ces attaques, elles tombent effectivement sous le coup du code pénal et de la loi sur la cyber-criminalité[28]. Mais les cyber-activistes sont conduis à naviguer dans des cadres juridiques de plus en plus complexes et des mécanismes de cyber-répression croissants, alignés sur les changements géopolitiques[29].

3. La souveraineté numérique Ouest africaine à l'épreuve de la Route de la soie numérique et du modèle techno-politique « Runet »

Les dynamiques de multipolarisation des États en Afrique ont exacerbé les préoccupations liées à la souveraineté et à la résilience numériques. La diversification des partenariats internationaux et une redéfinition des alliances traditionnelles ont des implications directes sur la manière dont les États africains gèrent leur cybersécurité et leur autonomie technologique. Les infrastructures numériques, tardivement mises en place au niveau national, souvent sous-développées et vulnérables aux cyberattaques sophistiquées, rendent les pays dépendants des expertises étrangères, ce qui accroît leurs vulnérabilités face aux pressions et entrismes externes, y compris les plus offensifs sur le plan commercial[30]. Par ailleurs, dans l'optique de rattraper à moindre coût les retards numériques et sans véritable alternative de financement, les États cèdent aux solutions technologiques et financières chinoises se présentant sous forme de "packaging techno-financier", clé en main et redoutablement attractif. Ainsi les fournisseurs

25 Polyakova, A., & Meserole, C. (2010). Exporting digital authoritarianism: The Russian and Chinese models. Democracy and Disorder,Brookings, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf; Cipesa. (2019). Digital Rights in Africa: Challenges and Policy Options.
26 « Modification de la loi sur la cybercriminalité au Niger : RSF alerte sur les risques pour les journalistes », Reporter sans Frontière, 19 juin 2024, https://rsf.org/fr/modification-de-la-loi-sur-la-cybercriminalit%C3%A9-au-niger-rsf-alerte-sur-les-risques-pour-les
27 https://www.article19.org/resources/senegal-fake-news-and-disinformation-laws-threaten-freedom-of-expression/; https://www.theafricareport.com/348123/nigeria-cybercrime-law-still-used-to-harass-citizens-despite-amendment/
28 Les articles 431-8, 431-9, et 431-10 du Code Pénal sénégalais, ainsi que les articles 431-1 et 431-3 de la loi sur la cybercriminalité du sénégal (https://adie.sn/sites/default/files/lois/4-cybercrime.pdf) .
29 Buss, H. (2022). Digital Rights Are Human Rights: An Introduction to the State of Affairs and Challenges in Africa. Friedrich-Ebert-Stiftung.
30 Il existe une corrélation significative entre l'aide chinoise à l'Afrique et les exportations chinoises vers le continent, et ce dans la plupart des secteurs. Voir par exemple le secteur de la santé Shajalal, M., Xu, J., Jing, J., King, M., Zhang, J., Wang, P., Bouey, J., & Cheng, F. (2017). China's engagement with development assistance for health in Africa. Global Health Research and Policy, 2.

chinois tels que Huawei et ZTE[31] par exemple attirent non seulement par leur technologie, mais aussi par les solutions de financement qu'ils proposent, telles que le schéma "EPC+F" (ingénierie, approvisionnement, construction + financement)[32]. Ce dispositif du Digital Silk Road (DSR) est une composante du BRI en vigueur depuis 2013[33] et cette route de la soie numérique a rencontré peu d'obstacles[34] ou a su s'adapter aux tentatives de contrer les termes de son expansion[35].

L'incident de janvier 2017, où les informaticiens de l'Union africaine (UA) ont détecté des activités anormales sur leurs serveurs, révèle des enjeux majeurs[36]. La découverte

31 ZTE (Zhongxing Telecommunication Equipment Corporation) est une entreprise chinoise fondée en 1985, spécialisée dans les équipements de télécommunications et les solutions réseaux. Elle est un acteur clé dans le déploiement des infrastructures 4G et 5G à l'échelle mondiale. Toutefois, ZTE a été critiquée pour ses liens étroits avec le gouvernement chinois et ses pratiques commerciales, ce qui a conduit à des sanctions et des restrictions par certains pays, notamment les États-Unis, en raison de préoccupations liées à la sécurité nationale et à l'espionnage potentiel. Les restrictions furent levées sous l'administration Trump. https://www.nytimes.com/2018/07/13/business/zte-ban-trump.html

32 https://theconversation.com/africa-needs-china-for-its-digital-development-but-at-what-price-222905

33 La Belt and Road Initiative (BRI), lancée par la Chine en 2013, vise à améliorer la connectivité entre l'Asie, l'Afrique et l'Europe. Elle se divise en deux axes principaux : la Ceinture Économique de la Route de la Soie, centrée sur les infrastructures de transport et l'énergie, et la Route de la Soie Maritime, axée sur les ports et la logistique. Bien que la BRI stimule le développement économique et les infrastructures, elle soulève des préoccupations liées, entre autres, à l'endettement et à l'influence politique croissante de la Chine. Pour différentes perspectives sur la BRI et la DSR voir par exemple Philippe Copinschi et al., "La BRI et la stratégie de sécurisation des approvisionnements énergétiques chinois en Afrique," Observatoire de la sécurité des flux et des matières énergétiques, 2019 ; et sur la DSR voir par exemple Tugendhat, Henry; Voo, Julia (2021) : China's Digital Silk Road in Africa and the Future of Internet Governance, Policy Brief, No. 60/2021, China Africa Research Initiative (CARI), School of Advanced International Studies (SAIS), Johns Hopkins University, Washington, DC

34 A l'exception notable du plan Global Gateway de l'Union européenne de 300 milliards d'euros visant notamment à contrer la BRI de 2021 à 2027, (https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6433). La part prévisionnelle dédiée au digital est de 100 milliards d'euros et vise à accélérer la transition numérique en Afrique, soutenir la construction de réseaux de câbles à fibres optiques dans toute l'Afrique subsaharienne, et favoriser le déploiement de services et d'innovations numériques (https://international-partnerships.ec.europa.eu/system/files/2023-10/GG_Factsheet_Africa_Digital%20Transition.pdf). Il convient de noter aussi le lancement récent du programme régional pour la transformation numérique de l'Afrique et l'intégration numérique en Afrique de l'Ouest (DTfA/WARDIP), initiative de la Banque mondiale visant à accélérer la transformation numérique dans la région avec un investissement de 266,5 millions USD financé par l'IDA. Ce programme cherche à améliorer l'accès à Internet en Gambie, en Guinée, en Guinée-Bissau et en Mauritanie en réduisant les coûts des services, en encourageant la concurrence entre fournisseurs, tout en améliorant les infrastructures. https://www.banquemondiale.org/fr/news/press-release/2023/12/01/accelerating-digital-transformation-in-west-africa#:~:text=Le%20Programme%20r%C3%A9gional%20pour%20la,concurrence%20entre%20les%20fournisseurs%20de.

35 Valerio Fabbri, "The Great Leap of China's Tech Companies in Africa," Geopolitica Info, 2023. https://www.geopolitica.info/great-leap-china-tech-africa/.

36 https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html; https://www.bbc.co.uk/news/resources/idt-sh/Huawei, Un évènement également ultérieur rapporté par Raphael Satter, "Exclusive-Suspected Chinese hackers stole camera footage from African Union - memo," Reuters, December 16, 2020. Pour une approche très éclairante des dynamiques de surveillances chinoises nationales et globalisantes voir la conférence de Sheena Chestnut Greitens, Surveillance with Chinese Characteristics: The Development and Global Adoption of Chinese Policing Technology, draft disponible a https://ncgg.princeton.edu/IR%20Colloquium/GreitensSept2019.pdf. L'auteur décrit les processus de répressions associées aux usages digitaux en Chine et souligne que les analyses politiques ont très

que des données étaient détournées chaque nuit vers Shanghai sur une période de cinq ans met en lumière la vulnérabilité des infrastructures numériques africaines aux cybermenaces sophistiquées, notamment quand ces dernières sont pré-implantées dans le cadre de ces schémas "EPC+F". Le bâtiment de l'Union africaine avait été en effet entièrement offert et financé par la China State Construction Engineering Corporation (CSCEC), acteur majeur de la BRI[37] et digitalisé par Huawei. Cette fuite de données, survenue de janvier 2012 à janvier 2017, souligne la capacité d'acteurs étrangers à exploiter les faiblesses des systèmes numériques africains, en l'occurrence en implémentant des failles ou des *backdoor*[38], compromettant ainsi la souveraineté

largement sous-estimé l'ampleur de l'utilisation des technologies de surveillance et des stratégies policières chinoises à travers le monde, ainsi que la rapidité avec laquelle elles ont été adoptées à l'échelle mondiale.

37 Les entreprises chinoises ayant investi en Afrique maintiennent des marges bénéficiaires élevées, même en dépit de contextes politiques complexes. Des études auprès de ces entreprises révèlent des marges pouvant atteindre jusqu'à 20%, incitant des sociétés à étendre leurs opérations sur le continent. Huawei n'a pas hésité à maximiser ses profits dans des environnements politiquement instables, bénéficiant notamment de l'absence de concurrence occidentale, souvent réticente à s'engager dans de telles conditions en Afrique. Voir à ce titre le chapitre éclairant de Bulelani Jili, "The Spread of Chinese Surveillance Tools in Africa: A Focus on Ethiopia and Kenya," in Africa–Europe Cooperation and Digital Transformation, 1st Edition, Routledge, 2022, ainsi que les analyses de William C. Kirby, Billy Chan, et John P. McHugh, "Huawei: A Global Tech Giant in the Crossfire of a Digital Cold War," Harvard Business School Case 320-089, mars 2020. Globalement la transition économique de la Chine influence ses relations avec l'Afrique, en introduisant des changements significatifs dans le commerce, les investissements, la stabilisation fiscale, l'internationalisation du renminbi (RMB), ainsi que dans les échanges culturels et éducatifs. Bien que la Chine demeure un partenaire commercial majeur pour l'Afrique, avec cependant une balance commerciale toujours aussi asymétrique, les investissements publics chinois dans les infrastructures se sont réduits, au profit d'une approche plus orientée vers l'industrialisation par les investissements directs étrangers (IDE). De plus, la Chine cherche à accroître l'utilisation du RMB en Afrique tout en adaptant ses stratégies d'investissement et de stabilisation fiscale en fonction de l'évolution des contextes nationaux et continentaux. Au niveau continental, sa stratégie tendancielle est de rééchelonner la dette plutôt que de la réduire (ce qui est une innovation récente de Pékin). Ce reprofilage financier permet ici à la Chine de renforcer son influence et son entrée sur des secteurs clés tels que le numérique et à travers le contrôle des chaînes d'approvisionnement stratégiques dans les technologies émergentes.
Voir Gbadamosi, Olumide. How Is China's Economic Transition Affecting Its Relations With Africa?" Carnegie Endowment for International Peace, 5 mai 2024, https://carnegieendowment.org/research/2024/05/how-is-chinas-economic-transition-affecting-its-relations-with-africa?lang=en&center=russia-eurasia, ainsi que Song-Pehamberger, David. "Controlling Tomorrow: China's Dominance Over Future Strategic Supply Chains," The Diplomat, 21 août 2024.

38 Une backdoor (ou porte dérobée) est une méthode secrète utilisée pour accéder à un système, un réseau, ou une application en contournant les mécanismes de sécurité habituels. Bien qu'elle soit souvent installée à des fins malveillantes, permettant ainsi un accès non autorisé aux systèmes, elle peut également être délibérément mise en place par des développeurs pour des besoins légitimes, tels que la maintenance, le dépannage ou les tests. Cependant, ces accès privilégiés présentent un risque significatif si des contrôles appropriés ne sont pas en place, car ils peuvent être exploités par des acteurs malveillants. Dans le contexte des infrastructures numériques installées en Afrique de l'Ouest, le contrôle et la gestion des backdoors, y compris celles potentiellement intégrées par les développeurs, sont cruciaux pour garantir la sécurité. Il s'agit de manière générale d'établir des audits continus du code source, la vérification des composants logiciels, et la surveillance régulière des systèmes, processus essentiels pour détecter toute porte dérobée non autorisée (avec dorénavant l'appui de l'IA). Cela constitue un enjeu technique majeur dans la protection des infrastructures critiques de la région contre les cybermenaces, particulièrement celles portées par des pays étrangers aux intentions incertaines. Il existe cependant d'autres techniques d'implémentations et des techniques accessibles pour les détecter. Voir par exemple les formes

des États et des institutions régionales. A noter que le schéma de financement établit également une dette à variables multiples [39] et entrainant par ailleurs une ventilation des effets visés en termes de gouvernance et de droits fondamentaux liés à la conditionnalité des APD[40], quand il ne s'agit pas d'une stricte exportation des approches répressives et de contrôle des populations[41]. Quant aux transferts techniques (TT) souhaitables et promis par cet arrimage massif aux technologies numériques chinoises, il n'est que très limité et conditionné par la stratégie politico-commerciale globale de la BRI[42].

