

INTELLIGENCE ARTIFICIELLE, SOUVERAINETÉ NUMÉRIQUE ET SÉCURITÉ AFRICAINE : RENFORCER LE RENSEIGNEMENT MILITAIRE, LA PRÉVISION ÉCONOMIQUE ET LA GOUVERNANCE RÉGLEMENTAIRE À L'ÈRE NUMÉRIQUE

INTRODUCTION

L'intelligence artificielle transforme rapidement l'architecture de la sécurité nationale, de la gouvernance économique et de l'administration publique. Partout en Afrique, les gouvernements, les institutions financières et les services de sécurité explorent de plus en plus les systèmes fondés sur l'IA afin de renforcer leurs capacités de renseignement, d'améliorer la résilience en matière de cybersécurité, de détecter les menaces émergentes, de protéger les infrastructures critiques et d'appuyer la prise de décision économique fondée sur les données. Ces évolutions offrent d'importantes possibilités d'innovation, de développement et d'autonomie stratégique. Elles soulèvent également de profondes questions juridiques et institutionnelles relatives à la redevabilité, aux droits humains, à la dépendance technologique et à la souveraineté.

La question centrale n'est donc plus de savoir si l'intelligence artificielle s'intégrera aux institutions africaines. Elle l'est déjà. La question la plus déterminante est celle de savoir selon quels termes cette transformation s'opérera. Les États africains exerceront-ils une autorité réelle sur les données, les infrastructures, les algorithmes et les normes réglementaires qui influencent de plus en plus leur sécurité et leur économie ? Ou le continent deviendra-t-il dépendant de systèmes technologiques dont l'architecture et la logique décisionnelle sont principalement contrôlées ailleurs ?

Cet article soutient que l'intelligence artificielle peut renforcer la sécurité, la résilience économique et l'autonomie stratégique de l'Afrique, mais uniquement si son déploiement repose sur trois fondements : une souveraineté numérique réelle, une capacité technologique et institutionnelle africaine suffisante, et une gouvernance réglementaire ancrée dans l'État de droit. L'analyse se déploie autour de trois domaines interconnectés : la sécurité et le renseignement militaire ; la prévision économique ; et la gouvernance réglementaire. Ces domaines sont reliés par une ressource commune - les données ; une dépendance commune - l'infrastructure numérique et informatique ; et une question juridique commune : qui exerce le contrôle, selon quelles règles, et devant qui rend-il des comptes ?

La souveraineté militaire sans souveraineté sur les données est incomplète. La souveraineté économique sans capacité technologique est fragile. La capacité technologique sans redevabilité juridique peut elle-même devenir une source d'insécurité. Cet article rejette par conséquent le faux choix entre innovation technologique et réglementation. Le choix véritablement déterminant pour l'Afrique se situe entre une innovation encadrée et une dépendance non maîtrisée.

LA SOUVERAINETÉ NUMÉRIQUE : LE FONDEMENT CONCEPTUEL

La souveraineté numérique est parfois assimilée à l'autosuffisance technologique. Une telle conception n'est ni réaliste ni nécessaire.

Aucun État contemporain ne jouit d'une indépendance technologique absolue. Les chaînes d'approvisionnement en semi-conducteurs, les infrastructures cloud, les réseaux de télécommunications, les ensembles de données et les modèles d'intelligence artificielle fonctionnent au sein d'écosystèmes transnationaux complexes. La souveraineté numérique africaine ne peut donc en aucun cas signifier un isolement technologique.

Elle doit plutôt être comprise comme la capacité des États et institutions africains à faire des choix autonomes, informés et juridiquement contraignants concernant les données, les infrastructures critiques, les dépendances technologiques, les relations d'approvisionnement et les normes réglementaires.

Quatre dimensions revêtent une importance particulière.

- i. Premièrement, la **souveraineté des données** concerne le contrôle de la collecte, du traitement, du transfert, du stockage et de l'accessibilité des données stratégiques et personnelles.
- ii. Deuxièmement, la **souveraineté des infrastructures** concerne un contrôle réel sur les infrastructures informatiques, cloud, de télécommunications et numériques dont dépendent les institutions critiques.
- iii. Troisièmement, la **souveraineté technologique et en matière de compétences** exige une expertise nationale et continentale suffisante pour comprendre, auditer, entretenir, acquérir et, lorsque cela est stratégiquement approprié, développer les technologies critiques.
- iv. Quatrièmement, la **souveraineté réglementaire** concerne la capacité de l'Afrique à déterminer les conditions juridiques d'exploitation de l'IA, plutôt que de se contenter de recevoir des normes réglementaires élaborées ailleurs.

