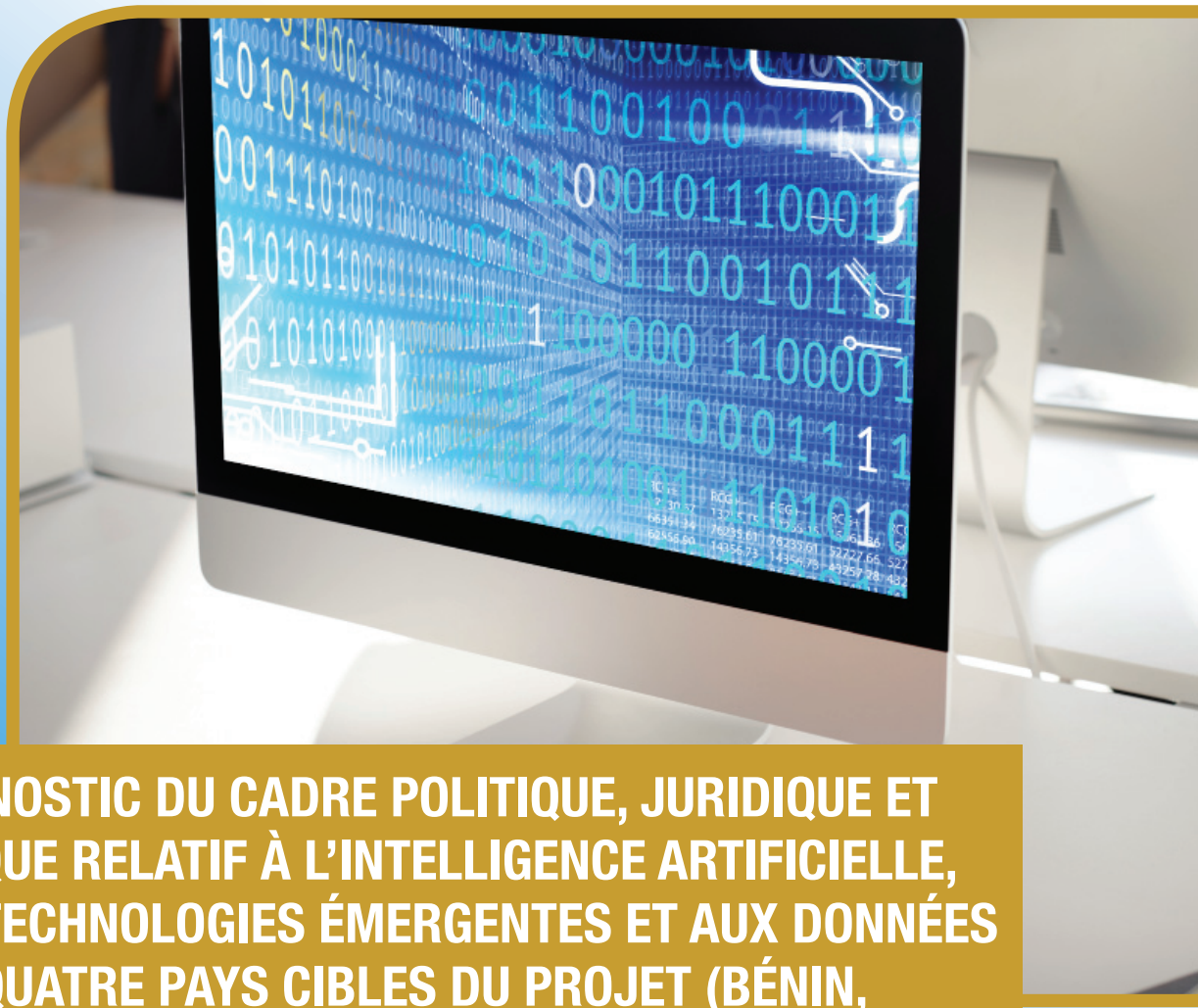
PROJET DUA

Développement et utilisation des systèmes d'intelligence artificielle pour le bien-être de tous en Afrique de l'Ouest (Bénin, Burkina Faso, Côte d'Ivoire et Sénégal)



DIAGNOSTIC DU CADRE POLITIQUE, JURIDIQUE ET ÉTHIQUE RELATIF À L'INTELLIGENCE ARTIFICIELLE, AUX TECHNOLOGIES ÉMERGENTES ET AUX DONNÉES DES QUATRE PAYS CIBLES DU PROJET (BÉNIN, BURKINA FASO, CÔTE D'IVOIRE ET SÉNÉGAL)

RAPPORT DE DIAGNOSTIC

Rédigé par :

Fatou FOFANA, Juriste

Mamadou NIANG, Statisticien

Cheikh FAYE, ingénieur statisticien, coordonnateur du projet

Laure TALL, Agroécologue, Directrice de recherche de l'IPAR

Juillet 2024

RÉSUMÉ

Le rapport «Diagnostic du cadre politique juridique et éthique relatif à l'intelligence artificielle, aux technologies émergentes et aux données dans quatre pays cibles du projet (Bénin, Burkina Faso, Côte d'Ivoire, et Sénégal)» présente une analyse détaillée des politiques, cadres juridiques et éthiques relatifs à l'intelligence artificielle (IA) et aux technologies émergentes dans ces pays africains. Il évalue les stratégies nationales existantes, identifie les forces, faiblesses, opportunités et menaces (SWOT) pour chaque pays, et propose des recommandations stratégiques pour améliorer l'intégration et l'utilisation de l'IA et des technologies connexes dans ces contextes.