Plus tardivement, la Russie a lancé aussi une offensive en Afrique, d'orientation plus techno-politique, ciblant notamment des pays tels que la Libye (région de la Cyrénaïque), Madagascar, la Centrafrique (RCA), le Soudan du Sud, le Mali, le Burkina Faso et le Niger. Certes la déclaration du second sommet Afrique-Russie de 2023 semble s'aligner sur des principes clefs d'une souveraineté numérique plus extravertie vers une partie de l'écosystème numérique global[43]. Cependant depuis une dizaine d'années, la Russie a influencé ces régions par la propagande et la désinformation à

intrusives bien connues ci-après : https://www.mandiant.com/resources/reports/apt41-double-dragon-dual-espionage-and-cyber-crime-operation.

39 Arnold, S. (2024). Africa's roads to digital development: paving the way for Chinese structural power in the ICT sector? Review of International Political Economy, 1–25 (*https://www.tandfonline.com/doi/epdf/10.1080/09692290.2023.2297363?needAccess=true*).

40 Il s'agit sans doute d'une des causes régulièrement évoquées mais encore trop peu décrite des processus de rupture démocratique dans des pays ouest africains, en particulier de la bande sahélienne. Voir Li, X. Does Conditionality Still Work? China's Development Assistance and Democracy in Africa. Chin. Polit. Sci. Rev. 2, 201–220 (2017).

41Erin Baggott Carter et Brett L. Carter, "Exporting the Tools of Dictatorship: The Politics of China's Technology Transfers to Africa," Working Paper 122, dec 2022, AIDDATA https://docs.aiddata.org/ad4/pdfs/WPS122_Exporting_the_Tools_of_Dictatorship__The_Politics_of_Chinas_Technology_Transfers_to_Africa.pdf

42 Bien que ZTE et Huawei aient engagé des initiatives de localisation promettant des liens significatifs, elles n'ont offert aucune opportunité d'apprentissage substantielle pour améliorer les compétences technologiques des entités locales. Ce qui semble au départ être des efforts de développement facilitant les transferts de technologie se révèle en réalité être des mécanismes de diffusion des infrastructures, matériels, logiciels, processus et normes chinois, formant ainsi des systèmes numériques distincts et dépendants. Voir sur ce point l'article documenté de Tin Hinane El-Kadi. "Learning along the Digital Silk Road? Technology transfer, power, and Chinese ICT corporations in North Africa." The Information Society: An International Journal, vol. 40, no. 2, 2024.

43 La déclaration du sommet Russie-Afrique de 2023 met en avant une volonté mutuelle de renforcer les relations bilatérales entre la Russie et les pays africains, en se concentrant sur des domaines clés tels que le commerce, la sécurité, la culture, et l'éducation. Le texte insiste sur le respect de la souveraineté des États africains et la non-ingérence, tout en promouvant des partenariats économiques visant à développer les infrastructures, l'industrialisation, et l'agriculture en Afrique. La coopération en matière de sécurité est également un point fort, avec un accent mis sur la lutte contre le terrorisme et le renforcement des capacités militaires. En parallèle, la déclaration souligne l'importance des échanges culturels et éducatifs, ainsi que la nécessité de réformer les institutions internationales pour une meilleure représentation des pays africains. La déclaration exprime au prime abord un soutien à un multilatéralisme ouvert, mais positionne en réalité la Russie et l'Afrique comme des acteurs-partenaires clés dans un monde multipolaire en mutation. https://summitafrica.ru/fr/about-summit/declaration-2023/

travers ses médias en ligne[44] et le groupe Wagner[45] ou African Initiative, nouvelle plateforme d'influence portée par Moscou qui prend le relais du groupe privé et de son African Back Office après son démantèlement[46]. Elle a ainsi fortement accéléré la déstabilisation de pays ouest-africains tout en renforçant le logiciel idéologique de ces nouveaux régimes militaires ancrés dans un tropisme décolonial. Des experts expliquent ainsi que la Russie cherche maintenant à fédérer ses alliés africains autour de l'indépendance numérique face à l'Occident[47]. A contrario des déclarations de juillet 2023, la Russie promeut ainsi un écosystème numérique indépendant similaire au « Runet »[48], permettant un contrôle politique strict[49] et la défense de valeurs conserva-

44 Audinet, Maxime, et Kévin Limonier. « Le dispositif d'influence informationnelle de la Russie en Afrique subsaharienne francophone : un écosystème flexible et composite », Questions de communication, vol. 41, no. 1, 2022, pp. 129-148.

45 Olech, A. (2024). The Wagner Group in Africa. The sham battle of Russian mercenaries against terrorism. Terrorism – Studies, Analyses, Prevention, no. 5. La dislocation récente de Wagner a permis à Moscou de reprendre le contrôle de l'appareil de désinformation et d'influence du groupe en Afrique.

46 https://disinfo.africa/african-initiative-russias-new-mouthpiece-in-africa-65aa76fcc255

47 https://incyber.org/article/offensive-russe-sur-la-souverainete-numerique-en-afrique/

48 Runet désigne l'écosystème numérique souverain de la Russie, composé de sites web, services en ligne, et infrastructures technologiques contrôlés et régulés par le gouvernement russe. Créé pour protéger le pays contre les cybermenaces étrangères et assurer un contrôle strict des informations, le Runet comprend des alternatives locales aux plateformes occidentales, telles que le moteur de recherche Yandex et le réseau social VKontakte. Ce système permet à la Russie de surveiller et de filtrer le contenu en ligne, renforçant ainsi son contrôle politique. Le Runet illustre une approche de souveraineté numérique où un État aspire à réduire sa dépendance aux technologies étrangères tout en assurant une stricte surveillance de son espace cybernétique. Voir Kevin Limonier, « Vers un « Runet souverain » ? Perspectives et limites de la stratégie russe de contrôle de l'Internet », EchoGéo [56 | 2021. Cependant, notons que cette volonté de contrôle hégémonique ne va pas sans rencontrer des résistances nationales, à commencer par la Russie elle-même. Entre 2014 et 2016, le service « Yandex.News » a été au centre d'un conflit politique intense entre la société Yandex et le gouvernement russe. L'algorithme de Yandex, conçu pour sélectionner et publier des nouvelles en ligne, a été accusé par les autorités russes de partialité politique, particulièrement en relation avec la crise ukrainienne. En 2016, Roskomnadzor, l'organisme de surveillance des communications en Russie, a finalement pris le contrôle de l'algorithme de Yandex.News. Ce conflit a ultimement conduit à la scission entre Yandex NV, la société mère basée aux Pays-Bas, et ses activités en Russie. En 2024, un consortium d'investisseurs russes a conclu l'acquisition des activités russes de Yandex, marquant ainsi la plus grande transaction de retrait d'une entreprise occidentale de la Russie depuis le début de la guerre en Ukraine, voir « La scission de Yandex est presque achevée : les traders russes finalisent l'échange d'actions », 10 juillet 2024, Reuters (https://www.zonebourse.com/cours/action/YANDEX-N-V-8037501/actualite/La-scission-de-Yandex-est-presque-achevee-les-traders-russes-finalisent-l-echange-d-actions-47352959/). Ce cas emblématique a suscité un vif débat sur les algorithmes d'agrégation de contenu et leur nécessité d'être transparents et indépendants pour soutenir la démocratie, ainsi que l'indépendance des États qui utilisent de tels algorithmes. Les débats en Europe concernant Google ont été du même ordre mais on conduit au Digital service act. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0825. Le Digital Services Act (DSA) impose des obligations strictes aux plateformes numériques concernant la transparence des algorithmes, incluant la divulgation des critères utilisés pour le classement et la personnalisation des contenus, afin de protéger les droits des utilisateurs et renforcer la responsabilité des plateformes.

49 La législation russe de 2016 (loi Yarovaya) impose aux opérateurs de télécommunications de conserver les données des utilisateurs et de fournir ces informations aux services de sécurité. Elle illustre la volonté de l'État de contrôler les flux d'information en établissant par ailleurs une gouvernance hybride efficace via des prises d'intérêt de partenaires du pouvoir qui reste un décideur central (une fois les résistances dépassées, voir note 47). Les oligarques et autres élites économiques, en étant en effet intégrés dans cette structure de contrôle par l'actionnariat, ont un intérêt direct à maintenir le statu quo politique, consolidant ainsi le régime en place. Voir également le rapport de Alena Epifanova. Deciphering Russia's

trices. Combinés à un *storytelling* géopolitique anti impérialiste (contre l'occident global) et empruntant au répertoire panafricaniste, Moscou propose également des approches de censure numérique sophistiquées aux pays africains tout en implantant potentiellement des outils employés sur le territoire russe à cet effet[50]. Ainsi, la Russie et la Chine, malgré une convergence multisectorielle plus nuancée qu'il n'y paraît, accentuent en parallèle la fracture des droits numériques entre deux tendances. D'une part, une approche collégiale (c'est-à-dire multi-parties prenantes, ce qui ne signifie pas strictement consensuelle ou homogène[51]) de la réglementation juridique de l'Internet, adoptée par les pays d'Europe et d'Amérique, et d'autre part, une approche fondée sur la conception de souveraineté numérique, soutenue par la Russie, l'Iran, et la Chine, sur laquelle s'alignent certains pays des régions asiatiques et africaines. Cette dernière approche se manifeste dans sa version nationaliste la plus prononcée par une hyper-centralisation étatique, tout en alimentant une segmentation en termes de coopération globale, en premier lieu à l'échelle régionale[52]. Cette stratégie vise aussi à créer une convergence idéologique avec les régimes autoritaires et néo-conserva-

"Sovereign Internet Law": Tightening Control and Accelerating the Splinternet. DGAP Analysis No. 2, German Council on Foreign Relations (DGAP), 2020.

50 Roskomnadzor et le Service fédéral de sécurité russe (FSB) disposent ainsi de "portes dérobées" vers les plateformes Internet nationales, en vertu de la loi Yarovaya (note 48). Les TSPU (acronyme pour « appareils de lutte contre les menaces » en russe) se distinguent par leur efficacité. Ces boîtiers DPI optimisés (Deep Packet Inspection, dispositifs permettant d'examiner en détail le contenu des paquets de données transmis sur Internet), installés sur les nœuds des réseaux chez les fournisseurs d'accès, permettent de filtrer le trafic Internet, y compris les VPN (Virtual Private Networks, réseaux privés virtuels qui masquent l'adresse IP et cryptent les données de navigation). Bien qu'il existe des avantages légitimes et importants à l'utilisation de DPI pour les infrastructures publics d'un pays, tels que la capacité de détecter les menaces et attaques cachées dans le contenu des paquets de données, de prévenir les fuites de données et d'identifier où les données sont envoyées, le détournement de leur usage à des fins de contrôle et de censure politique devient de plus en plus saillant, y compris pour l'Afrique. Voir Christian Fuchs, "Societal and Ideological Impacts of Deep Packet Inspection Internet Surveillance," *Journal of Communication*, vol. 63, no. 6, 2013, pp. 1328-1359. What is Deep Packet Inspection (DPI)?, PagerDuty. (www.pagerduty.com/resources/learn/what-is-deep-packet-inspection/). Russia's digital authority pushes DPI tools and IP geolocation to surveil Internet traffic, Meduza, mai 2023. (*www.meduza.io/en/news/2023/05/24/russia-s-digital-authority-pushes-dpi-tools-and-ip-geolocation-to-surveil-internet-traffic*); A new anti-democratic tool: The Deep Packet Inspection technique, Democracy in Africa.org, 2023. (www.democracyinafrica.org/a-new-anti-democratic-tool-the-deep-packet-inspection-technique/). Voir également Rio, 2024, infra note 46.