Cette distinction révèle un paradoxe central de la souveraineté technologique contemporaine : **la propriété n'équivaut pas nécessairement au contrôle.**

Un État peut posséder des drones militaires tout en dépendant de systèmes de navigation étrangers et de logiciels propriétaires. Une banque centrale peut déployer une analyse prédictive sophistiquée tout en traitant des informations financières sensibles au moyen d'infrastructures contrôlées à l'étranger. Un département gouvernemental peut acquérir un système d'IA tout en demeurant incapable de vérifier le modèle sur lequel il repose.

Dans chacun de ces cas, la capacité technologique a augmenté tandis que le contrôle souverain a pu diminuer. La Stratégie continentale de l'Union africaine sur l'intelligence artificielle constitue un fondement important pour relever ce défi. Cependant, la stratégie continentale doit en définitive se traduire en infrastructures, institutions, financements, compétences et règles contraignantes.

Le Cap-Vert offre un exemple concret de ce à quoi peut ressembler, dans la pratique, cette conception multidimensionnelle de la souveraineté numérique.

Le Cap-Vert offre un exemple instructif de la manière dont la transformation numérique peut allier infrastructures technologiques, numérisation du secteur public et capacités réglementaires. Dans le cadre du projet « Digital Cabo Verde », soutenu par la Banque mondiale, environ 40 millions de dollars américains ont été alloués au renforcement de l'économie numérique du pays, notamment par des investissements dans les services publics numériques et dans l'environnement juridique et réglementaire. Cette transformation a produit des résultats mesurables : plus de 700 institutions publiques sont interconnectées, plus de 100 solutions d'administration en ligne ont été développées et le taux de pénétration du haut débit mobile a atteint 85,8 % en mars 2025. Le portail consulaire traite également 62 % des demandes en moins d'une journée et a réduit de 85 % le délai de délivrance des documents électroniques.

Le Cap-Vert passe désormais d'une numérisation classique à une gouvernance fondée sur l'intelligence artificielle. La coopération entre la NOSi et l'Université du Cap-Vert a permis d'étudier des solutions basées sur l'IA pour le secteur public, tandis que des applications potentielles ont également été identifiées dans le domaine des marchés publics. L'expérience du pays démontre que la souveraineté numérique ne se limite pas à la mise en ligne des services publics. À mesure que l'IA s'intègre dans l'administration publique, les capacités technologiques doivent se développer parallèlement à la résilience en matière de cybersécurité, aux capacités réglementaires, à la transparence et à une gouvernance responsable. Le Cap-Vert illustre ainsi à la fois le potentiel de la transformation numérique africaine et les garanties institutionnelles nécessaires pour la pérenniser.

L'objectif de l'Afrique ne devrait donc pas être l'autosuffisance technologique. Il devrait être l'interdépendance stratégique : la capacité de participer aux écosystèmes technologiques mondiaux sans renoncer à un contrôle réel sur les intérêts africains essentiels. La question centrale n'est par conséquent pas de savoir si l'Afrique dépendra de

technologies extérieures. Une certaine dépendance est inévitable. La question est de savoir si l'Afrique peut choisir, diversifier, négocier et encadrer ces dépendances, plutôt que de simplement les hériter.

L'IA, LE RENSEIGNEMENT MILITAIRE, LA CYBERSÉCURITÉ ET LA SÉCURITÉ PUBLIQUE

A. L'IA en tant que capacité de sécurité

La nature des menaces sécuritaires auxquelles les États africains sont confrontés évolue. Dans le Sahel, la Corne de l'Afrique, l'est de la République démocratique du Congo et d'autres régions touchées par les conflits, les défis sécuritaires classiques se conjuguent de plus en plus aux drones, à la surveillance numérique, aux opérations cybernétiques, à la désinformation et aux groupes armés technologiquement équipés. L'intelligence artificielle peut renforcer le renseignement, l'analyse d'images satellitaires, la reconnaissance, la logistique, les systèmes d'alerte précoce, la surveillance en matière de cybersécurité et la détection des menaces.

L'examen par le Conseil de paix et de sécurité de l'Union africaine des questions relatives à l'intelligence artificielle, à la gouvernance, à la paix et à la sécurité démontre que l'IA n'est plus une simple question de politique technologique. Elle est devenue un enjeu de sécurité continentale. Or, l'accroissement de la capacité technologique peut générer de nouvelles dépendances stratégiques.

Une institution de défense africaine qui dépend de logiciels, d'infrastructures de communication ou de systèmes propriétaires contrôlés à l'étranger peut améliorer sa capacité opérationnelle immédiate tout en créant simultanément des vulnérabilités relatives à l'accès, à la maintenance, à la sécurité des données et à la continuité du service. La véritable mesure de la souveraineté n'est donc pas de savoir si un État possède un équipement sophistiqué, mais s'il exerce un contrôle suffisant sur l'écosystème technologique dont cet équipement dépend.

B. Cybersécurité et infrastructures critiques

Cette préoccupation devient particulièrement aiguë dans le cyberspace.