Le rapport commence par définir l'état actuel des politiques nationales en IA et technologies émergentes, soulignant les initiatives gouvernementales, les collaborations internationales, et les projets de développement en cours. Il examine ensuite le cadre juridique et réglementaire, évaluant la législation en place pour l'IA et les technologies émergentes, ainsi que les défis liés à la mise en œuvre efficace des lois existantes.

Une attention particulière est accordée aux questions éthiques liées à l'IA, mettant en lumière les préoccupations en matière de confidentialité, de sécurité, de droits de l'homme et de propriété intellectuelle. Le rapport explore les aspects institutionnels, tels que les infrastructures, les ressources humaines et les capacités de recherche et de développement dans ces pays.

Enfin, le rapport conclut avec des recommandations générales visant à renforcer le cadre politique, juridique et éthique de l'IA et des technologies émergentes dans les pays étudiés. Ces recommandations incluent l'amélioration des politiques nationales, le renforcement des cadres juridiques et réglementaires, la promotion de l'éthique dans le développement et l'application de l'IA, et le soutien au développement de capacités institutionnelles et humaines.

TABLE DES MATIÈRES

LISTE DES SIGLES ET ABREVIATIONS

AIDA	Commission spéciale sur l'intelligence artificielle à l'ère du numérique
ANSSI	Agence nationale de la Sécurité des Systèmes d'information
APDP	Autorité de Protection des données à caractère personnel
ARTCI	Autorité de Régulation des Télécommunications de Côte d'Ivoire
CDP	Commission des données personnelles
CEA	Commission économique pour l'Afrique
CEDEAO	Communauté Economique des Etats de l'Afrique de l'Ouest
CIL	Commission Informatiques et Libertés
CNCDH	Commission nationale consultative des droits de l'homme
CNDP	Commission nationale de contrôle de la protection des Données à caractère personnel
CNIL	Commission nationale de l'Informatique et des Libertés
COMEST	Commission mondiale d'éthique des connaissances scientifiques et des technologies
DPO	Délégué à la protection des données
IA	Intelligence artificielle
IoT	Internet of things (internet des objets)
LOSI	Loi d'orientation sur la Société de l'Information
MOCC	Massive open online Course
OAPI	Organisation Africaine de la propriété intellectuelle
OCDE	Organisation de Coopération et de Développement économiques
ODD	Objectifs de développement durable
SNCS	Stratégie nationale de Cybersécurité
SAAD	Systèmes algorithmique d'Aide à la Décision
SIA	Système d'intelligence artificielle
TIC	Technologies de l'Information et de la Communication
UA	Union Africaine
UE	Union européenne
UNESCO	Organisation des Nations Unis pour l'Education, la Science et la Culture

INTRODUCTION

1. Contexte et Justification

Le continent africain enregistre des signes encourageants en matière d'innovation et de développement dans le domaine de l'intelligence artificielle (IA) et des technologies émergentes. Ce développement de l'IA en Afrique est matérialisé par la mise en place de formations relatives à l'IA dans les Universités publiques que privées (master en IA à l'Université Virtuelle du Sénégal,), la création de pôles d'innovations technologiques (Datacenter de Diamniadio au Sénégal, Supercalculateur...). C'est ce qui a permis l'utilisation de l'IA et des technologies émergentes dans plusieurs secteurs de la vie économique comme dans le secteur de l'industrie, de la santé, de l'agriculture, de l'enseignement, du commerce et du transport. Toutefois, ce développement de l'IA et des technologies émergentes est accompagné souvent d'un certain nombre de problèmes liés notamment à la violation des droits humains et à la dégradation de l'environnement.

Ainsi, pour parer aux effets négatifs de l'utilisation de l'IA et des technologies émergentes dans le monde, certains pays ont mis en place un cadre politique, juridique et institutionnel encadrant leur utilisation. Les pays africains notamment ceux au sud du Sahara semblent moins outillés pour faire face au développement et l'utilisation de l'IA et des technologies émergentes, malgré l'existence d'instruments juridiques, politiques et institutionnels encadrant le développement fulgurant des nouvelles technologies. C'est ce qui justifie une étude sur le cadre politique, juridique et institutionnel de l'intelligence artificielle afin de mesurer le niveau de prise en compte de son développement par les autorités publiques dans les quatre (4) pays d'Afrique de l'Ouest francophone : Bénin, Burkina Faso, Côte d'Ivoire et le Sénégal. Ainsi dans le cadre de cette étude, il s'avère nécessaire d'analyser et d'évaluer le dispositif politique, juridique, éthique et institutionnel en vigueur dans les quatre pays cibles ayant trait à l'usage de l'intelligence artificielle et des technologies émergentes.

2. Méthodologie

Ce travail de diagnostic se base sur la cartographie des textes politiques et juridiques de l'intelligence artificielle, des données et technologies émergentes dans les quatre pays cibles et la revue documentaire. L'application de la méthode d'analyse FFOM (forces, faiblesses, opportunités, menaces) ou SWOT (en anglais) à ces textes cartographiés a permis d'identifier où en sont ces 4 pays dans la prise en compte de l'IA dans leur environnement politique et juridique.