51 Cette schématisation introductive doit en effet être nuancée, car malgré des valeurs communes, l'Europe et l'Amérique divergent sur plusieurs aspects de la gouvernance de l'Internet dans les faits. L'Europe, avec le RGPD, est stricte sur la protection des données, tandis que les États-Unis ont une approche plus fragmentée. En matière de neutralité du Net, l'UE maintient une position ferme, contrairement aux États-Unis, où les politiques ont fluctué, notamment avec l'abrogation des règles en 2017 par la FCC. L'Europe est également proactive dans la régulation des grandes plateformes numériques avec des lois comme le DSA (Digital Services Act) et le DMA (Digital Markets Act), alors que les États-Unis débattent encore des régulations appropriées. Enfin, l'Europe impose des restrictions plus strictes sur le discours de haine, contrairement aux États-Unis, qui protègent largement la liberté d'expression sous le premier Amendement. Pour les différences essentielles entre l'Europe et les États-Unis sur ces points, voir notamment Christopher T. Marsden, Net Neutrality: Towards a Co-regulatory Solution (Bloomsbury Publishing, 2017) ; Ari Ezra Walman, Privacy as Trust: Information Privacy for an Information Age (Cambridge University Press, 2018).

52 Selon l'organisation russe indépendante Roskomsvoboda, la divergence des approches et des compréhensions de la manière dont la réglementation de l'Internet et les droits de l'homme qui y sont exercés pourrait conduire à une crise d'une nature et ampleur inédite dans les années à venir (voir le rapport ici).

teurs d'Afrique, renforçant l'influence russe et chinoise par l'exploitation des défis internes à la fois sociétaux et techniques. Ainsi les divisions socio-politiques telles que celles alimentées par l'échec de la gouvernance portée par les classes dirigeantes et du modèle démocratique, ou encore l'instabilité sécuritaire autant que les retards technologiques et spécifiquement digitaux, sont présentés comme les conséquences d'une extraversion vers l'occident qui freinerait le développent technologique sur le continent. Alternativement la promotion de modèles de souveraineté numérique centralisés et très rapidement déployés contribue à alimenter à peu de frais le capital politique des régimes du moment, mais fragmente et ralentit les possibilités d'une coopération régionale plus dynamique et sécurisée.

L'Intelligence artificielle : limites actuelles et opportunités transformatives pour les états Ouest-africains

L'intelligence artificielle (IA) représente une opportunité transformative pour l'Afrique, offrant un potentiel considérable pour résoudre des défis persistants et accélérer le développement socio-économique. Les applications possibles sont vastes, allant de l'amélioration des systèmes de santé grâce au diagnostic médical assisté par l'IA à l'optimisation des rendements agricoles grâce à des prévisions précises basées sur des données[53]. Ainsi, l'intégration de l'IA peut jouer un rôle de facilitateur dans l'atteinte de 134 des objectifs de développement durable[54] (79 %), principalement grâce à des avancées technologiques qui pourraient contribuer à surmonter diverses limitations actuelles[55]. Cependant, la réalisation de ces avantages exige de relever plusieurs défis. L'un des principaux obstacles est la disparité dans l'accès aux données et aux ressources nécessaires à l'adoption efficace de l'IA. De nombreux pays africains souffrent en effet d'une fracture numérique qui entrave la collecte, la gestion et l'utilisation locale des données[56], limitant ainsi le potentiel de l'IA. Les infrastructures sont par ailleurs encore insuffisantes et le développement des algorithmes et applications adaptés aux besoins spécifiques du continent restent limités.

D'un autre côté, l'écart se creuse avec les cybercriminels qui utilisent de plus en plus l'IA afin, par exemple, d'analyser en temps réel l'efficacité de leurs attaques. Ils ajustent ainsi leurs stratégies pour maximiser les perturbations causées tout en minimisant les risques de détection, notamment à travers des attaques de type DDoS[57]. Ces at-

53 Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University. (2023). A voir également The State of AI in Africa Report 2023, https://cipit.strathmore.edu/wp-content/uploads/2023/05/The-State-of-AI-in-Africa-Report-2023-min.pdf.

54 Pour rappel les Objectifs de Développement Durable (ODD) sont un ensemble de 17 objectifs mondiaux adoptés par les États membres des Nations Unies en 2015 dans le cadre de l'Agenda 2030 pour le développement durable. Ils visent à éradiquer la pauvreté, protéger la planète et garantir la prospérité pour tous d'ici à 2030, en s'attaquant aux défis mondiaux tels que la pauvreté, les inégalités, le changement climatique, la dégradation de l'environnement, la paix et la justice. Ces objectifs sont déclinés en 169 cibles spécifiques et mesurés par 232 indicateurs. Voir https://www.un.org/sustainabledevelopment/fr/objectifs-de-developpement-durable/

55 Vinuesa, R., Azizpour, H., Leite, I., et al. (2020). The role of artificial intelligence in achieving the Sustainable Development Goals. Nature Communications, 11, 233

56 Voir section IV.1 sur l'enjeux des data center neutres.

57 Cybercriminalité et cyber espionnage se rejoignent par ailleurs dans l'usage de l'IA. Par exemple APT41, soutenu par l'État chinois et également connu sous le nom "Double Dragon" (reflétant des opérations de cyberespionnage et des cyberattaques motivées par le profit), utilise des techniques de spear phishing pour compromettre les réseaux cibles. Une fois infiltré, le groupe déploie des malwares

taques assistées par IA peuvent imiter un trafic normal, contournant ainsi les mécanismes de défense traditionnels Or l'IA peut précisément renforcer la cybersécurité en détectant proactivement les menaces *via* l'analyse prédictive et comportementale, et en répondant rapidement aux attaques grâce à l'automatisation. Elle améliore continuellement ses défenses en apprenant des nouvelles attaques, ce qui la rend particulièrement efficace contre les cybercriminels utilisant eux-mêmes l'IA.
Mais les politiques et les cadres réglementaires actuels ne sont souvent pas adaptés pour soutenir le développement et l'adoption de l'IA en Afrique. Il existe un besoin urgent de politiques qui encouragent l'innovation tout en protégeant les droits des utilisateurs et en atténuant les risques liés à l'éthique et à la confidentialité des données. Cela implique une collaboration étroite entre les gouvernements, les institutions de recherche, les entreprises, les start-ups et la société civile pour garantir que l'IA est développée et utilisée de manière responsable, en tenant compte des besoins et des enjeux nationaux et transnationaux. Les reculs démocratiques, entre autres, avec par exemple l'affaiblissement des sociétés civiles, ne favorisent pas de tels processus d'élaboration et d'appropriation collégiale[58]. L'exportation de technologies d'IA intrusives et clandestines vers des pays africains où les droits humains sont souvent bafoués risque à ce titre de renforcer les systèmes de répression existants et d'introduire de nouvelles formes de contrôle. Tandis que la désinformation et ses effets déstabilisateurs sur les États sont considérablement dopés par l'IA[59].

La Conférence sur l'état de l'IA en Afrique (COSAA) le 15 mars 2023 a souligné ces défis et appelé à une action coordonnée pour surmonter ces obstacles. La mise en œuvre de politiques et de réglementations efficaces, ainsi que l'investissement dans l'infrastructure de données et les compétences en IA, sont essentielles pour maximiser les avantages de l'IA tout en minimisant ses risques potentiels[60]. Notons cependant que l'enjeu des intelligences artificielles *open source*, pourtant un vecteur important de l'autonomisation numérique des états ouest-africains, reste proportionnellement peu abordé.

sophistiqués et des web shells (scripts malveillants installés sur un serveur web pour un accès à distance) pour maintenir l'accès et exfiltrer des données sensibles. L'IA est utilisée pour automatiser l'analyse de grandes quantités de données, identifier des anomalies, contourner les systèmes de sécurité et personnaliser les attaques de phishing. SentinelOne. "APT41 Infiltrates Multiple Sectors in a Worldwide Cyberattack." iZOOlogic, 2023; Agrawal, Jatin, Samarjeet Singh Kalra, et Himanshu Gidwani. "AI in Cyber Security." International Journal of Communication and Information Technology, 2023.Voir également ici les dernières actions d'APT41: https://izoologic.com/region/china/apt41-infiltrates-multiple-sectors-in-a-worldwide-cyberattack/. Voir également note 38.

58 Gyimah-Boadi, E. (2021, décembre). Le recul démocratique en Afrique de l'Ouest : Caractéristiques, causes et solutions. Fondation Kofi Annan, https://www.kofiannanfoundation.org/app/uploads/2022/02/Le-recul-democratique-en-afrique-de-louest_caracteristiques-causes-et-solutions_Boadi_Decembre2021.pdf Voir également le rapport sur les libertés numériques en Afrique Francophone, AFD, 2023, https://www.afd.fr/fr/ressources/libertes-numeriques-pays-francophones-afrique.
59 Pauwels, Eleonore. The Anatomy of Information Disorders in Africa: Geostrategic Positioning & Multipolar Competition Over Converging Technologies. Konrad-Adenauer-Stiftung, 2020
60 Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University. (2023). The State of AI in Africa Report 2023, https://cipit.strathmore.edu/wp-content/uploads/2023/05/The-State-of-AI-in-Africa-Report-2023-min.pdf.

III. Impacts et enjeux

1. Impacts économiques et sécuritaires

Les cyberattaques dans les pays ouest africains comme le Nigeria, le Ghana et le Sénégal ont eu des répercussions financières, opérationnelles et sécuritaires significatives. Au Nigeria, les pertes dues aux opérations frauduleuses dans le secteur bancaire ont atteint 193,5 milliards de nairas (544 millions de dollars) en 2021, augmentant à 273 milliards de nairas (762 millions de dollars) en 2022, et en 2023 à près de 300 milliards de nairas (833 millions de dollars)[61]. La fraude par SIM swap[62], utilisée pour détourner les comptes de mobile money, a coûté aux consommateurs de télécommunications plus de 20 milliards de nairas (55 millions de dollars) en 2022, selon un rapport de la Commission des communications du Nigeria (NCC). Ces pertes financières soulignent la vulnérabilité des plateformes de mobile money et la nécessité de mesures de sécurité renforcées. Les impacts opérationnels au Nigeria restent également préoccupants. Les attaques contre les infrastructures énergétiques ont perturbé les opérations des compagnies pétrolières et gazières, essentielles pour l'économie nationale[63]. De plus, les cyberattaques contre les infrastructures sensibles montrent que la cyber-menace peut être utilisée comme un outil de déstabilisation politique et sociale.

La croissance rapide de la pénétration d'Internet au Ghana, avec une augmentation de 2,31 millions à 24,06 millions d'utilisateurs entre 2012 et 2024, lorsque le taux de pénétration d'internet s'élevait à 69,8%[64], a permis de développer de nombreux services en ligne. Cependant, cette croissance expose également le pays à des cyberattaques qui menacent de saper la confiance dans ces services, retardant ainsi les progrès économiques. Ainsi, les pertes financières directes dues à la fraude cybernétique ont atteint 4,32 millions de dollars (49,5 millions GH₵) en 2023[65]. Les attaques DDoS ont perturbé les transactions financières sur les plateformes de paiement en ligne, compromettant la confiance des clients. Le Sénégal fait par exemple face à des conséquences graves des cyberattaques. Les attaques contre les institutions gouvernementales et les infrastructures critiques ont entraîné des fuites de documents sensibles et perturbé les opérations essentielles. Les attaques DDoS ont par ailleurs paralysé temporairement les services en ligne des sites web du gouvernement, démontrant la vulnérabilité des systèmes en place. Ces cyberattaques contre les ministères ont mis en péril la sécurité nationale et la diplomatie, soulignant l'urgence de renforcer les mesures de cybersécurité pour protéger les infrastructures et les utilisateurs[66].