L'intelligence artificielle peut aider les gouvernements et les institutions à détecter les comportements anormaux du réseau, à identifier les logiciels malveillants, à hiérarchiser les incidents et à renforcer la protection des systèmes bancaires, des réseaux énergétiques, des infrastructures de télécommunications et des bases de données gouvernementales. Mais l'IA est intrinsèquement à double usage. Les mêmes capacités peuvent améliorer l'hameçonnage, automatiser certains éléments des cyberattaques, renforcer la désinformation et permettre aux acteurs malveillants d'opérer avec davantage de rapidité et d'ampleur.

Les conceptions africaines de la sécurité nationale doivent par conséquent dépasser la seule sécurité territoriale. Une attaque sérieuse contre les réseaux électriques, les systèmes financiers, les infrastructures de télécommunications, les infrastructures électorales ou les bases de données gouvernementales peut déstabiliser un État sans qu'aucune arme conventionnelle ne franchisse sa frontière. La résilience cybernétique doit donc être comprise comme un élément de la souveraineté elle-même.

C. Sécurité prédictive et suspicion algorithmique

L'IA soulève également des questions délicates lorsque les gouvernements emploient des technologies prédictives à des fins de police, de contrôle des frontières ou de sécurité publique. Les systèmes prédictifs peuvent aider les autorités à repérer des tendances et à répartir des ressources limitées. Mais leur apparente objectivité peut être trompeuse. Un algorithme ne comprend pas intrinsèquement les conditions historiques, politiques ou socioéconomiques reflétées dans les données qu'il traite. Lorsque les ensembles de données historiques intègrent des pratiques discriminatoires, un système d'IA peut reproduire ces inégalités tout en présentant la décision qui en résulte comme technologiquement neutre. Le biais algorithmique n'est donc pas un simple problème d'ingénierie. Lorsque l'IA influence les arrestations,

la surveillance, l'accès aux frontières ou d'autres exercices de la puissance publique, le biais devient un problème constitutionnel et un problème d'État de droit.

Le danger s'accroît lorsque l'analyse prédictive est combinée à la reconnaissance faciale ou à la surveillance de masse. Les objectifs de sécurité ne sauraient justifier une intrusion technologique illimitée. L'IA au service de la sécurité publique devrait donc demeurer régie par la légalité, la nécessité, la proportionnalité, la non-discrimination, un contrôle indépendant et un recours effectif.

D. L'IA militaire et la responsabilité humaine

L'analyse juridique doit également distinguer entre le renseignement assisté par IA, les systèmes télé-opérés, les technologies de ciblage automatisé et les armes autonomes. Ces technologies ne soulèvent pas des questions juridiques identiques. Ce qu'elles ont en commun, c'est que l'innovation technologique ne dispense pas des obligations existantes en vertu du droit international humanitaire. Les principes de distinction, de proportionnalité et de précaution continuent de régir les opérations militaires, indépendamment du degré de sophistication de la technologie employée.

Un contrôle humain réel revêt une importance particulière lorsqu'un système d'IA influence de manière substantielle des décisions relatives au recours à la force. L'IA peut accroître la quantité d'informations dont dispose un décideur. Elle ne possède ni agentivité morale, ni responsabilité juridique, ni jugement contextuel équivalents à ceux d'une décision humaine. Le principe fondamental doit donc demeurer le suivant : l'intelligence artificielle peut assister le décideur ; elle ne doit jamais devenir un décideur non redevable.

L'IA ET LA PRÉVISION ÉCONOMIQUE : VERS UNE POLITIQUE MONÉTAIRE AUGMENTÉE

La sécurité n'est pas exclusivement militaire. L'instabilité économique, l'inflation, l'insécurité alimentaire, les pénuries énergétiques et les mouvements de capitaux déstabilisateurs peuvent fragiliser les institutions et engendrer une instabilité politique. La résilience économique doit donc faire partie de toute conception sérieuse de la sécurité africaine.

L'IA offre à cet égard d'importantes possibilités. Elle peut traiter de vastes ensembles de données relatifs à l'inflation, aux rendements agricoles, aux prix des matières premières, à la consommation énergétique, au comportement financier, aux échanges commerciaux et aux flux de capitaux, à des vitesses dépassant l'analyse humaine conventionnelle. Correctement déployés, ces systèmes peuvent améliorer les prévisions, favoriser une intervention plus précoce et permettre une allocation plus efficace des ressources publiques.