Pour rappel, les « outputs » du travail de cartographie sont :

i. une présentation de tous les textes politiques et juridiques pertinents pour l'IA dans les 4 pays cible, de leurs objectifs et des articles spécifiques traitant de l'intelligence artificielle, des données et technologies émergentes ;

ii. un recueil des textes juridiques compilant l'intégralité de tous les instruments légaux et règlementaires applicables à l'IA dans ces 4 pays ; et

iii. une présentation des principaux acteurs du cadre juridique de l'IA, des données et technologies émergentes dans chaque pays

La revue documentaire donne des informations exhaustives sur le cadre politique, juridique et éthique de l'intelligence artificielle, des technologies émergentes et des données au niveau international, régional et national.

3. Résultats attendus

- L'Analyse et l'évaluation des instruments politiques et stratégies de chaque pays cible afin d'identifier leurs forces notamment dans la prise en compte de l'IA et des technologies émergentes ;
- L'analyse et l'évaluation du cadre juridique des quatre pays cible relatif au numérique, aux technologies émergentes et à l'IA en vue de déterminer s'il offre un encadrement adéquat permettant de bénéficier les avantages de l'IA et de minimiser ses impacts négatifs particulièrement sur les droits humains, la protection des données, la cybersécurité, propriété intellectuelle ;

- La mise en exergue des principes éthiques édictés par les pays cibles permettant une utilisation de l'IA et des technologies émergentes conforme à la morale et l'éthique ;
- L'identification des limites du cadre politique, juridique et éthique des pays cibles sur les aspects de l'IA et des technologies émergentes en déterminant de manière non limitative :
  - les freins du cadre politique, juridique et éthique de chaque pays cible dans la prise en compte de l'IA et des technologies émergentes ;
  - les faiblesses du dispositif politique, juridique et éthique pour qu'une IA digne de confiance puisse prendre son envol dans les pays cibles du projet ;
- L'identification des potentielles menaces pouvant affecter le dispositif politique, juridique et éthique des pays cibles sur les aspects de l'IA et des technologies émergentes ;
- Une proposition des pistes d'amélioration du dispositif politique, juridique et éthique dans une démarche de benchmark afin de contribuer pour les pays cibles :
  - disposer d'un meilleur encadrement politique, juridique et éthique prenant suffisamment en compte les enjeux de l'IA et des technologies émergentes ;
  - instaurer un cadre favorable à l'émergence des systèmes IA sûrs pour le bien-être des populations des pays cibles ;
  - renforcer le dispositif de protection des droits humains et des données notamment à caractère personnel ;

Toutefois, au préalable, il est nécessaire de déconstruire et de démystifier cette notion de l'Intelligence artificielle (IA) qui fait l'objet de beaucoup de supputations, et de fantasmes.

4. Définition de la notion d'IA

L'expression IA a été utilisée pour la première fois en 1956 par John McCarthy, informaticien lors de la conférence à Darmouth college[1]. L'objectif était de concevoir les mécanismes de fonctionnement du cerveau humain à l'intérieur d'un ordinateur[2]. L'IA est désormais la première innovation citée parmi les technologies émergentes.

Mais, que recouvre vraiment cette notion ? Il faut dire qu'il n'existe pas de définition universelle de la notion d'intelligence artificielle. Les différentes définitions proposées renvoient à des domaines disciplinaires comme l'informatique, la robotique ou à l'aspect fonctionnel c'est-à-dire aux multiples usages de l'IA.

Plusieurs définitions émanant notamment des organisations internationales telles que l'UNESCO, l'OCDE, le Parlement européen, ont émergé depuis quelques années.

Ainsi, l'UNESCO, considère les systèmes de l'IA comme « *des systèmes capables de traiter les données et l'information par un processus s'apparentant à un comportement intelligent et comportant généralement des fonctions de raisonnement, d'apprentissage, de perception, d'anticipation, de planification ou de contrôle*[3]».

L'OCDE définit l'IA « *un système automatisé qui, pour des objectifs explicites ou implicites, déduit, à partir d'entrées reçues, comment générer des résultats en sortie tels que des prévisions, des contenus, des recommandations ou des décisions qui peuvent influer sur des environnements physiques ou virtuels. Différents systèmes d'IA présentent des degrés variables d'autonomie et d'adaptabilité après déploiement* »[4].

Toujours, dans cette perspective de tentative de définition de cette notion, le Parlement européen, à travers la commission spéciale AIDA[5], considère que le terme IA est un terme générique qui renferme diverses

1 DUGUET Julien, CHASSANG Gauthier, BERANGER Jérôme, « Enjeux, répercussions et cadre éthique relatifs à l'Intelligence Artificielle en santé. Vers une Intelligence Artificielle éthique en médecine », Droit, Santé et Société, 2019/3 (N° 3), p. 30-39. DOI : 10.3917/dsso.064.0030. URL : https://www.cairn.info/revue-droit-sante-et-societe-2019-3-page-30.htm

2 AZOULAY Warren, « Des machines et des hommes. La guerre n'aura pas lieu », Droit et société, 2019/3 (N° 103), p. 595-607. DOI : 10.3917/drs1.103.0595. URL : https://www.cairn.info/revue-droit-et-societe-2019-3-page-595.htm

3 Recommandations de l'UNESCO sur l'éthique de l'intelligence artificielle, Recommandation sur l'éthique de l'intelligence artificielle | UNESCO

4 Recommandation du Conseil sur l'Intelligence artificielle, OECD Legal Instruments

5 Commission spéciale sur l'intelligence artificielle à l'ère du numérique (AIDA)

technologies et techniques. Ces technologies et techniques désignent « *tous les systèmes fondés sur des machines qui n'ont pas souvent guère plus en commun que d'être guidés par un ensemble donné d'objectifs définis par l'homme, avec des degrés d'autonomie variables dans leurs actions et de s'engager dans des prédictions, des recommandations ou de prise de décision fondées sur les données disponibles* »[6] C'est d'ailleurs pourquoi elle préconise l'usage de l'expression générique de « *systèmes d'intelligence artificielle* » à la place du vocable intelligence artificielle.