61 Nigerian communications commission annual report 2023, (https://www.ncc.gov.ng/documents/885-annual-report-2022/file); Banks lose N18bn to fraudsters in 2023 -NIBSS, 29 avril 2024 (https://punchng.com/banks-lose-n18bn-to-fraudsters-in-2023-nibss/)
62 Ekeh, G.E., Afolabi, Y.I., Uche-Nwachi, E.O., Ekeh, L.K., & Eze-Udu, E. (2022). Awareness of BVN, SIM Swap and Clone Frauds: Methods and Controls. Science World Journal, 17(2). Department of Computer Science, Alex Ekwueme Federal University, Ndufu Alike-Ikwo, Ebonyi, Nigeria.
63 https://punchng.com/hackers-attack-39-nigerias-oil-sector-computers-report/;
64 Digital 2023: ghana; https://datareportal.com/reports/digital-2023-ghana; https://www.askyazi.com/useful-data-sources-for-africa/ghanas-digital-statistics-2023#:~:text=There%20were%2023.05%20million%20internet,percent%20of%20the%20total%20population.
65 Bank of Ghana Annual Report 2022](https://www.bog.gov.gh)
66 Osiris, Observatoire sur les Systèmes d'Information, les Réseaux et les Inforoutes au Sénégal. 2024. "La souveraineté numérique, une question de sécurité nationale." 26 février 2024. Accessible à : http://www.osiris.sn/La-souverainete-numerique-une.html.

2. Impacts sur le développement

Au Nigeria, l'initiative d'inclusion financière de la Central Bank of Nigeria, lancée en 2012, visait à intégrer 80 % de la population adulte dans le système financier formel d'ici 2020[67]. Cependant, les fraudes par carte bancaire et les piratages de comptes en ligne ont rapidement sapé la confiance du public dans les services bancaires numériques, entraînant des pertes de 3 milliards de nairas (8,3 millions USD) en 2018[68]. Au Sénégal, le projet de modernisation des systèmes de santé, soutenu par la Banque mondiale a été gravement perturbé par des attaques de ransomware en 2016. Ces attaques ont paralysé les systèmes informatiques des hôpitaux, entraînant des pertes financières et interrompant les services de santé. Enfin, au Ghana, le projet de développement agricole visant à améliorer la productivité des petits exploitants agricoles a été compromis par des cyberattaques en 2018. Les cybercriminels ont ciblé les plateformes de paiement mobile, volant des fonds et érodant la confiance des agriculteurs dans les technologies numériques. Ces incidents montrent que la cybercriminalité entraîne des pertes financières directes, une diminution de la confiance du public et des retards dans la mise en œuvre des projets, compromettant ainsi les objectifs de développement.

3. Impacts sur la stabilité sociale et politique

Les cyber-crimes en Afrique de l'Ouest, particulièrement au Nigeria, au Sénégal et au Ghana, ont des impacts dévastateurs sur la stabilité sociale et politique. Au Nigeria, si la cybercriminalité a entraîné une perte de revenus pour les entreprises, elle a concrètement augmenté le chômage et exacerbé les tensions sociales. L'exode des investisseurs, comme après l'attaque de 2017 contre une grande banque nigériane, a ralenti la croissance économique et compromis les projets de développement, suscitant des protestations contre le gouvernement[69]. Au Sénégal, les cyberattaques telles que l'attaque DDoS du 26 mai 2023 contre des sites gouvernementaux, ont perturbé l'économie locale et ont eu des impacts sensibles sur la confiance des investisseurs[70]. De même au Ghana, lors des élections de 2016, des cyberattaques contre la Commission électorale[71] ont semé des doutes sur l'intégrité du processus électoral, participant à générer des violences post-électorales. Évènements non isolés qui alarment de plus en plus les experts[72]. Au-delà des pertes économiques immédiates, les cyber-crimes menacent la confiance des citoyens dans leurs institutions, sapent les efforts de développement et peuvent déstabiliser des sociétés déjà fragiles.

67 National financial inclusion strategy, 2012, https://www.afi-global.org/wp-content/uploads/publications/mfg-en-paper-national-financial-inclusion-strategy-oct-2012.pdf
68 National financial inclusion strategy revised, 2018, https://www.cbn.gov.ng/out/2019/ccd/national%20financial%20inclusion%20strategy.pdf
69 https://www.vanguardngr.com/2017/07/hackers-target-nigerian-banks/;https://www.premiumtimesng.com/news/top-news/228166-north-korean-hackers-attack-banks-in-nigeria-17-other-countries-kaspersky.html?tztc=1
70 https://incyber.org/en/article/a-cyberattack-hits-government-sites-in-senegal/
71 BBC News. 2016. "Ghana Election Commission Website Hit by Cyber Attack." 8 December 2016. https://www.bbc.co.uk/news/world-africa-38247987.
72 Sarah O'Connor, Fergus Hanson, Emilia Currey, Tracy Beattie. Cyber-enabled Foreign Interference in Elections and Referendums. ASPI, Policy Brief Report No. 41/2020.

IV. Réponses et défis de la souveraineté numérique en Afrique de l'Ouest

1. Initiatives dans la consolidation de la souveraineté numérique

Les efforts des pays africains tels que le Sénégal, le Ghana et le Nigeria pour renforcer leur souveraineté numérique reflètent une prise de conscience croissante de l'importance de contrôler et protéger les infrastructures et les données dans un environnement numérique en constante évolution. Ces initiatives comprennent la création de centres de données sécurisés, le développement de cadres réglementaires et l'adhésion à des conventions internationales telles que la Convention de Malabo sur la cybersécurité et la protection des données personnelles[73].

Le Sénégal a mis en place un datacenter à Diamniadio, soutenu par l'Agence De l'Informatique de l'État (ADIE)[74], tandis que le Ghana a créé la Ghana Cyber Security Authority (CSA) et investi dans l'amélioration de ses infrastructures de télécommunications pour garantir une connectivité résiliente. De même, le Nigeria a pris des mesures significatives avec la Commission des Communications du Nigeria (NCC) et la National Information Technology Development Agency (NITDA), axées sur la régulation du secteur des télécommunications et la promotion de la sécurité des réseaux en 2022. Une composante essentielle de ces efforts semble aussi se situer dans la montée en puissance des datacenters "neutres"[75]. Ces approches permettent de contrôler et de protéger les données locales, de stimuler l'innovation technologique locale et de garantir une plus grande autonomie stratégique dans le domaine numérique. Entre 5 et 6 milliards de dollars devraient être ainsi investis en Afrique dans de tels datacenters au cours des 3 à 5 prochaines années (portés par des compagnies telles qu'Equinix, Vantage et Digital Realty). Parallèlement, un nombre croissant de gouvernements africains adoptent des politiques, des lois et des réglementations sur la localisation des données et la protection de la vie privée. Des pays comme le Nigeria[76], le Ghana[77], l'Afrique du Sud[78] et le Kenya[79] ont mis en place des lois sur la protection des données

73 Union Africaine. (2014). Convention de l'Union Africaine sur la Cyber Sécurité et la Protection des Données à Caractère Personnel. Récupéré de https://www.afapdp.org/wp-content/uploads/2018/06/CONV-UA-CYBER-PDP-2014.pdf.

74 ADIE (Agence de l'Informatique de l'État). (s.d.). Datacenter de Diamniadio, lieu d'impulsion de la transformation digitale du Sénégal. Récupéré de https://www.adie.sn/actualites/le-datacenter-de-diamniadio-lieu-d%E2%80%99impulsion-de-la-transformation-digitale-du-s%C3%A9n%C3%A9gal.

75 Un datacenter « neutre » est une installation indépendante de tout fournisseur de télécommunications ou de cloud particulier. Il offre aux clients la liberté de choisir leurs opérateurs et fournisseurs de services, garantissant ainsi une grande flexibilité et interconnectivité. Ces centres de données hébergent des infrastructures critiques de manière indépendante, ce qui renforce la sécurité et la résilience des systèmes numériques, tout en garantissant que les données sont localisées dans le pays des usagers. Cela contribue à l'innovation technologique locale et à la souveraineté numérique des pays.

76 National Information Technology Development Agency (NITDA). (2019). Nigeria Data Protection Regulation (NDPR). Abuja : NITDA, https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf ainsi que le cadre d'application deux ans plus tard https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf

77 Government of Ghana. (2012). Data Protection Act, 2012 (Act 843). Accra: Government of Ghana, https://www.dataprotection.org.gh/data-protection/data-protection-acts-2012#:~:text=OVERVIEW%20OF%20DATA%20PROTECTION%20ACT%2C%202012%20(ACT%20843)&text=It%20recognises%20a%20person's%20right,accordance%20with%20the%20individual's%20rights.

78 South African Government. (2013). Protection of Personal Information Act (POPIA), 2013. Pretoria: South African Government, https://www.justice.gov.za/legislation/acts/2013-004.pdf

79 Kenya Law. (2019). Data Protection Act, 2019. Nairobi: Kenya Law, http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

et de la vie privée, tandis que d'autres envisagent des mesures similaires pour renforcer leur cadre juridique en matière de cybersécurité[80]. L'adhésion à la Convention de Malabo sur la cybersécurité et la protection des données personnelles est un exemple de l'engagement des États africains à élaborer des lois nationales conformes aux normes et principes énoncés dans le texte. Cependant, avec seulement 15 pays sur 55 ayant ratifié cette convention, des questions subsistent quant aux raisons derrière cette situation, soulignant la nécessité de promouvoir la sensibilisation et l'engagement en matière de cybersécurité en Afrique. Enfin, la feuille de route stratégique et le plan d'action du Nigeria pour la protection des données, lancés par la Nigeria Data Protection Commission (NDPC) en décembre 2023[81], témoignent des efforts déployés pour renforcer la sécurité des données et accroître la confiance des utilisateurs dans l'environnement numérique.

2. Défis et Perspectives

Les défis rencontrés dans la quête de souveraineté numérique en Afrique de l'Ouest sont nombreux et complexes. Tout d'abord, la dépendance technologique vis-à-vis des partenariats avec des entreprises étrangères soulève des inquiétudes quant à la sécurité et à l'autonomie des infrastructures numériques. Ces partenariats peuvent entraîner une vulnérabilité accrue aux pratiques commerciales et politiques des entreprises étrangères, mettant ainsi en péril la confidentialité des données et la protection des intérêts nationaux.

La prédominance des géants technologiques mondiaux tels que les GAFAM et les géants du web chinois aggrave cette dépendance et menace la souveraineté numérique africaine. Ces entreprises contrôlent souvent les plateformes et les services numériques les plus utilisés sur le continent, ce qui les place dans une position de pouvoir significative pour influencer les politiques et les réglementations dans le domaine numérique[82].

80 Voir a ce titre les rapports successifs de 2019 a 2021 de United Nations Conference on Trade and Development (UNCTAD).Value Creation and Capture – Implications for Developing Countries. Geneva: UNCTAD.https://unctad.org/topic/ecommerce-and-digital-economy/digital-economy-report.
L'accélération des mesures juridiques de protection des données sur une plage de temps de quelques années pour certains pays aurait été dopé par la crise du covid 19 durant laquelle les alternatives numériques ont été d'un appui central dans le maintien minimal des activités économiques.

81 National Data Protection Commission. (2023). Strategic Roadmap and Action Plan (SRAP), https://ndpc.gov.ng/Srap.pdf.

82 Les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) dominent les marchés numériques africains, limitant la croissance des entreprises locales et posant des défis en matière de souveraineté des données et de protection de la vie privée, tout en influençant les dynamiques socioculturelles locales. Leur relation interdépendante avec les gouvernements, qui les soutiennent géopolitiquement et économiquement, complique les efforts de régulation stricte et de démantèlement, car ces entreprises sont profondément intégrées dans les économies nationales et internationales ([IRIS - Les GAFAM et l'État : quelles évolutions du champ du pouvoir, https://www.iris-france.org/167483-les-gafam-et-letat-quelles-evolutions-du-champ-du-pouvoir/). Malgré des moyens institutionnels et financiers conséquents, les régulations européennes peinent à circonscrire cette domination. Joëlle Toledano souligne la fragmentation des régulateurs européens et l'insuffisance des ressources de contrôle, qui permettent ainsi aux GAFAM de contourner les nouvelles régulations (DMA et DSA). Elle propose de regrouper les missions de régulation en trois pôles européens pour une meilleure coordination ([Le Monde - Sans régulation efficace, la politique de souveraineté numérique européenne échouera selon l'auteur (https://www.lemonde.fr/idees/article/2023/09/01/sans-regulation-efficace-la-politique-de-souverainete-numerique-europeenne-echouera_6187365_3232.html). Les leçons tirées de l'Europe sont instructives pour l'Afrique, qui doit développer des régulations claires et coordonnées pour gérer l'influence des GAFAM et protéger sa

Un autre défi majeur est le manque de ressources humaines qualifiées en cyber sécurité et en gestion des infrastructures numériques. La pénurie de personnel formé dans ces domaines rend difficile la protection efficace des réseaux et des données contre les menaces croissantes telles que les cyberattaques et les violations de la vie privée. Il est impératif d'investir dans des programmes d'éducation et de formation spécialisés pour développer une main-d'œuvre compétente capable de relever ces défis.