Les estimations de la contribution économique potentielle de l'IA en Afrique illustrent l'ampleur de cette opportunité. Dans un rapport publié le 25 février 2021, la Commission économique des Nations unies pour l'Afrique (CEA) a observé que l'Afrique pourrait voir son économie croître d'environ 1 500 milliards de dollars américains d'ici 2030 si le continent parvenait à capter ne serait-ce que 10 % du marché mondial de l'intelligence artificielle, en pleine expansion, qui devrait alors atteindre environ 15 700 milliards de dollars américains d'ici 2030. Bien que ces projections ne soient ni définitives ni garanties, elles fournissent une indication utile de l'ampleur de la contribution potentielle de l'IA à la transformation économique de l'Afrique. La concrétisation de ce potentiel dépendra toutefois non seulement de l'adoption des technologies, mais aussi de la capacité du continent à développer les infrastructures numériques, le capital humain, les écosystèmes d'investissement, les capacités institutionnelles et les cadres de gouvernance efficaces nécessaires.

L'engagement de la BCEAO envers l'intelligence artificielle constitue un exemple africain instructif. La création d'une initiative de réflexion sur l'IA et l'organisation, en 2025, de sa conférence internationale sur l'IA et la banque centrale témoignent d'une reconnaissance institutionnelle croissante de la pertinence de l'IA pour la gouvernance monétaire. Mais la prévision augmentée par l'IA crée un problème nouveau : lorsque la puissance analytique augmente, les conséquences d'une erreur analytique peuvent augmenter avec elle.

Un modèle opaque ou insuffisamment validé qui influence de manière substantielle la politique monétaire pourrait produire des erreurs touchant l'ensemble d'une économie ou d'une union monétaire. Il existe également une préoccupation systémique moins évidente. Si de nombreuses institutions financières dépendent des mêmes modèles, fournisseurs de données ou prestataires technologiques, l'erreur algorithmique peut devenir corrélée. Ce qui semble être une efficacité technologique peut ainsi créer un risque de concentration systémique.

La réglementation financière africaine doit donc évoluer au-delà de la protection classique des données afin d'aborder la gouvernance des modèles, l'auditabilité, la validation, la cybersécurité, la concentration des fournisseurs, l'explicabilité et la responsabilité institutionnelle. L'intelligence artificielle peut augmenter la gouvernance monétaire. Elle ne doit pas la rendre non redevable.

LA GOUVERNANCE RÉGLEMENTAIRE : UN CHANTIER INACHEVÉ

Le défi réglementaire de l'Afrique ne réside pas principalement dans l'absence de principes. Il réside dans la conversion de ces principes en institutions effectives et en obligations exécutoires.

La Convention de Malabo constitue le cadre continental de référence en matière de cybersécurité et de protection des données. Adoptée le 27 juin 2014, il lui aura fallu près de neuf années pour entrer en vigueur, en juin 2023, faute d'un nombre suffisant de ratifications. Aujourd'hui encore, le constat demeure préoccupant : selon les données les plus récentes de l'Union africaine, seuls 20 des 55 États membres, soit à peine deux sur cinq, ont ratifié la Convention ou y ont adhéré et déposé leurs instruments. Le Cap-Vert, pays hôte de cette conférence, fait figure d'exemple encourageant : il a ratifié la Convention ou y a adhéré dès le 13 novembre 2020, avant de déposer son instrument le 5 février 2022. Cet engagement témoigne d'une volonté précoce de renforcer la gouvernance numérique et la protection des données sur le continent. Puisse cet exemple inspirer les autres États africains à transformer l'ambition continentale en engagement juridique effectif.

Les États ne peuvent poursuivre crédiblement une transformation numérique de plus en plus sophistiquée tout en laissant sous-développée l'architecture juridique protégeant la cybersécurité, les données personnelles et les droits individuels. Mais la Convention de Malabo, à elle seule, ne peut répondre à toutes les questions que soulève l'IA contemporaine.

L'intelligence artificielle soulève des problèmes réglementaires que la législation classique sur la protection des données ne résout pas entièrement :

- v. Qui est responsable lorsqu'un algorithme contribue de manière substantielle à une décision administrative illégale ?
- vi. Dans quels cas la prise de décision automatisée est-elle inappropriée, indépendamment de son efficacité ?
- vii. Quelles informations doivent être communiquées à une personne concernée par une décision gouvernementale assistée par l'IA ?
- viii. Comment la discrimination algorithmique doit-elle être prouvée ?
- ix. À partir de quand la dépendance technologique envers un fournisseur étranger devient-elle un enjeu de sécurité nationale ?
- x. Et quels recours devraient exister lorsque l'IA cause un préjudice juridiquement reconnu ?

Ces questions appellent une réponse réglementaire spécifique à l'IA.

L'émergence d'initiatives de gouvernance spécifiques à l'IA au sein de certains États africains montre toutefois que le continent ne part pas d'un vide réglementaire. Le Rwanda en offre un exemple particulièrement instructif.