Dans le même sillage, le Parlement européen définit l'IA dans le Règlement européen comme suit : « *un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuel* [7]»

La définition de l'IA posée par le Parlement européen est quasi similaire à celle donnée par l'OCDE. Ces définitions nous renseignent que les systèmes de l'IA sont des structures capables de fonctionner de façon autonome et pouvant donner, sur la base d'instructions, des prévisions, un contenu, des recommandations comme l'aurait pu le faire un humain.

Une autre question surgit : Quel est le rapport entre le système de l'IA et les algorithmes ? En d'autres termes, existe-t-il une différence entre les algorithmes et l'IA ?

L'algorithme est défini comme « *une suite finie et non ambiguë d'instructions et d'opérations permettant de résoudre une classe de problème* »[8]. Sur la base des définitions de l'intelligence artificielle évoquées supra, il est possible de conclure que le système d'intelligence artificielle est un algorithme *« plus ou moins évolué qui imite des actions humaines* »[9] notamment à travers la technique de l'apprentissage plus communément appelé machine learning dans laquelle l'homme exerce le système en lui donnant des données lui permettant d'apprendre et d'effectuer de façon autonome les opérations ou tâche en question[10]. En d'autres termes, la méthode d'apprentissage est la stimulation des ordinateurs grâce à des données fournies par l'homme. Le Deep learning appelé apprentissage approfondi reprend le fonctionnement du cerveau humain grâce à ses capacités cognitives.

Ainsi, considérant que les systèmes d'IA sont majoritairement fondés sur des algorithmes, la Commission Nationale Consultative des Droits de l'Homme française (**CNCDH**) a recommandé l'usage du vocable de « ***systèmes algorithmiques d'aide à la décision (*SAAD**)** »[11] , plus neutre et objective, en lieu et place de l'expression « intelligence artificielle » qui peut être source de confusion ou de polémiques. Cette recommandation nous semble appropriée considérant les effets, mythes et autres considérations subjectives que soulèvent la notion de l'IA.

5. Quelques cas d'usages des SIA

Comme précédemment évoqué, il est noté un développement fulgurant des systèmes d'intelligence artificielle qui occupent de plus en plus notre quotidien. Comme illustration banale de la prégnance des systèmes de l'IA sur notre vie, la fonction Spam dans les boites mail qui redirige automatiquement de manière intuitive les messages considérés comme indésirés, sans doute l'une des applications de l'IA les plus courante et simple, peut être citée.

L'usage de l'IA est également retrouvé, dans le cadre des robots conventionnels ainsi que des assistants vocaux utilisés couramment comme le SIRI d'Apple, l'Alexa d'Amazon, le Bixby de Samsung ou encore le Cortana de Microsoft.

6 Rapport sur l'intelligence artificielle à l'ère du numérique, commission AIDA, https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_FR.html

7 Règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'IA, pdf (europa.eu)

8 https://fr.wikipedia.org/wiki/Algorithme

9 https://penseeartificielle.fr/difference-intelligence-artificielle-machine-learning-deep-learning

10 CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique par la loi pour une république numérique, décembre 2017, https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

11 CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, , 7 avril 2022, https://www.cncdh.fr/sites/default/files/2022-04/A%20-%202022%20-%206%20%20-%20Intelligence%20artificielle%20et%20droits%20fondamentaux%2C%20avril%202022.pdf

Dans le cadre des réseaux sociaux, les systèmes de l'IA sont utilisés de manière récurrente c'est le cas notamment que Tik tok, qui en se basant sur les données collectées sur l'utilisateur lui offre des contenus personnalisés afin d'augmenter son temps d'utilisation de l'application. Il en est de même des sites d'achat en ligne qui par l'usage des systèmes d'IA orientent le comportement des utilisateurs afin de capter leur attention et de les pousser à acheter un produit.

Au-delà du domaine technologique, les systèmes de l'IA s'appliquent également dans le domaine de la santé, de l'éducation, de l'agriculture etc.

IA et santé

Les systèmes de l'IA ont joué un rôle fondamental dans la lutte contre la pandémie COVID 19. Son usage a été noté notamment dans le séquençage du génome et la mise en place de diagnostic rapide. Ils ont également contribué dans la recherche de traitement pour concevoir des vaccins et le partage des connaissances scientifiques. Durant la pandémie, les systèmes de l'IA ont été également utilisés aux fins de prédiction de l'évolution de la pandémie et de contrôle de la population comme en Singapour. Ceci dénote les potentialités de l'IA dans le domaine de la santé. A titre illustratif des applications de l'IA dans le domaine de la santé, au Sénégal, la start-up XAIL[12] , a conçu un système IA permettant une détection précoce du cancer du cerveau à base d'images radiographiques et a même reçu un premier financement de Villgro AFrica.[13]. La startup kényane Ilara Health utilise l'IA pour améliorer la précision des diagnostics de maladies telles que la tuberculose et le paludisme.