La cybercriminalité représente le défi croissant le plus urgent en Afrique de l'Ouest, en particulier au Nigeria. Les attaques informatiques, telles que les ransomwares, les fraudes en ligne et le vol de données, sont devenues fréquentes et peuvent causer des dommages importants aux individus, aux entreprises et aux gouvernements. La lutte contre ces menaces nécessite une coordination efficace entre les acteurs nationaux et internationaux, ainsi que des mesures de sécurité robustes et des stratégies de prévention efficaces.

Le financement des projets numériques ambitieux constitue de manière générale un obstacle majeur. Les initiatives visant à renforcer la souveraineté numérique nécessitent des investissements considérables en infrastructures, en technologies et en capacités humaines. Cependant, l'accès à des sources de financement adéquates reste limité, ce qui entrave la mise en œuvre de projets stratégiques dans ce domaine. Pourtant les mesures de facilitation numérique de l'investissement ont un impact économique significatif sur l'environnement des affaires et afin d'attirer les IDE dans un contexte de fragilisation marqué[83]. L'OCDE suggère que réduire la complexité administrative des pays en développement au niveau médian pourrait augmenter le stock d'IDE de 20 %[84]. Grâce à leur coût relativement faible, ces mesures numériques bénéficient particulièrement aux petites économies et à celles ayant peu de ressources pour attirer les investissements. Elles améliorent la gouvernance et les institutions, surtout dans les pays ayant des faiblesses dans ces domaines, et favorisent la diversification économique en soutenant davantage les IDE dans les secteurs manufacturiers et de services. Les PME, souvent entravées par les obstacles administratifs, profitent de manière considérable de la facilitation numérique de l'investissement, ce qui rend le processus plus accessible et attractif [85]. De même les engagements concrets, par

souveraineté numérique. Investir dans les capacités locales et s'assurer que les régulations sont précises et contraignantes est crucial pour éviter que les entreprises technologiques globales ne contournent les obligations imposées. Au Sénégal, l'approche récente vise, pour commencer, à appliquer une contrainte fiscale rigoureuse. Depuis le 1er juillet 2024, les GAFAM et autres prestataires étrangers doivent collecter et reverser la TVA sur les services numériques fournis au Sénégal, ce qui marque une avancée vers la régulation des transactions numériques malgré des préoccupations quant à la conformité des fournisseurs étrangers ([Digital Business Africa - Les GAFAM vont collecter et reverser au fisc sénégalais la TVA sur les activités numériques dès le 1er juillet 2024, https://www.digitalbusiness.africa/les-gafam-et-cie-vont-collecter-et-reverser-au-fisc-senegalais-la-tva-sur-les-activites-numeriques-des-le-1er-juillet-2024/). Cependant, il y a des craintes que ces entreprises répercutent les coûts sur les consommateurs ou réduisent leurs investissements dans la région. Des régulations trop strictes pourraient décourager les investissements étrangers et freiner l'innovation locale qui s'épanouit dans un équilibre entre la collecte de revenus fiscaux et la promotion d'un environnement favorable à la croissance économique et technologique ([Social Net Link - Taxer les GAFAM, un pari risqué pour les pays africains] (https://www.socialnetlink.org/2024/07/03/taxer-les-gafam-un-pari-risque-pour-les-pays-africains/)).

83 Comme indiqué précédemment (voir note 10)

84 Coopération pour le développement 2023 : quel système d'aide pour demain ?, OCDE, 2023, https://www.oecd.org/fr/publications/cooperation-pour-le-developpement-2023_83b806cb-fr.html

85 Iyaji Danjuma, "Insurgency, Political Risk, and Foreign Direct Investment Inflows in Nigeria: A Sectorial Analysis," CBN Journal of Applied Statistics, vol. 12, no. 2 (December 2021), Adewale Samuel Hassan, "Does

exemple à l'égard de l'Ati (Addis Tax Initiative), ont montré une accélération des processus de numérisation des services publics comme par exemple la mise en place au Ghana d'une plateforme en ligne pour la publication des informations fiscales et des rapports financiers des administrations publiques ou encore pour le paiement en ligne[86]. Cette initiative a amélioré la perception de transparence et a permis aux citoyens de suivre l'utilisation des fonds publics[87].

Mais la digitalisation des services publics, stratégie essentielle, ne répond pas en elle-même à tous les défis.

Les pays Ouest africains doivent davantage combiner les approches afin de préserver leur intégrité numérique, acquérir rapidement les compétences techniques essentielles, gérer régionalement les variations financières telles que les attentes de plus en plus réactives des IDE, tout en promouvant des partenariats équilibrés et mutuellement bénéfiques avec des acteurs internationaux. Quelques soient les combinaisons envisagées pour atteindre ces objectifs, elles semblent devoir intégrer quelques éléments stratégiques primordiaux. Il est possible d'en isoler trois. **Le premier s'intègre dans une logique d'autonomisation par la diversification financière**. Il s'agit de renforcer une approche en termes de leviers de financements alternatifs et de diversification continue, y compris au niveau local (national ou régional), Cela permet de favoriser des dynamiques plus résilientes au regard des impacts économiques de la globalisation des crises et des entrismes politico-commerciaux très offensifs qui profitent de vulnérabilités circonstancielles ou structurelles. **La seconde composante stratégique se résume par une collaboration accrue, notamment au niveau régional et par un partage des ressources.** Le principe est de maximiser les ressources disponibles et de promouvoir l'efficacité en favorisant par exemple une coopération renforcée entre les secteurs public et privé, ainsi qu'une mutualisation des infrastructures régionales. Ce qui accroit en retour la diversification financière. **Enfin, la troisième est de centrer les efforts sur l'innovation technologique et l'accroissement des compétences locales.** Cette approche vise à renforcer l'autonomie technologique grâce à l'*open source*, au transfert de technologie, et à la promotion des compétences locales, en particulier sur les enjeux de cyber sécurité. Quelques propositions peuvent aller dans ce sens.

Autonomie par la diversification financière

La diversification financière est essentielle pour autonomiser les investissements en Afrique de l'Ouest. Que ce soit à travers l'aide publique au développement ou des investissements directs étrangers (IDE), tous deux sous pression, la tendance semble se projeter sur des projets offrant des rendements à la fois économiques et sociaux. Par

Country Risk Influence Foreign Direct Investment Inflows? Evidence from Nigeria and South Africa," Journal of Contemporary Management, vol. 20, no. 1, 2023, https://www.bloomberg.com/news/articles/2024-02-17/nigeria-s-capital-inflows-fell-26-in-2023-amid-economic-turmoil.

86 https://gra.gov.gh/file-and-pay-taxes/e-commerce/

87 Cependant, ce point met en lumière deux dimensions importantes : d'une part, les défis liés à l'équilibrage et à la séquentialisation fiscale, le Ghana cherchant à exploiter les opportunités offertes par le numérique et les Fintech pour élargir sa base fiscale en taxant les services numériques tout en risquant de dissuader les utilisateurs potentiels. D'autre part, une perception positive des processus de numérisation ne se traduit pas nécessairement par un engagement effectif du public à leur égard. Ofosu-Ampong K souligne ainsi l'importance cruciale d'une structuration adéquate des composantes fiscales ainsi que de la facilitation de l'utilisation du système mis en place (Ofosu-Ampong, K. (2024). New policies, new behaviors: How digital taxation shapes mobile money use in Ghana. Engineering Reports, https://onlinelibrary.wiley.com/doi/epdf/10.1002/eng2.12860).

exemple, l'inclusion financière des fintechs, a su attirer des capitaux-risques et des fonds de capital-investissement, réduisant leur dépendance aux IDE traditionnels[88]. Cette stratégie de diversification continue et plus intensive, à l'échelle locale ou régionale, viserait à créer des dynamiques économiques résilientes face aux crises globales et aux entrismes politico-commerciaux offensifs exploitant les vulnérabilités locales. La création de fonds souverains numériques pourrait également jouer un rôle crucial, alimentés par les revenus des ressources naturelles ou d'autres actifs publics, et destinés à financer des infrastructures numériques, des startups technologiques et des projets de recherche en innovation numérique. Par exemple, les recettes minières pourraient être au moins partiellement réinvesties dans des initiatives numériques, garantissant ainsi une utilisation stratégique des ressources nationales pour le développement technologique[89]. L'adoption de crypto-monnaies et d'actifs numériques comme la eCFA au Sénégal pourrait offrir des alternatives aux systèmes financiers traditionnels, facilitant ainsi l'accès aux capitaux pour les startups et les petites entreprises. De plus, la blockchain peut être utilisée pour créer des systèmes d'épargne et de crédit collaboratifs, renforçant l'inclusion financière et stimulant l'entrepreneuriat local. Les crypto-monnaies peuvent également servir de réserve de valeur pour les fonds souverains, diversifiant ainsi les actifs et réduisant la dépendance aux monnaies étrangères[90]. Le développement de plateformes de financement participatif (crowdfunding) pourrait aussi offrir une solution d'appoint pour lever des fonds à travers des contributions populaires, soutenant ainsi des projets innovants et à fort impact social. En parallèle, la création de fonds de capital-risque locaux, axés sur les startups technologiques africaines, permettrait de canaliser des investissements vers des projets prometteurs. Ces initiatives peuvent également attirer des investisseurs étrangers à la recherche d'opportunités de croissance sur le continent. Mais l'accompagnement à la gestion des capitaux pour les startups est essentiel, notamment en matière de gouvernance entrepreneuriale, pour éviter certains échecs observés au Nigeria et au Ghana.

88 Par exemple voir Jaoui, F., O. Amoussou, and H.F. Kemeze (2022), Catch Me if You Can': On Drivers of Venture Capital Investment in Africa, Working Paper Series N° 364, African Development Bank, Abidjan, Côte d'Ivoire, https://www.afdb.org/sites/default/files/documents/publications/wps_no364_catch_me_if_you_can_on_drivers_of_venture_capital_investment_in_africa_repaired.pdf).

89 Pour convaincre les gouvernements et les classes politiques, il est crucial de démontrer les bénéfices économiques à court terme et la solidité de la redistribution des dividendes dans les secteurs des TIC. Cela peut être accompli en mettant en avant les gains en efficacité et en transparence des services publics, en fournissant des données probantes et des études de cas, et en soulignant les impacts sociaux positifs. En outre, proposer des politiques et des stratégies concrètes pour soutenir le développement des TIC peut renforcer la crédibilité et l'attrait des investissements dans ce secteur. Le Rwanda pourrait être à ce titre une illustration pertinente. Le pays a mis en œuvre une stratégie nationale de développement des TIC (Vision 2020) et a réussi à attirer des investissements étrangers significatifs dans le secteur des TIC, à créer des emplois et à stimuler l'innovation locale. Kigali est devenu un hub technologique régional, accueillant des événements technologiques majeurs et des incubateurs de startups. Sur le plan des dividendes structurels, hormis l'amélioration de l'administration publique grâce à la digitalisation des services gouvernementaux (ce qui a conduit à une plus grande transparence et efficacité), l'augmentation de l'assiette fiscale est notable grâce à la croissance économique stimulée par les TIC. Voir par exemple IFC report shows digitalization holds immense promise, economic potential for african businesses of all sizes, may 2024 https://pressroom.ifc.org/all/pages/PressDetail.aspx?ID=28167). il s'agit d'une synthèse du rapport complet accessible sur le portail de l'IFC : https://openknowledge.worldbank.org/server/api/core/bitstreams/e6f2cc1b-ad12-460f-9f17-ff95b69cb378/content.