Le Rwanda offre un exemple instructif d'intégration délibérée de l'intelligence artificielle dans la politique nationale de développement. Sa politique nationale en matière d'intelligence artificielle, adoptée en 2023, vise à tirer parti de l'IA pour accélérer la croissance économique, améliorer les services publics et promouvoir une innovation responsable et inclusive. Il est important de noter que cette ambition technologique s'inscrit dans le cadre de dispositifs régissant la protection des données à caractère personnel, la vie privée, la cybersécurité et la gouvernance responsable des données, démontrant ainsi que l'innovation et la réglementation ne doivent pas nécessairement évoluer en parallèle.

Le Rwanda s'est également engagé dans le développement d'applications d'IA adaptées au contexte local. Un projet pilote notable d'IA générative destiné à soutenir les agents de santé communautaires a combiné le GPT-4 avec un modèle de traduction anglais-kinyarwanda ; les évaluations indiquent que la précision est passée de 8 % (valeur de référence) à 71 %. Cet exemple est significatif non seulement en raison des progrès technologiques réalisés, mais aussi parce qu'il illustre l'importance de développer des systèmes d'IA adaptés aux langues locales, aux besoins institutionnels et aux réalités socio-économiques.

L'Afrique n'a pas à construire ce cadre dans l'isolement. Les évolutions réglementaires internationales offrent des enseignements utiles. La Recommandation de l'UNESCO sur l'éthique de l'intelligence artificielle met l'accent sur les droits humains, la proportionnalité, la vie privée, la transparence, la redevabilité, la sûreté, la non-discrimination et le contrôle humain. Les Principes de l'OCDE sur l'IA insistent de même sur les valeurs centrées sur l'humain, la transparence, la robustesse, la sécurité et la redevabilité.

La loi européenne sur l'intelligence artificielle démontre l'utilité d'une réglementation fondée sur le risque : le principe selon lequel l'intensité réglementaire doit croître avec la gravité potentielle du préjudice causé par une application donnée de l'IA. L'Afrique devrait s'inspirer de ces cadres sans les reproduire mécaniquement.

Une réglementation conçue pour la capacité institutionnelle, les structures économiques et les marchés technologiques européens ne peut être simplement transposée dans les juridictions africaines en espérant des résultats identiques. Le meilleur objectif est une interopérabilité réglementaire sans dépendance réglementaire. L'Afrique a besoin d'un modèle de gouvernance suffisamment compatible avec les normes internationales pour faciliter le commerce, l'investissement et la coopération technologique, tout en étant suffisamment africain dans sa conception pour refléter les capacités institutionnelles, les langues, les traditions constitutionnelles, les environnements sécuritaires et les priorités de développement du continent.

L'île Maurice offre un exemple récent de la manière dont une telle approche, centrée sur l'Afrique et intégrée sur le plan institutionnel, pourrait fonctionner dans la pratique.

L'île Maurice propose un modèle émergent de gouvernance intégrée de l'IA. Son « Plan directeur de transformation numérique 2025-2029 » associe les infrastructures numériques, la réforme réglementaire, la cybersécurité, la gouvernance des données et l'IA au sein d'une stratégie nationale unifiée. En avril 2026, l'île Maurice a en outre lancé sa stratégie nationale en matière d'IA et ses lignes directrices FAIR, mettant l'accent sur l'équité, la responsabilité, l'inclusivité, l'intégrité et la responsabilité, avec le soutien d'une unité dédiée à l'IA.

Il est significatif de noter que la cyber-résilience - notamment la protection des infrastructures critiques, le partage d'informations sur les menaces et la capacité de cloud souverain - est considérée comme une composante à part entière de la transformation numérique. Élaborée dans le cadre d'un partenariat entre les pouvoirs publics, le secteur privé et la population, l'approche mauricienne démontre que l'adoption durable de l'IA nécessite que les capacités technologiques, les institutions responsables, la cybersécurité, une réglementation appropriée et la confiance du public évoluent de concert.

UN CADRE AFRICAIN DE REDEVABILITÉ EST NÉCESSAIRE

Un cadre continental pourrait s'articuler autour de huit principes fondamentaux :

- a. **Légalité** : l'IA du secteur public doit reposer sur une autorité juridique identifiable.
- b. **Nécessité** : le déploiement doit répondre à un objectif légitime et démontrable.
- c. **Proportionnalité** : l'intrusion technologique ne doit pas excéder ce que requiert raisonnablement l'objectif poursuivi.
- d. **Transparence** : les personnes substantiellement concernées par l'IA devraient recevoir une information significative sur son rôle dans la décision.
- e. **Redevabilité** : la responsabilité juridique doit demeurer attribuable à des acteurs humains et institutionnels identifiables.
- f. **Non-discrimination** : les systèmes doivent être évalués au regard des intrants, des extrants et des effets disproportionnés discriminatoires.
- g. **Sécurité** : les systèmes à haut risque doivent satisfaire à des exigences appropriées de cybersécurité, d'essais et de résilience.
- h. **Contrôle humain et recours effectif** : les personnes concernées par des décisions d'IA à conséquences importantes doivent conserver un examen humain réel et un accès à un recours indépendant ou judiciaire.