Toutefois, même si les systèmes d'IA peuvent constituer un atout dans le domaine de la santé, son usage est susceptible de soulever des questions juridiques. En effet, le diagnostic des maladies qui doit relever de la prérogative exclusive du médecin ne doit pas être délégué à une machine aussi performante soit elle. Les systèmes d'IA ne pouvant servir qu'à l'aide à la prise de décision et non de devenir le décideur effectif. Or, en utilisant les systèmes de l'IA en matière de diagnostic, il serait difficile par exemple d'apprécier l'autonomie du médecin vis à vis de résultats du système censé donner de résultats plus fiables. Dans ce cas d'espèce, le système d'IA sont susceptibles de prendre la place et le rôle du médecin au lieu de lui apporter un support[14].

IA et éducation

Les systèmes d'IA peuvent permettre de relever de nombreux défis dans le domaine de l'éducation et même de la révolutionner en aidant au développement de pratiques d'enseignement et d'apprentissages innovantes dans le cadre de la réalisation de l'objectif de développement durable 4 (ODD 4)[15] et conformément au consensus de Beijing sur l'intelligence artificielle et l'éducation adopté en 2019 [16].

En effet, il est noté depuis quelques années l'apparition des MOCC (Massive Open Online Cours), des cours d'enseignement diffusés via internet permettant ainsi de démocratiser et de rendre plus accessible la connaissance.

Au niveau africain, il existe des initiatives sur l'utilisation de l'IA dans le domaine de l'éducation. C'est le cas, l'application Djehuty, développée au Sénégal, un système de tutorat intelligent (ITS) ludique utilisant l'IA pour permettre aux enfants d'apprendre l'écriture manuscrite à l'aide d'une application mobile. Ce système a d'ailleurs été sélectionné en 2021 comme faisant partie des 100 projets mondiaux résolvant des défis liés aux objectifs de développement durable des Nations unies grâce à l'application de l'IA[17]

Le gouvernement rwandais s'est associé à l'Institut africain des sciences mathématiques (AIMS) pour développer une plateforme «TeachLab» qui utilise l'IA pour fournir un soutien personnalisé aux enseignants et aux étudiants[18]. L'IA va donc contribuer à ajouter une dimension très importante à l'éducation via la personnalisation.

12 Stratégie nationale sur l'Intelligence artificielle, Sénégal
13 Stratégie nationale, op citée
14 CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique par la loi pour une république numérique, décembre 2017, https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_rapport_garder_la_main_web.pdf
15 https://fr.unesco.org/themes/tic-education/intelligence-artificielle
16 https://unesdoc.unesco.org/ark:/48223/pf0000368303
17 Stratégie nationale op citée
18 Stratégie nationale op citée.

L'IA permet en effet d'analyser les résultats de chaque élève et d'identifier les domaines dans lesquels des améliorations peuvent être apportées.

Autre exemple, Educore, une entreprise zambienne de technologie éducative (Edtech), utilise l'IA pour analyser les données des élèves et fournir aux enseignants des informations sur leurs progrès.

IA et Agriculture

Face aux enjeux de l'agriculture auxquels doivent faire face le monde notamment le continent africain pour nourrir sa population, les systèmes d'IA peuvent constituer une grande opportunité pour accroitre la production agricole. Actuellement, le monde est résolument tourné vers le e- agriculture19 et l'Afrique n'est pas en reste. L'usage des systèmes d'IA est remarqué dans la gestion des sols, des intrants, des maladies et ravageurs, la maitrise du changement climatique, le financement. Grace à ces multiples usages dans le domaine agricole, les systèmes d'IA à travers l'agriculture de précision, donnent à l'agriculteur les informations lui permettant de faire les choix idoines en matière de semis, de récolte, d'intrants. L'usage des drones dans le domaine agricole est fortement également remarqué. Ces drones qui fonctionnent grâce aux systèmes d'IA, permettent ainsi de réaliser entre autres, une cartographie et une analyse précise des sols participant à l'accroissement des rendements agricoles. Comme on le constate, les systèmes de l'IA pourraient s'avérer utiles pour le développement agricole en jouant un rôle d'assistance à l'agriculteur afin de lui permettre de se concentrer davantage sur les taches nécessitant impérativement l'intervention humaine.

A titre d'exemple, on peut notamment citer TOLBI, une startup de technologie agricole (AgriTech) basée au Sénégal qui développe des solutions innovantes basées sur l'IA et les images satellitaires, permettant de traduire les intrants sur le terrain en informations exploitables pour une agriculture intelligente face au climat. On peut d'ailleurs observer que l'écosystème numérique sénégalais est très impliqué sur le secteur de l'agriculture, sous l'impulsion notamment du Yeesal Agri Hub, un groupement qui a présenté un projet en collaboration avec l'Université Cheikh Anta Diop (UCAD) visant à développer l'utilisation de la science des données dans l'agriculture, en s'appuyant sur les données géospatiales.[20] D'autres initiatives sont également notées dans le continent comme au Cameroun avec AgrixTech, qui utilise des modèles d'apprentissage automatique pour analyser les données agricoles et fournir des recommandations personnalisées aux agriculteurs, ou encore l'alliance Connected Farmer, un partenariat public privé en Afrique de l'Est qui propose une plateforme mobile basée sur l'IA qui permet aux agriculteurs de bénéficier d'informations en temps réel sur les cultures, les sols et les conditions météorologiques à partir de données de drones et des satellites. Au Kenya, l'entreprise, Apollo Agriculture propose des solutions de financement et de conseil agricole en utilisant l'IA pour évaluer les risques, prédire les rendements et offrir des recommandations personnalisées aux petits exploitants agricoles.[21].