90 Entretien avec un expert de crypto-économie basé en Afrique, 18/07/24.

La résilience par la collaboration accrue et le partage des ressources

La collaboration régionale et le partage des ressources maximiseraient le déploiement, l'efficacité et l'utilisation des infrastructures. Les partenariats public-privé (PPP), comme ce qui pourrait s'appeler les Groupements d'Investissement Numérique (GIN), permettraient de mutualiser les capitaux privés et publics pour financer des centres de données et des infrastructures de télécommunication. Les GIN, inspirés ici des Groupements Fonciers Agricoles (GFA), seraient des organisations civiles où chaque part serait proportionnelle au capital apporté, garantissant une distribution équitable des revenus. L'État jouerait un rôle limité mais stratégique, garantissant la gestion souveraine des données. Cette approche encouragerait théoriquement des investissements intermédiaires, diversifiant les sources de financement et réduisant les risques tout en favorisant une coopération entre les secteurs public et privé et la mutualisation à terme des infrastructures régionales[91]. La coopération régionale, en s'appuyant sur ces dynamiques nationales PPP pourrait en effet jouer un rôle clé dans la création d'un environnement favorable aux investissements. Comme évoqué plus haut, en accélérant la réduction de la complexité administrative par la digitalisation et en harmonisant les régulations à l'échelle régionale, les pays d'Afrique de l'Ouest pourraient attirer davantage d'IDE et faciliter l'accès aux capitaux. Au-delà, la création de zones économiques spéciales (ZES)[92] dédiées aux technologies numériques pourrait également stimuler les investissements en offrant par ailleurs des avantages fiscaux. Enfin, la mutualisation des infrastructures, comme les centres de données et les réseaux de télécommunications, à travers des initiatives régionales pourrait réduire les coûts et améliorer l'accès aux technologies de pointe. L'approche de réseaux maillés (meshing[93])

91 Il existe au prime abord des approches similaires, plus globalisantes et ambitieuses, telles que l'Alliance Smart Africa en faveur des TIC, soutenue par l'Agenda 2063 de l'Union Africaine (https://au.int/en/agenda2063/overview). Ces initiatives incontournables rencontrent toutefois des contraintes dans la mobilisation des ressources financières, en raison entre autre d'un manque de stratégie de diversification plus dynamique. Cela maintient une dépendance marquée aux financements internationaux, eux-mêmes en cours de fragilisation.

92 Une zone économique spéciale (ZES) est une région délimitée au sein d'un pays où les règles économiques, fiscales et commerciales sont distinctes de celles appliquées sur le reste du territoire. Ces zones sont conçues pour attirer les investissements étrangers, dynamiser le développement économique et favoriser des secteurs industriels spécifiques. Elles offrent divers avantages, tels que des exonérations fiscales, une réglementation plus souple, un accès facilité aux infrastructures, et parfois un cadre juridique particulier. L'objectif principal des ZES est de stimuler la croissance économique, de créer des emplois et de promouvoir le développement technologique dans des zones stratégiques. D'après la CNUCED, leurs performances en Afrique sont souvent inférieures aux objectifs fixés pour des raisons institutionnelles et des dynamiques nuisibles de concurrence ou encore des cadres stratégiques faibles. Toutefois, la mise en place de ZES très sectorisées (dédiées en l'occurrence au digital) et bien définies stratégiquement, territorialisées au niveau national, transfrontalières ou le cas échéant « de-spatialisées » (ce qui stimulerait une harmonisation des réglementations des différentes parties prenantes nationales sur le numérique) pourrait représenter un modèle plus opérationnel. En particulier en prenant appui à cet effet sur la Zone de libre-échange continentale africaine (ZLECAf). Voir Conférence des Nations Unies sur le commerce et le développement (CNUCED). Guide sur les zones économiques spéciales en Afrique : vers une diversification économique à travers le continent. UNCTAD/DIAE/IA/2021/3, 2021. De plus face aux modèles chinois de zones économiques de coopération implémentées en Afrique et qui posent de sérieux problèmes politiques et économiques dans la durée, des ZES bien pensées en faveur numérique pourrait à l'inverse représenter une alternative. Voir à ce titre les avertissements déjà datés mais toujours pertinents en 2024 de Bräutigam D, Xiaoyang T. African Shenzhen: China's special economic zones in Africa. The Journal of Modern African Studies. 2011;49(1):27-54.

93 Le meshing, ou réseau maillé, est une approche innovante pour construire des infrastructures de communication décentralisées et résilientes. En Afrique de l'Ouest, cette méthode offre une solution viable et économique pour améliorer la connectivité et renforcer la souveraineté numérique. Elle permet

permettrait par exemple de créer des réseaux décentralisés et résilients, améliorant la sécurité et la stabilité des infrastructures numériques. Par exemple, une collaboration entre le Sénégal, la Côte d'Ivoire et le Ghana pourrait mutualiser les infrastructures de télécommunications pour améliorer la couverture et réduire les coûts. Des incubateurs techniques pourraient également se greffer à ces structures régionales pour favoriser le renforcement des compétences des différents pays. Pour les data center neutres, une approche régionale permettrait de créer des centres de données partagés entre plusieurs pays, garantissant une indépendance technologique et une sécurité des données renforcée tout en réduisant les coûts d'infrastructure grâce à la mutualisation des ressources[94].

Innovation technologique, transfert technique et renforcement des compétences locales

Centrer les efforts sur l'innovation technologique et le renforcement des compétences locales, particulièrement en termes de cyber-sécurité, est crucial pour l'autonomie technologique. La promotion de l'*open source* et le transfert de technologies sont à ce titre des éléments clés pour consolider l'atteinte des objectifs de souveraineté numérique. Par exemple, des programmes de formation en développement de logiciels *open source*, des hackathons[95] et des incubateurs de startups technologiques encou-

une couverture étendue, une résilience accrue grâce à la redondance et à l'auto-réparation, et des économies de coûts via l'infrastructure partagée. Pour une présentation didactique du principe de meshing voir https://www.intechopen.com/chapters/66938. Pour des exemples de meshing locaux en Afrique voir par exemple ces projets :
https://tunapanda.org/ ou https://www.internetsociety.org/issues/community-networks/success-stories/ (Ouganda, Maroc, Afrique du sud). Ces projets sont à des échelles très restreintes mais particulièrement efficace. S'il est possible de les mettre à l'échelle, ils sont à développer sur les zones périphériques et frontalières des états où la connectivité est encore liminaire ou inexistante. Voir également les références suivantes Sanchez, Alain, Joe Robertson, and Courtney Radke. "Cybersecurity Roundtable: Fortinet CISOs Discuss Mesh Architectures." FORTINET, February 22, 2022. https://www.fortinet.com/blog/industry-trends/cybersecurity-mesh-architectures-fortinet-cisos-discuss-the-importance/; Internet access in Africa - Are mesh networks the future?" BBC News, https://www.bbc.com/news/av/world-africa-47723967

94 Au regard des sensibilités nationales actuelles sur les questions de souveraineté, il convient de préciser le schéma de fonctionnement possible de ces dispositifs mutualisés au niveau régional. Tout d'abord le chiffrement des données, à la fois en transit et au repos, protège les informations sensibles. Le partitionnement et l'isolation logique assurent une séparation des données de chaque pays, même si elles sont physiquement situées au même endroit. L'accès restreint et contrôlé est essentiel, utilisant des politiques basées sur des rôles et une authentification multi-facteurs pour limiter les accès non autorisés. A ce titre des initiatives européennes telles que Gaia -X peuvent inspirer des dispositifs de gouvernance partagée. Des accords de niveau de service stricts définiraient les responsabilités de chaque partie en matière de sécurité. Une surveillance constante et des audits réguliers permettraient en outre de détecter et de répondre rapidement aux (tentatives de) violations éventuelles de sécurité. L'utilisation de technologies de sécurité avancées, telles que les pare-feu, les systèmes de détection et de prévention des intrusions (IDPS) et les solutions de gestion des informations et des événements de sécurité (SIEM), renforcerait ainsi la protection. Le respect des normes internationales, comme celles du RGPD (voir plus haut), assurait la conformité légale. Enfin, des plans de continuité et de récupération garantiraient la disponibilité des données en cas d'incident. Pour des détails sur le projet Gaia X voir GAIA-X : le projet européen entre dans une nouvelle phase (https://www.entreprises.gouv.fr/files/files/01-nouveau-portail/secteurs-d-activite/Numerique/bmwi_gaia-x_papier_umbrella-master_frz-web.pdf) et Gaia-X : un projet européen trop ambitieux ? (https://afee-cedece.eu/gaia-x-un-projet-europeen-trop-ambitieux/).

95 Un hackathon est un événement intensif où des participants collaborent pour créer des solutions innovantes sur un sujet spécifique, souvent en 24 à 48 heures. Ils développent des prototypes fonctionnels ou des concepts en utilisant leurs compétences variées, comme la programmation, le design ou

rageraient l'innovation locale. Plus spécifiquement des initiatives telles que des formations techniques spécialisées, des ateliers de codage et des programmes de certification en développement de logiciels *open source* pourraient être mis en place pour former une nouvelle génération de développeurs et techniciens locaux. Des incubateurs de startups technologiques et des hackathons pourraient également être organisés pour stimuler l'innovation locale et identifier des solutions adaptées aux défis spécifiques de la région et de chaque pays partenaire du dispositif de mutualisation. Enfin, il s'agirait de renforcer les transferts technologiques et de compétences comme priorité des partenariats étrangers (favorisant de surcroit la réalisation des précédentes propositions). Il serait à ce titre aussi urgent qu'essentiel d'intégrer des clauses de transfert technologique dans tous les accords internationaux. Ces clauses devraient inclure des obligations pour les partenaires étrangers de partager des technologies, de former les travailleurs locaux et de soutenir les institutions éducatives centrées idéalement sur ces technologies. Les stratégies incluent la création de programmes de formation et de certification en partenariat avec des institutions locales et internationales, la promotion de la recherche et du développement collaboratif, et la mise en place de mécanismes de suivi et d'évaluation pour garantir le respect des engagements. Ces initiatives permettraient de former des spécialistes dans des domaines clés et de développer des technologies adaptées aux besoins locaux, tout en évitant les mécanismes de dépendance technologique qui pourraient limiter le développement autonome et durable de la région.

Conclusion

Les bouleversements géopolitiques, tels que l'essor de la multipolarité et les tensions entre grandes puissances de plus en plus incarnées au niveau continental, accentuent la nécessité pour les États ouest-africains de trouver un équilibre entre indépendance numérique et interconnectivité mondiale. Et ceci, au risque de subir une stagnation ou une récession numérique et d'exposer durablement leur intégrité nationale aux stratégies de pénétration techno-politiques et économiques d'origine étrangères.

Plutôt que de se diriger vers une souveraineté numérique fermée, qui risquerait d'isoler les nations et de freiner les progrès technologiques à moyen et long terme, il est crucial de favoriser une autonomie stratégique, adaptative et résiliente pour répondre à ces défis et qui s'inscrive simultanément dans une logique de mutualisation. Cela passe par le développement de processus régionaux de coopération et d'intégration technologique, adaptés aux contextes nationaux variés, et par ailleurs informés par des monitorings continus sur le plan technique, politique, économique et sociologique. Plus particulièrement, en développant des réseaux de collaboration régionaux robustes, les États ouest-africains peuvent par ailleurs protéger leurs infrastructures numériques contre les cybermenaces croissantes et favoriser ainsi un développement technologique harmonisé et durable. La promotion de l'*open source*, la mutualisation des infrastructures régionales, la renégociation informée des conditions de transfert technologique durable ainsi que l'innovation technologique et financière, soutenues par une éducation numérique renforcée, sont à ce titre des axes importants pour une souveraineté numérique inclusive et dynamique. Davantage, il paraît essentiel d'impliquer plus largement les acteurs économiques nationaux et régionaux (et sur un

l'ingénierie. À la fin, les projets sont présentés et évalués, offrant parfois des opportunités de financement ou de partenariat.

spectre de capitalisation nettement plus ouvert et transparent) afin de favoriser l'émergence d'une classe "éco-numérique" élargie qui pourrait soutenir et stimuler les politiques à l'échelle nationale et régionale en faveur de solutions résilientes et rentables. Cela nécessite pour ce faire de mobiliser une volonté de générer des solutions innovantes et réactives transversales tout en répondant aux défis spécifiques de chaque pays.