Ces principes ne devraient pas demeurer de simples aspirations éthiques.

Pour les systèmes à haut risque, ils devraient se traduire en exigences d'approvisionnement, en études d'impact algorithmique, en obligations d'audit, en exigences de tenue de registres, en supervision indépendante et en recours exécutoires.

C'est cette transition - des principes vers les institutions - qui déterminera en définitive le succès ou l'échec du projet africain de gouvernance de l'IA.

LE RÔLE DE L'ASSOCIATION DU BARREAU AFRICAIN : BÂTISSEUR D'INSTITUTIONS

La profession juridique porte une responsabilité particulière dans cette transition. La gouvernance de l'IA ne saurait être laissée exclusivement aux ingénieurs, aux entreprises technologiques ou aux exécutifs gouvernementaux. Elle touche de plus en plus au droit constitutionnel, aux droits humains, à la sécurité nationale, aux marchés publics, à la réglementation bancaire, à la concurrence, à la contractualisation commerciale et à la déontologie professionnelle.

L'Association du barreau africain a donc l'occasion de dépasser le simple commentaire pour devenir un architecte institutionnel de la gouvernance africaine de l'IA. Trois rôles s'avèrent particulièrement importants.

1. Premièrement, le **plaidoyer et l'harmonisation**. L'Association du barreau africain peut promouvoir une mise en œuvre plus large des normes continentales de cybersécurité et de protection des données, tout en encourageant une convergence autour de principes minimaux de gouvernance de l'IA.
2. Deuxièmement, le **renforcement des capacités professionnelles**. Les avocats ne peuvent réglementer, plaider, effectuer des acquisitions ou conseiller avec compétence sur des systèmes qu'ils ne comprennent pas. La formation juridique continue en matière d'IA, de cybersécurité, de prise de décision automatisée, de preuve numérique et de redevabilité algorithmique devrait donc faire partie intégrante de la compétence professionnelle moderne.
3. Troisièmement, la **vigilance démocratique**. La souveraineté numérique ne doit jamais devenir une justification rhétorique d'une surveillance illimitée ou d'un pouvoir technologique exécutif sans contrôle.

Exiger des limites juridiques ne place pas la profession juridique en opposition à l'État. Cela remplit la responsabilité fondamentale de la profession, qui est de veiller à ce que le pouvoir étatique - y compris le pouvoir étatique augmenté par la technologie - demeure soumis au droit.

Les expériences du Cap-Vert, du Rwanda et de l'île Maurice montrent que la souveraineté numérique africaine ne doit pas nécessairement rester une aspiration abstraite : bien que leurs modèles diffèrent, chacun d'entre eux illustre l'importance de développer les capacités technologiques parallèlement à la résilience en matière de cybersécurité, aux institutions de régulation et à une gouvernance responsable.

Recommandations prioritaires

Six priorités se dégagent directement de cette analyse.

Premièrement, l'Association du barreau africain devrait mettre en place un Groupe de travail continental sur l'intelligence artificielle, la souveraineté numérique et l'État de droit, capable de coordonner la recherche, le plaidoyer et les propositions réglementaires.

Deuxièmement, l'AFBA devrait élaborer des Principes africains types sur l'IA et l'État de droit, intégrant la légalité, la nécessité, la proportionnalité, la transparence, la redevabilité, la non-discrimination, la cybersécurité, un contrôle humain réel et un recours effectif.

Troisièmement, les barreaux nationaux devraient créer des comités spécialisés en IA, en cybersécurité et en droit numérique, appuyés par une formation professionnelle continentale continue.

Quatrièmement, les États africains devraient exiger des études d'impact algorithmique ou relatives aux droits humains renforcées avant le déploiement de systèmes d'IA à haut risque dans les domaines de la défense, du maintien de l'ordre, de la gestion des frontières, des infrastructures critiques et des services publics essentiels.

Cinquièmement, l'Association du barreau africain devrait élaborer des clauses types d'approvisionnement et contractuelles régissant la localisation des données, les droits d'audit, la cybersécurité, l'interopérabilité, la réversibilité, le signalement des incidents, la dépendance envers les fournisseurs et le transfert de connaissances.

Sixièmement, les institutions africaines devraient plaider en faveur d'une capacité technologique et d'un financement panafricain, incluant la recherche partagée, l'infrastructure de calcul et l'expertise spécialisée, afin que la souveraineté numérique ne demeure pas l'apanage des seuls marchés technologiques les plus riches du continent.

Ces recommandations partagent un même objectif : transformer la souveraineté d'une rhétorique en une capacité institutionnelle.

CONCLUSION

L'intelligence artificielle n'a pas besoin de la permission de l'Afrique pour s'introduire dans les sociétés africaines. Elle est déjà présente dans le secteur bancaire, l'administration publique, la cybersécurité et, de plus en plus, dans la sécurité et la défense. La question pertinente n'est donc pas de savoir si l'Afrique participera à la révolution de l'IA. La question est de savoir selon quels termes.