6. Les risques potentiels de l'IA sur les droits fondamentaux

En dépit des applications très utiles des systèmes d'IA dans de nombreux domaines, ils peuvent malheureusement avoir de fortes répercussions sur les droits fondamentaux notamment le respect de la vie privée, la justice, la protection des données, l'égalité, la non-discrimination.

Dans le domaine du respect de la vie privée, certains usages de l'IA peuvent avoir des conséquences importantes. A titre d'exemple, on peut citer le système de la notation sociale (Scoring social)[22] consistant à évaluer les personnes en fonction de leur comportement social, personnalité ou caractéristiques personnelles. Un autre usage très contesté des systèmes de l'IA entravant la vie privée, l'identification biométrique à distance à des fins répressives, c'est-à-dire la reconnaissance automatisée d'attributs humains comme le visage, la voix et la démarche dans les espaces accessibles au public.

En matière de justice, les systèmes de l'IA sont utilisés dans certains pays comme les Etats unis pour prédire les éventuelles infractions, fixer une peine et apprécier les risques de récidive. Or, avec l'usage de l'IA, il n'est

19 L'Intelligence Artificielle, une opportunité pour l'agriculture au Togo, Kondi Napo SONHAYE, journals open éditions, https://doi.org/10.4000/ctd.7219

20 Stratégie nationale op citée

21 Stratégie nationale op citée

22 CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, , 7 avril 2022, https://www.cncdh.fr/sites/default/files/2022-04/A%20-%202022%20-%206%20%20-%20Intelligence%20artificielle%20et%20droits%20fondamentaux%2C%20avril%202022.pdf page 10

pas possible notamment pour les acteurs du pouvoir judicaire tels que le juge, l'avocat de comprendre par quel cheminement a abouti le système rendant ainsi difficile les possibilités de motivation et de contestation et remettant en cause l'impartialité du juge. L'usage des systèmes de l'IA dans le domaine judiciaire entraine ainsi comme conséquence une probable atteinte du droit à la liberté, à la sécurité et au droit à un procès équitable. Les systèmes de l'IA doivent être utilisés pour aider les acteurs de la justice et non se subroger à eux. Il en est ainsi par exemple de l'application permettant de vieillir les personnes disparues accroissant les chances de les retrouver[23]. Le pouvoir notamment de fixer les peines doivent relever exclusivement du ressort de l'Homme qui dispose de capacités que n'auront surement pas une machine malgré toute sa sophistication.

Par ailleurs, les systèmes de l'IA sont susceptibles de reproduire des biais et d'accentuer ou de créer les discriminations. On retrouve de nombreux exemples de logiciels qui ont été indexés comme générant des discriminations. Même si, il faut le reconnaitre, un algorithme n'est pas totalement objectif, il n'est que le reflet des choix et des données fournies par son programmateur. Par exemple, en 2015, un logiciel de reconnaissance faciale de Google a classé une photo de couple de noirs américains dans la catégorie de gorille.[24] Toujours avec Google, une étude avait démontré que sa plateforme publicitaire créait des discriminations au détriment des femmes qui se voyaient proposer des offres moins bien rémunérées que celles proposées aux hommes[25]. Au-delà de la discrimination individuelle, les systèmes de l'IA peuvent générer des discriminations collectives, c'est ce qui est passé avec l'entreprise Amazon, qui en se basant sur un algorithme discriminant certaines zones du fait du peu de profit qu'il générait pour l'entreprise, avait exclu ces zones de service de livraison gratuite. Or, ces zones sont majoritairement habitées par des populations défavorisées[26].

De plus, les systèmes de l'IA peuvent constituer une entrave à la liberté de choix et à l'autonomie de l'être humain. C'est le cas des effets bulle filtrante, des algorithmes qui proposent aux utilisateurs du contenu toujours conforme à leur comportement numérique (c'est-à-dire leurs précédents choix), limitant ainsi la diversité du contenu qui leur est proposé ou les chances de découvrir de nouvelles préférences[27]. L'IA pourrait également constituée une entrave à la démocratie à l'image de la création des « chambres à écho » sur le web, ne proposant à un individu que du contenu qui lui est agréable, au lieu de forcer la personne à confronter ses idées avec d'autres points de vue contraires[28].L'utilisation IA est également observée dans la création des deepfakes avec comme conséquence une polarisation de l'espace public et des répercussions politiques importantes. Par ailleurs, l'IA pourrait porter atteinte à la liberté de manifestation dans la mesure où son usage pourrait permettre de localiser ou de profiler les personnes[29].