Ainsi, la souveraineté numérique de l'Afrique de l'Ouest pour les années à venir doit être envisagée comme un équilibre subtil et singulier entre autonomie nationale, interdépendance régionale et connectivité globale. Une diplomatie digitale proactive et informée, axée sur la coopération et l'adaptation contextuelle, serait à ce titre essentielle à constituer pour porter et aider à transformer les défis actuels en opportunités durables, garantissant ainsi une place forte et résiliente pour l'Afrique de l'Ouest dans l'économie numérique mondiale.

Bibliographie

Awoleye, O. M. (2021). Reconfiguring Data Infrastructure Ecosystem in Africa: A Primer Toward Digital Sovereignty. ArXiv

Bagayoko, C., Bediang, G., Anne, A., Niang, M., Traoré, A., & Geissbuhler, A. (2017). Digital health and the need to develop centers of expertise in sub-Saharan Africa: two examples in Mali and Cameroon. Medecine et sante tropicales, 27(4), 348-353.

Baromètre des connexions Internet mobiles en Afrique de l'Ouest. (2024). nPerf

Camara, O. M. (2019). Cellular Telephone Internet, and Electronic Communication in Senegal, Mali, and Gambia. Thèse de doctorat. Fort Hays State University.

ChainAnalysis. (2023). The 2023 Geography of Cryptocurrency Report

Degila, J., Tognisse, I. S., Honfoga, A.-C., Houetohossou, S. C. A., Sodedji, F. A. K., Avakoudjo, H. G. G., Tahi, S. P. G., & Assogbadjo, A. E. (2023). A Survey on Digital Agriculture in Five West African Countries. Agriculture, 13, 1067.

Drescher, Daniel. (2017). Blockchain Basics: A Non-Technical Introduction in 25 Steps Apress.

El-Kadi, Tin Hinane. (2024). Learning along the Digital Silk Road? Technology transfer, power, and Chinese ICT corporations in North Africa. The Information Society: An International Journal, 40(2).

Epifanova, Alena. (2020). Deciphering Russia's "Sovereign Internet Law": Tightening Control and Accelerating the Splinternet DGAP Analysis No. 2, German Council on Foreign Relations (DGAP)

Evans, O. (2019). Digital politics: internet and democracy in Africa. Journal of Economic Studies

Gehl Sampath, P., & Tregenna, F. (Eds.) (2022). Digital Sovereignty: African Perspectives Johannesburg: DSI/NRF South African Research Chair in Industrial Development.

Interpol (2024). Rapport Interpol de 2024 sur l'évaluation des cybermenaces en Afrique: Perspectives du Bureau pour les opérations de lutte contre la cybercriminalité en Afrique - 3ème édition

Les annales des Mines (2023). La souveraineté numérique : dix ans de débats, et après ?. N° 23 - Septembre 2023.

Mascellino, A. (2021). DangerousSavanna' Hackers Targeted Financial Institutions in Africa For Two Years. Infosecurity Magazine

OECD. (2023). Blockchain Adoption in Africa: Trends in Market Activity and Policy Development

Partech. (2023). Africa Tech Venture Capital Report 2023

Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4).

Statista. (2024) Internet penetration rate in Ghana. Statista

Ude, N., Ude, K., Ugbor, U., Igwe, C., & Ogu, E. (2021). E-Governance and Economic Development in Sub-Saharan Africa: A Case of Nigeria. International Journal of Development Strategies in Humanities, Management and Social Sciences

UNCTAD. (2024). World Investment Report 2024: Investment Facilitation and Digital Government Geneva: United Nations Conference on Trade and Development (UNCTAD).

ANNEXE 1 :

Tableau 1 : Objectifs principaux de l'Union africaine pour la transformation numérique de l'Afrique (2020-2030)[96]

Objectif	Description
Accès internet universel et abordable	Garantir à tous les citoyens africains un accès sécurisé et abordable à l'internet (6 MB/s à 1/100 de dollar américain par MB) et promouvoir des dispositifs intelligents fabriqués localement (100 dollars maximum).
Investissements dans les infrastructures	Encourager les investissements pour combler le fossé des infrastructures numériques, assurant une bande large accessible, sûre et abordable pour tous, transcendant les différences démographiques et géographiques.
Renforcement du commerce intra-africain	Établir et améliorer les réseaux et services numériques pour renforcer le commerce intra-africain, les flux d'investissements et de capitaux, et l'intégration socio-économique du continent.
Politiques et régulations	Mettre en œuvre des politiques et règlements pour accélérer la transformation numérique aux niveaux national, régional et continental, favorisant la cohérence des stratégies numériques existantes et futures.
Cybersécurité et protection des données	Sensibiliser aux enjeux de cybersécurité et de protection des données, promouvoir des normes ouvertes et l'interopérabilité, et soutenir la mise en vigueur de la Convention de l'Union africaine sur la cybersécurité et la protection des données.
Développement des compétences numériques	Développer des compétences numériques inclusives et des capacités humaines dans les sciences numériques et l'éducation, avec des programmes de formation en ligne visant à fournir des compétences de base à 100 millions d'Africains par an d'ici 2021, et à 300 millions par an d'ici 2025.
Télémédecine et télé-éducation	Soutenir des programmes de télémédecine et de télé-éducation pour transformer la prestation de services et faire de la révolution numérique la base de la société africaine.
Identité légale numérique	Assurer que 99,9% de la population africaine ait une identité légale numérique d'ici 2030.

96 Tableau construit à partir du rapport Union Africaine. (2020). Stratégie de transformation numérique pour l'Afrique 2020-2030

ANNEXE 2

Tableau 2 : Souveraineté et opportunités numériques en Afrique de l'Ouest : enjeux et conditions de déploiement

Ce tableau vise à présenter une analyse des opportunités technologiques numériques déjà examinées ou implantées en faveur de divers secteurs, en y associant les enjeux dans le secteur associé et les conditions standards pour que de telles opportunités puissent être effectives. Cette analyse repose sur des références bibliographiques et des échanges informels avec des experts.

SECTEUR	OPPORTUNITES	ENJEUX	CONDITIONS STANDARDS
Gouvernance	Paiement mobile et plateformes de marketing mobile	Améliorer la transparence des transactions gouvernementales et faciliter l'accès aux services publics.	CYBERSECURITE (cryptographie forte, authentification à deux facteurs), INFRASTRUCTURES (large bande passante, serveurs sécurisés), CAPACITE LOCALE DE DEVELOPPEMENT (développement d'applications mobiles, maintenance des systèmes), CADRE LEGISLATIF(réglementations sur la protection des données, lois sur la confidentialité des utilisateurs)
	Alertes sécuritaires et sanitaires via mobile (SMS, apps)	Renforcer la sécurité publique en fournissant des informations en temps réel et en encourageant la participation citoyenne.	CYBERSECURITE (chiffrement des communications), INFRASTRUCTURES (réseaux mobiles fiables, systèmes de diffusion d'alertes), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en développement de systèmes d'alerte), CADRE LEGISLATIF (lois sur la gestion des urgences, protection des données sensibles)
	Données B2B analytiques FinTech[97]	Utiliser les données analytiques pour améliorer les politiques publiques et la prise de décision stratégique.	CYBERSECURITE (protection contre les cyberattaques, contrôle d'accès), INFRASTRUCTURES (centres de données sécurisés, plateformes d'analyse de données), CAPACITE LOCALE DE DEVELOPPEMENT (expertise en analyse de données, développement de solutions FinTech), CADRE LEGISLATIF(régulations sur l'utilisation des données financières, lois sur la protection des informations financières)
Justice	Blockchain pour la chaîne de valeur et traçabilité	Accroître la transparence et la fiabilité des registres publics, réduisant ainsi la corruption et les fraudes.	CYBERSECURITE (algorithmes de consensus robustes, immuabilité des données), INFRASTRUCTURES (réseaux décentralisés, plateformes blockchain), CAPACITE LOCALE DE DEVELOPPEMENT (connaissances en technologie blockchain, développement de contrats intelligents), CADRE LEGISLATIF(régulations sur l'adoption de la blockchain, lois sur la gestion des registres publics)
Développement Agricole	Systèmes de surveillance électronique des ravageurs et des maladies	Améliorer la productivité agricole et réduire les pertes de récoltes.	CYBERSECURITE (sécurisation des données de surveillance), INFRASTRUCTURES (réseaux de capteurs, plateformes d'analyse en temps réel), CAPACITE LOCALE DE DEVELOPPEMENT (expertise en technologie de détection, analyse de données agricoles), CADRE LEGISLATIF(normes sur la collecte et l'utilisation des données agricoles)
	Agriculture de précision et machines agricoles automatisées	Optimiser les rendements agricoles en utilisant des technologies de pointe pour la gestion des cultures.	CYBERSECURITE (sécurisation des systèmes automatisés), INFRASTRUCTURES (réseaux de communication pour l'IoT, machines agricoles avancées), CAPACITE LOCALE DE DEVELOPPEMENT (formation en utilisation et maintenance des machines agricoles), CADRE LEGISLATIF(régulations sur l'utilisation des technologies agricoles)
	Robotique agricole et traçage des équipements agricoles	Augmenter l'efficacité et la traçabilité des opérations agricole.	CYBERSECURITE (protocole de sécurité pour les équipements robotiques), INFRASTRUCTURES (réseaux de communication, systèmes de gestion d'équipements), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en robotique, gestion des

97 Les données B2B analytiques FinTech (technologies financières) se réfèrent aux informations et aux analyses utilisées par les entreprises (business-to-business, ou B2B) pour prendre des décisions financières stratégiques et améliorer leurs opérations. Ces données proviennent de diverses sources et sont traitées à l'aide de technologies analytiques avancées pour offrir des insights précieux.

			équipement agricoles), CADRE LEGISLATIF(normes sur l'utilisation des équipements agricoles)
	Plateformes de marché numérique agricole en mode cloud	Faciliter l'accès des agriculteurs aux marchés et aux informations en temps réel.	CYBERSECURITE (sécurisation des transactions et des données sur le cloud), INFRASTRUCTURES (centres de données sécurisés, plateformes cloud), CAPACITE LOCALE DE DEVELOPPEMENT (expertise en e-commerce agricole, solutions cloud), CADRE LEGISLATIF(régulations sur les transactions numériques, protection des données)
	Prévision des prix agricoles	Aider les agriculteurs à prendre des décisions informées en fonction des tendances du marché.	CYBERSECURITE (sécurisation des données de prévision), INFRASTRUCTURES (plateformes d'analyse de données, accès à des données de marché), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en analyse de marché, modélisation économique), CADRE LEGISLATIF(régulations sur l'utilisation des données de marché)
	Assurance-index météorologique / télédétection	Fournir des solutions d'assurance basées sur des indices pour protéger les agriculteurs contre les risques climatiques.	CYBERSECURITE (protection des données météorologiques et des indices de risque), INFRASTRUCTURES (systèmes de télédétection, plateformes d'analyse climatique), CAPACITE LOCALE DE DEVELOPPEMENT (expertise en télédétection, analyse climatique), CADRE LEGISLATIF(régulations sur les assurances agricoles, gestion des risques climatiques)
	Test des sols en temps réel	Améliorer la gestion des sols et la fertilité des terres agricoles.	CYBERSECURITE (sécurisation des dispositifs de test et des données), INFRASTRUCTURES (réseaux de capteurs, plateformes d'analyse de données), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en agronomie, technologies de test), CADRE LEGISLATIF(normes sur la collecte et l'utilisation des données de sols)
	Transfert d'ingénierie agricole open source avec tutoriel	Faciliter l'accès aux technologies agricoles avancées pour les petits agriculteurs.	CYBERSECURITE (protection des plateformes de partage), INFRASTRUCTURES (plateformes open source, accès à internet), CAPACITE LOCALE DE DEVELOPPEMENT (formation et éducation en ingénierie agricole), CADRE LEGISLATIF(régulations sur les licences open source, partage des connaissances)
	Relevé simplifié des prix locaux pour un suivi plus granulaire de l'évolution des marchés locaux	Fournir des informations précises et à jour sur les prix des produits agricoles, aidant ainsi les agriculteurs à obtenir des prix équitables.	CYBERSECURITE (sécurisation des données de marché), INFRASTRUCTURES (plateformes de collecte de données, réseaux de communication), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en collecte et analyse de données de marché), CADRE LEGISLATIF(régulations sur la transparence des prix, protection des données)
	Mécanisation électronique	Améliorer l'efficacité des opérations agricoles grâce à l'automatisation.	CYBERSECURITE (protection des systèmes électroniques), INFRASTRUCTURES (réseaux de communication, équipements automatisé), CAPACITE LOCALE DE DEVELOPPEMENT (formation en utilisation et maintenance des équipements), CADRE LEGISLATIF(normes sur l'utilisation des technologies agricoles)
	Traçabilité partielle et suivi de la chaîne d'approvisionnement	Assurer la traçabilité des produits agricoles depuis la ferme jusqu'au consommateur, améliorant ainsi la transparence et la qualité.	CYBERSECURITE (sécurisation des données de traçabilité), INFRASTRUCTURES (plateformes de gestion de la chaîne d'approvisionnement, réseaux de communication), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en gestion de la chaîne d'approvisionnement, technologie de traçabilité), CADRE LEGISLATIF(régulations sur la traçabilité des produits, protection des données)
	Systèmes d'irrigation intelligents alimentés à l'énergie solaire	Optimiser l'utilisation de l'eau pour l'irrigation tout en utilisant des sources d'énergie renouvelables.	CYBERSECURITE (protection des systèmes d'irrigation automatisés), INFRASTRUCTURES (réseaux de capteurs, systèmes d'irrigation intelligents), CAPACITE LOCALE DE DEVELOPPEMENT (formation en gestion des systèmes d'irrigation, utilisation de l'énergie solaire), CADRE LEGISLATIF(régulations sur l'utilisation de l'eau, promotion des énergies renouvelables)
Société civile et participation citoyenne	Services consultatifs hors ligne utilisant des outils audio et vidéo (tablettes)	Améliorer l'accès à l'information et aux services pour les communautés éloignées et marginalisées.	CYBERSECURITE (sécurisation des dispositifs et des communications), INFRASTRUCTURES (accès à internet, dispositifs audio et vidéo), CAPACITE LOCALE DE DEVELOPPEMENT (formation en utilisation des technologies, maintenance des dispositifs), CADRE LEGISLATIF(régulations sur la protection des données personnelles, droits d'accès à l'information)
Santé	Alertes sanitaires via mobile (SMS, apps)	Fournir des informations en temps réel sur les urgences sanitaires et améliorer la gestion des crises.	CYBERSECURITE (chiffrement des données de santé), INFRASTRUCTURES (réseaux mobiles fiables, systèmes de diffusion d'alertes sanitaires), CAPACITE LOCALE DE DEVELOPPEMENT