Les institutions africaines se contenteront-elles de consommer des systèmes conçus ailleurs ? Les fonctions publiques essentielles deviendront-elles dépendantes de technologies que les gouvernements ne peuvent auditer de manière significative ? Les objectifs sécuritaires éroderont-ils progressivement les garanties constitutionnelles ? Ou l'Afrique

bâtira-t-elle une capacité juridique, technologique et institutionnelle suffisante pour gouverner l'intelligence artificielle selon ses propres priorités et l'État de droit ?

Le renseignement militaire, la cybersécurité, la prévision économique et la gouvernance réglementaire peuvent sembler être des sujets distincts, mais ils ne le sont pas. Ce sont différentes manifestations d'un même défi sous-jacent : la préservation d'une souveraineté réelle dans un monde de plus en plus algorithmique. Cette souveraineté ne peut être proclamée par des déclarations politiques ni acquise par le simple achat de technologies sophistiquées. Elle doit être construite par le droit, les infrastructures, les institutions, les compétences et la coopération continentale.

L'expérience de l'Afrique en matière de télécommunications mobiles et de paiements numériques démontre que le continent peut faire plus qu'adopter le changement technologique. Il peut innover face à ses contraintes structurelles et produire des solutions d'une portée mondiale. L'intelligence artificielle représente une opportunité de même nature. Mais les fondements juridiques doivent accompagner l'ambition technologique.

Nous devons en convenir : pas d'intelligence artificielle sans redevabilité. Pas de sécurité sans respect des droits. Pas de transformation numérique sans souveraineté réelle. Et pas de souveraineté numérique africaine durable sans coopération africaine.

La tâche de la profession juridique n'est donc pas de résister au progrès technologique. Elle est de veiller à ce que le pouvoir technologique demeure compatible avec la dignité humaine, la stabilité institutionnelle, la redevabilité démocratique et l'État de droit. L'Afrique n'a pas à choisir entre innovation et réglementation. Son choix le plus déterminant se situe entre une innovation encadrée et une dépendance non maîtrisée. Ce choix se présente à nous dès maintenant. Et c'est à nous de le faire !

Présenté par Maître Lylie Naomie Ngninkeu.

Sources institutionnelles

1. Union africaine, *Stratégie continentale sur l'intelligence artificielle*, 2024. (https://au.int/sites/default/files/documents/44004-doc-FR_Strategie_Continentale_sur_Intelligence_Artificielle_3.pdf)
2. Union africaine, *African Digital Compact*, juillet 2024. (https://au.int/sites/default/files/documents/44005-doc-EN_African_Digital_Compact_-_July_2024.pdf).
3. Conseil de paix et de sécurité de l'Union africaine, *Communiqué de la 1267e réunion sur l'intelligence artificielle et son impact sur la paix, la sécurité et la gouvernance en Afrique*, 20 mars 2025. (<https://www.peaceau.org/en/article/communique-of-the-1267th-meeting-of-the-peace-and-security-council-held-on-20-march-2025-on-artificial-intelligence-and-its-impact-on-peace-security-and-governance-in-africa>).
4. Conseil de paix et de sécurité de l'Union africaine, *Communiqué de la 1339e réunion sur l'intelligence artificielle : gouvernance, paix et sécurité*, 16 avril 2026. (<https://www.peaceau.org/fr/article/communique-de-la-1339e-reunion-du-cps-tenue-le-jeudi-16-avril-2026-sous-le-theme-intelligence-artificielle-gouvernance-paix-et-securite>)
5. Banque Centrale des États de l'Afrique de l'Ouest, *L'intelligence artificielle : opportunités et défis pour les banques centrales*, conférence internationale, Dakar, 21 mai 2025. (<https://www.bceao.int/sites/default/files/inline-files/Communiqu%C3%A9%20sur%20la%20conf%C3%A9rence%20sur%20l'IA%20%C3%A0%20poster%20sur%20internet.pdf>).
6. Banque Centrale des États de l'Afrique de l'Ouest, *Clôture de la Conférence sur l'intelligence artificielle : opportunités et défis pour les banques centrales*. (<https://www.bceao.int/index.php/fr/content/cloture-de-la-conference-sur-lintelligence-artificielle-les-gouverneurs-des-banques>)
7. Union africaine, *Convention sur la cybersécurité et la protection des données à caractère personnel*, Malabo, 27 juin 2014. ([https://au.int/sites/default/files/treaties/29560-sl-AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION.pdf](https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION%20(1).pdf))
8. Union africaine, *List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection*. ([https://au.int/sites/default/files/AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION%20\(1\).pdf](https://au.int/sites/default/files/AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION%20(1).pdf))
9. Commission africaine des droits de l'homme et des peuples, *Résolution 473 sur les droits de l'homme et l'intelligence artificielle en Afrique*, 2021. (<https://achpr.au.int/fr/adopted-resolutions/473-resolution-sur-la-necessite-delaborer-une-etude-sur-les-droits-de-lhomme-et>)
10. Commission africaine des droits de l'homme et des peuples, *Draft Study on Human and Peoples' Rights and Artificial Intelligence, Robotics and Other New and Emerging Technologies in Africa*, 2025. (<https://achpr.au.int/sites/default/files/files/2025-04/draft-achpr-ai-study-march-2025.pdf>)
11. Gouvernement de Cabo Verde, *Estratégia Nacional para a Cibersegurança*, 2016. (<https://www.governo.cv/conselho-de-ministros-aprova-estrategia-nacional-para-a-ciberseguranca/>)
12. Gouvernement de Cabo Verde, *Estratégia para a Governação Digital de Cabo Verde*. (<https://www.governo.cv/documentos/boletim-oficial-14-de-dezembro-de-2021/>)
13. Gouvernement de Cabo Verde, *Plano de Ação da Estratégia para a Governação Digital de Cabo Verde*, 2023. (<https://www.governo.cv/publicado-plano-de-acao-da-estrategia-para-a-governacao-digital-de-cabo-verde/>)
14. *Politique nationale d'intelligence artificielle du Rwanda — Ministry of ICT and Innovation* - Source principale pour la politique nationale d'IA adoptée en 2023, notamment ses six domaines prioritaires et quatorze recommandations.
15. *Répertoire officiel des politiques du ministère rwandais des TIC* - Permet notamment d'accéder à la politique nationale d'IA et aux autres instruments stratégiques du Rwanda.
16. *AI Readiness and Maturity Framework for Rwanda — document officiel PDF* - Important pour évaluer le niveau réel de maturité et de préparation du Rwanda en matière d'IA, et pas uniquement ses ambitions politiques.
17. *Autorité rwandaise de protection des données et de la vie privée — cadre institutionnel* — Présente le cadre institutionnel établi autour de la Loi n° 058/2021 relative à la protection des données personnelles et de la vie privée.