Compte tenu, de ces nombreuses incidences sur les droits fondamentaux, des recommandations ont été formulées par l'UNESCO, le 24 novembre 2021 visant à « *mettre les systèmes d'IA au service de l'humanité, des individus, des sociétés, de l'environnement et des écosystèmes ainsi que prévenir des préjudices* »[30]. Des recommandations similaires ont été formulées par l'OCDE dans la version mise à jour de sa Recommandation du conseil sur l'IA allant dans le sens « *promouvoir une approche d'une IA digne de confiance qui soit centrée sur l'humain, favorise la recherche, préserve les incitations économiques en faveur de l'innovation et vaille pour l'ensemble des parties prenantes* [31]». Toutefois, en dépit de ces recommandations, il s'avère nécessaire de de songer à la mise en place d'un cadre juridique plus contraignant, plus respectueux des droits fondamentaux. C'est d'ailleurs l'objet du Règlement Européen établissant des règles harmonisées concernant l'intelligence artificielle. Par ailleurs, il a été recommandé également d'adopter au niveau du conseil de l'Europe, à l'instar de la Convention 108[32] sur la protection des données à caractère personnel, un texte similaire applicable en matière d'IA[33]. Au niveau africain, l'Union africaine a adopté une résolution visant

23 CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique par la loi pour une république numérique, décembre 2017, https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_rapport_garder_la_main_web.pdf, page 26

24 Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, CNCDH, 2022, op cité

25 Comment permettre à l'homme de garder la main, rapport CNIL, 2017

26 op cité

27 CNIL op cité, page 36

28 Intelligence artificielle : opportunités et risques | Thèmes | Parlement européen (europa.eu)

29 Op citée

30 UNESCO, Recommandation sur l'éthique de l'intelligence artificielle, 2021, SHS/BIO/REC-AIETHICS/2021, https://unesdoc.unesco.org/ark:/48223/pf0000380455_fre

31 Recommandation du Conseil de l'OCDE sur l'intelligence artificielle, 2019,https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449 référence texte 2024 OCDE, Recommandation du Conseil sur l'intelligence artificielle, OECD/LEGAL/0449, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449

32 Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (STE n°108), version révisée 2018, https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726

33 CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, , 7 avril 2022, https://www.cncdh.fr/sites/default/files/2022-04/A%20-%202022%20-%206%20%20-%20Intelligence%20artificielle%20et%20droits%20fondamentaux%2C%20avril%202022.pdf

à l'élaboration d'une étude afin d'affiner des lignes directrices et des normes sur les questions relatives aux technologies de l'intelligence artificielle, la robotique et d'autres technologies nouvelles et émergentes et leur impact sur les droits de l'homme en Afrique. On suppose qu'après cette étude, l'UA adoptera certainement des recommandations sur l'IA et le respect de droits de l'homme. Ce ne sera pas suffisant, il faudrait l'UA prenne le leadership en adoption un instrument juridique plus contraignant à l'instar de la convention de l'Union africaine sur la Cybersécurité et la protection des données à caractère personnel afin de pousser les Etats membres de l'UA à disposer d'un cadre juridique pour la gouvernance de l'IA qui est d'ailleurs l'un des besoins identifiés par l'UNESCO[34].

II. ANALYSE DES POLITIQUES ET STRATEGIES NATIONALES LIEES A L'IA , LES DONNEES ET LES TECHNOLOGIES EMERGENTES DES QUATRE PAYS CIBLES

A. La cybersécurité au centre des stratégies nationales

Le développement fulgurant du numérique s'est accompagné de menaces et de risques sur les réseaux, les systèmes informatiques et données informatiques susceptibles de porter atteinte aux intérêts tant publics que privés. Ces menaces et risques réduisent fortement ainsi les impacts positifs du numérique sur l'économie et la société. Avec l'apparition de l'Internet des objets, émetteur de quantité importante de données, ces attaques de cybercriminalité se sont accentuées.

Par ailleurs, l'émergence des SIA soulève un enjeu de cybersécurité du fait des fragilités spécifiques inhérentes aux SIA telles que vol de données et l'empoisonnement des données d'apprentissage. Même si, d'un autre côté, les SIA peuvent contribuer à explorer et solutionner ces menaces en la matière.

Conscients de ces enjeux de cybersécurité, presque tous les pays cibles ont élaboré des stratégies nationales de cybersécurité pour circonscrire les risques et lutter efficacement contre la cybercriminalité.

Au niveau du continent africain, **la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel** adopté le 27 juin 2014, donne obligation aux Etats parties d'adopter des stratégies qu'ils jugent pertinents, appropriés et suffisants pour mettre en œuvre une politique nationale de cybersécurité. Ces stratégies se doivent de définir les structures organisationnelles, fixer les objectifs et les délais pour la mise en œuvre effective de la politique de cybersécurité[35]. Parmi les pays cibles, le Sénégal et la Côte d'ivoire ont ratifié la convention de Malabo le faisant entrer en vigueur dans leur corpus juridique.