			(compétences en développement de systèmes d'alerte sanitaire), CADRE LEGISLATIF(lois sur la gestion des urgences sanitaires, protection des données de santé)
Fintech et données b2b analytiques	Analyse des données pour l'agriculture	Utiliser les données pour optimiser les pratiques agricoles et améliorer les rendements.	CYBERSECURITE (protection des données agricoles), INFRASTRUCTURES (plateformes d'analyse de données, réseaux de communication), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en analyse de données, technologies agricoles), CADRE LEGISLATIF(régulations sur l'utilisation des données agricoles)
	Observatoire de l'agriculture	Suivre les tendances et les développements agricoles pour une prise de décision informée.	CYBERSECURITE (sécurisation des systèmes de collecte et d'analyse de données), INFRASTRUCTURES (centres de données sécurisés, plateformes d'observation), CAPACITE LOCALE DE DEVELOPPEMENT (expertise en surveillance agricole, analyse de données), CADRE LEGISLATIF(régulations sur la collecte et la diffusion des données agricoles)
Éducation	Plateformes d'apprentissage en ligne	Faciliter l'accès à l'éducation pour tous, notamment dans les zones rurales et isolées.	CYBERSECURITE (protection des données des apprenants), INFRASTRUCTURES (accès à internet, plateformes d'apprentissage en ligne), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en développement de contenus éducatifs, utilisation des technologies d'apprentissage), CADRE LEGISLATIF(régulations sur l'éducation numérique, protection des données)
	Suivi de la performance scolaire	Permettre une évaluation précise et continue des performances scolaires des élèves.	CYBERSECURITE (sécurisation des données scolaires), INFRASTRUCTURES (plateformes de suivi scolaire, accès à internet), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en gestion des données scolaires, analyse de performance), CADRE LEGISLATIF(régulations sur la collecte et l'utilisation des données éducatives)
Environnement	Surveillance de la biodiversité	Protéger et surveiller la biodiversité pour une gestion durable des ressources naturelles.	CYBERSECURITE (sécurisation des systèmes de collecte et d'analyse de données), INFRASTRUCTURES (réseaux de capteurs, plateformes de gestion de données environnementales), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en écologie, analyse de données environnementales), CADRE LEGISLATIF(régulations sur la protection de la biodiversité, gestion des ressources naturelles)
Emploi	Plateformes de recrutement en ligne	Faciliter la recherche d'emploi et la mise en relation entre les employeurs et les demandeurs d'emploi.	CYBERSECURITE (protection des données personnelles des utilisateurs), INFRASTRUCTURES (plateformes de recrutement en ligne, accès à internet), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en gestion de plateformes de recrutement, matching algorithmique), CADRE LEGISLATIF(régulations sur la protection des données personnelles, droit du travail)
	Formation professionnelle	Offrir des cours en ligne et des ressources de formation professionnelle accessibles via des applications mobiles pour développer les compétences et augmenter les chances d'emploi.	CYBERSECURITE (protection des données des apprenants), INFRASTRUCTURES (plateformes de formation en ligne, accès à internet), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en développement de contenus de formation, utilisation des technologies éducatives), CADRE LEGISLATIF(régulations sur l'éducation numérique, protection des données)
Infrastructure	Suivi des projets d'INFRASTRUCTURES	Utiliser des applications mobiles pour suivre la progression des projets d'INFRASTRUCTURES, collecter des données en temps réel et assurer la transparence dans la gestion des fonds publics.	CYBERSECURITE (sécurisation des systèmes de suivi), INFRASTRUCTURES (réseaux de communication fiables, plateformes de gestion de projets), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en gestion de projets d'infrastructure, analyse de données en temps réel), CADRE LEGISLATIF(régulations sur la transparence des projets publics, gestion des fonds publics)
	Maintenance préventive	Mettre en place des systèmes de maintenance préventive basés sur des capteurs connectés pour prolonger la durée de vie des INFRASTRUCTURES et réduire les coûts de réparation.	CYBERSECURITE (protection des systèmes de maintenance), INFRASTRUCTURES (réseaux de capteurs, plateformes de gestion de maintenance), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en technologie de capteurs, gestion de maintenance préventive), CADRE LEGISLATIF(régulations sur l'entretien des INFRASTRUCTURES publiques, utilisation des capteurs)
Tourisme	Guides touristiques numériques	Développer des applications mobiles pour fournir des guides touristiques interactifs, des informations sur les sites	CYBERSECURITE (protection des données des utilisateurs), INFRASTRUCTURES (plateformes d'information touristique, réseaux de communication), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en développement d'applications

		historiques et culturels, et faciliter les réservations en ligne.	touristiques, gestion de contenus culturels), CADRE LEGISLATIF(régulations sur la protection des données, lois sur le tourisme)
	Promotion de l'écotourisme	Utiliser des plateformes en ligne pour promouvoir les destinations écotouristiques, sensibiliser à la conservation de la nature et encourager un tourisme durable..	CYBERSECURITE (sécurisation des données des utilisateurs), INFRASTRUCTURES (plateformes de promotion touristique, réseaux de communication), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en gestion de contenus écotouristiques, promotion en ligne), CADRE LEGISLATIF(régulations sur la protection des données, lois sur le tourisme)
Finance Inclusive	Microfinance numérique	Faciliter l'accès aux services financiers pour les populations non bancarisées à travers des plateformes de microfinance numérique, permettant des transactions sécurisées via mobile.	CYBERSECURITE (sécurisation des transactions financières), INFRASTRUCTURES (plateformes de microfinance, accès à internet mobile), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en gestion de microfinance, technologies financières), CADRE LEGISLATIF(régulations sur les services financiers, protection des données financières)
	Épargne et crédit collaboratifs	Mettre en place des systèmes d'épargne et de crédit collaboratifs basés sur la blockchain pour encourager l'inclusion financière et stimuler l'entrepreneuriat local.	CYBERSECURITE (protection des transactions et des données), INFRASTRUCTURES (plateformes blockchain, accès à internet), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en technologies blockchain, gestion de services financiers), CADRE LEGISLATIF(régulations sur la blockchain, services financiers collaboratifs)
Culture et Art	Promotion des arts locaux	Utiliser des plateformes en ligne pour promouvoir les artistes locaux, faciliter la vente d'œuvres d'art et encourager l'appréciation de la culture africaine.	CYBERSECURITE (protection des données des utilisateurs), INFRASTRUCTURES (plateformes de promotion artistique, accès à internet), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en gestion de plateformes artistiques, marketing digital), CADRE LEGISLATIF(régulations sur la protection des données, droits d'auteur)
	Archivage numérique du patrimoine culturel	Développer des archives numériques pour préserver le patrimoine culturel africain, y compris la musique, la littérature, l'artisanat et les traditions orales.	CYBERSECURITE (sécurisation des archives numériques), INFRASTRUCTURES (plateformes d'archivage, accès à internet), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en numérisation et gestion des archives, préservation du patrimoine), CADRE LEGISLATIF(régulations sur la protection des données, droits d'auteur)
Innovation Technologique	Incubateurs de startups Technologiques	Créer des incubateurs de startups Technologiques pour soutenir l'innovation locale, encourager l'entrepreneuriat et stimuler l'économie numérique.	CYBERSECURITE (protection des données et des innovations), INFRASTRUCTURES (espaces de coworking, accès à internet haut débit), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en gestion d'incubateurs, développement de startups), CADRE LEGISLATIF(régulations sur l'innovation, soutien à l'entrepreneuriat)
	Hackathons et compétitions technologiques	Organiser des événements de codage et des compétitions technologiques pour stimuler la créativité, encourager la collaboration et résoudre les défis locaux grâce à la technologie.	CYBERSECURITE (protection des données des participants), INFRASTRUCTURES (espaces pour événements, accès à internet haut débit), CAPACITE LOCALE DE DEVELOPPEMENT (compétences en organisation d'événements, gestion de communautés technologiques), CADRE LEGISLATIF(régulations sur l'innovation, soutien à l'entrepreneuriat)

PASAS

Introduction

PLATEFORME D'ANALYSE,
DE SUIVI ET D'APPRENTISSAGE
AU SAHEL

PORTÉ PAR

MINKA | AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT

pasas-minka.fr

Ce rapport a été élaboré dans le cadre d'un financement du Fonds Paix et Résilience Minka.

Le Fonds Minka, mis en œuvre par le groupe AFD, est la réponse opérationnelle de la France à l'enjeu de lutte contre la fragilisation des États et des sociétés. Lancé en 2017, Minka finance des projets dans des zones affectées par un conflit violent, avec un objectif : la consolidation de la paix. Il appuie ainsi quatre bassins de crise via quatre initiatives : l'Initiative Minka Sahel, l'Initiative Minka Lac Tchad, l'Initiative Minka RCA et l'Initiative Minka Moyen-Orient.

La Plateforme d'Analyse, de Suivi et d'Apprentissage au Sahel (PASAS) est financée par le Fonds Paix et Résilience Minka. Elle vise à éclairer les choix stratégiques et opérationnels des acteurs de développement locaux et internationaux, en lien avec les situations de crises et de fragilités au Sahel et dans le bassin du Lac Tchad. La PASAS se met en œuvre à travers d'un accord-cadre avec le groupement IRD-ICE après appel d'offres international dont le rôle est double : (i) produire des connaissances en réponse à nos enjeux opérationnels de consolidation de la paix au Sahel et (ii) valoriser ces connaissances à travers deux outils principaux : une plateforme numérique, accessible à l'externe, qui accueillera toutes les productions et des conférences d'échange autour des résultats des études. La plateforme soutient ainsi la production et le partage de connaissances, en rassemblant des analyses robustes sur les contextes sahéliens et du pourtour du Lac Tchad.

IRD Institut de Recherche pour le Développement FRANCE | ICE FRANCE | UK International Development Partnership | Progress | Prosperity | ALLIANCE SAHEL