18. [Loi n° 058/2021 relative à la protection des données personnelles et de la vie privée — texte officiel PDF](#)
19. [Texte consultable de la législation rwandaise sur la protection des données](#)
20. [World Economic Forum — Centre for the Fourth Industrial Revolution Network Impact Report 2023–2024](#) — Source particulièrement intéressante concernant le projet utilisant GPT-4 et un modèle de traduction anglais–kinyarwanda pour soutenir les agents de santé communautaires. Le rapport fait état d'une amélioration évaluée de **8 % à 71 %**.
21. [World Economic Forum — présentation de l'utilisation de l'IA dans le secteur de la santé au Rwanda](#) - Ressource complémentaire et plus accessible sur cette initiative.
22. [Artificial Intelligence Unit de Maurice — portail officiel](#)
23. [National AI Strategy — Gouvernement de Maurice](#) - Source officielle relative à la stratégie nationale actuelle en matière d'intelligence artificielle.
24. [Lancement de la National AI Strategy et des FAIR Guidelines — avril 2026](#) - Source gouvernementale confirmant le lancement officiel de la nouvelle stratégie et des lignes directrices FAIR.
25. [Digital Transformation Blueprint 2025–2029 — Gouvernement de Maurice](#) - Le Blueprint repose sur quatre piliers stratégiques et cinq facilitateurs nationaux, notamment la réforme juridique et réglementaire, la cybersécurité et la confiance, ainsi que la gouvernance des données et de l'IA.
26. [Mauritius Artificial Intelligence Strategy 2018 — document officiel](#)
27. [Public–Private–People Partnership pour l'élaboration de la stratégie d'IA](#) - Montre l'implication du gouvernement, du secteur privé, du monde universitaire et de la société civile.
28. [Bulletin du ministère mauricien des TIC — groupes de travail sur la stratégie d'IA](#) - Source pour les 14 séances de consultation recensées en octobre 2025, comprenant deux réunions centrales et douze séances de travail spécialisées.
29. [Banque mondiale — Digital Transformation in Cabo Verde, ressource vidéo](#) - Ressource complémentaire sur l'ambition du pays de devenir un pôle numérique en Afrique de l'Ouest.
30. [Banque mondiale — documentation officielle du projet Digital Cabo Verde](#)
31. [NOSi et Université du Cabo Verde — développement de solutions fondées sur l'IA](#) - Source de juillet 2025 confirmant la coopération destinée à développer des solutions d'IA pour la gouvernance numérique, notamment dans le domaine de l'interopérabilité.
32. [NOSi — intelligence artificielle et marchés publics au Cabo Verde, mai 2026](#)