Au niveau régional, des initiatives communautaires sont notées telles que **la Stratégie régionale de la cybersécurité et de lutte contre la cybercriminalité.** L'objectif général de cette stratégie est « d'établir le cadre stratégique communautaire à prendre en compte par les Etats Membres dans leurs stratégies nationales et à mettre en œuvre dans leurs plans d'action sur la cybersécurité et la lutte contre la cybercriminalité avant la fin de l'année 2022 avec l'accompagnement de la CEDEAO ». Cette stratégie communautaire se décline en cinq objectifs stratégiques majeurs que sont :

- la formulation d'une politique nationale et une stratégie nationale de cybersécurité et de lutte contre ma cybercriminalité. A travers cet objectif, les états membres doivent établir et mettre à jour au moins tous les cinq (05) ans une stratégie nationale se basant sur la stratégie régionale
- le renforcement de la cybersécurité avec un cyberspace sûr et sécurisé avec la mise en place par les Etats membres d'une autorité nationale de cybersécurité ;
- la réduction de la cybercriminalité par un environnement adapté et la capacité de traduire les délinquants en justice par la mise en place d'un cadre juridique avec l'adoption de dispositions pénales et de procédure pénales adéquates et conformes aux recommandations régionales, continentales et mondiales ;
- la promotion de la coordination et de la coopération dans le renforcement de la cybersécurité et de la lutte contre la cybercriminalité avec l'obligation pour les Etats membres de ratifier les conventions régionales, continentales et internationales ;

34 UNESCO, Evaluation des besoins en Intelligence artificielle en Afrique, , 2021, 86 pages, https://unesdoc.unesco.org/ark:/48223/pf0000375321
35 Art 29 de la convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel

- l'établissement de mécanismes régionaux avec le soutien de la CEDEAO aux Etats membres dans la déclinaison au niveau national de cette stratégie.

Les quatre pays cibles (Bénin, Burkina Faso, Côte d'Ivoire et Sénégal), objet de notre étude, Etats membre de la CEDEAO ont élaboré chacun une stratégie nationale de cybersécurité, conformément à la stratégie régionale.

1. Stratégie nationale de sécurité numérique du Bénin

Considérant l'ambition du gouvernement Béninois de faire des techniques de l'information et de communication, l'un des leviers du développement socio-économique du pays, le Bénin a élaboré la Stratégie Nationale de la Sécurité Numérique (2020-2022) dont la vision est d'avoir *"un cyberspace sécurisé et attrayant pour une économie numérique florissante"*[36].

Cette stratégie a pour objectifs de (i) créer des compétences béninoises en matière de cybersécurité, (ii) protéger les systèmes d'informations critiques, (iii) mettre en place d'un cadre réglementaire attrayant, (iv) renforcer la lutte contre la cybercriminalité, (v) promouvoir la confiance numérique.

Cette stratégie comporte cinq (05) axes que sont :

1. la protection des systèmes d'information et des infrastructures avec la mise en place d'instruments nécessaires pour assurer un bon niveau de protection des systèmes d'information ;
2. la lutte contre la cybercriminalité et le développement du cadre juridique et réglementaire vise le renforcement du cadre juridique déjà complet avec des décrets d'application
3. le développement des compétences et de la culture de la sécurité numérique visant à renforcer le capital humain local par le développement de réseau de spécialistes et d'experts sur la culture numérique avec l'implication de l'Etat, des Universités et du secteur privé ;
4. la promotion de la confiance numérique avec la protection des données, des échanges numériques, les moyens de traçabilité et la sécurisation des transactions en ligne
5. la coordination nationale et la coopération internationale.

Cette stratégie est arrivée à terme depuis la fin de l'année 2022 mais sur ces cinq axes des résultats notables sont à relever tels qu'un dispositif réglementaire protecteur, la mise en place d'un organe de contrôle chargé de la cybersécurité (ANSSI-BENIN).

2. Stratégie nationale de cybersécurité du Burkina Faso 2019-2023

Le Burkina Faso a également adopté une stratégie nationale de la cybersécurité (2019-2023). Cette stratégie fixe les orientations stratégiques nationales en matière de cybersécurité et ambitionne de permettre au Burkina à l'horizon 2023, un cyberspace de confiance favorable au développement économique et social.

Cette stratégie trouve ses fondements au niveau international et régional dans la convention de Budapest et la Convention de Malabo sur la cybersécurité et la protection des données personnels et au niveau national à travers les différentes lois adoptées par le pays tels que la loi sur la protection des données à caractère personnel, la loi sur les réseaux et services des communications électroniques et la loi sur les services et transactions électroniques. Les orientations déclinées dans la stratégie sont :

- faire de la lutte contre la cybercriminalité et du renforcement des capacités de cybersécurité une priorité ;
- renforcer la coordination entre les différents acteurs du cyberespace et avec les homologues internationaux ;
- respecter les droits fondamentaux des personnes ;
- mettre en œuvre des mesures appropriées et proportionnées aux menaces ;
- mobiliser, fédérer et engager les différents acteurs privés du cyberespace et de la société civile autour des actions prévues dans la SNCS en vue de lutter contre la cybercriminalité.

36 Stratégie nationale de la sécurité numérique 2020-2022

Comme pour le Bénin, la stratégie du Burkina Faso est également arrivée à terme. Un bilan devra être fait sur l'état de leur mise en œuvre notamment sur le taux de réalisation, les acquis, les contraintes et les perspectives.

3. Stratégie nationale de cybersécurité de la Côte d'Ivoire 2021 -2025

A l'instar des autres pays cibles, le gouvernement ivoirien a adopté une stratégie dans le domaine de la cybersécurité en 2021 et comme échéance 2025. Cette stratégie a pour objectifs :

- le renforcement du cadre légal,
- la protection du cyberespace,
- le renforcement de la confiance numérique ;
- la refonte du cadre institutionnel,
- le renforcement de la capacité du capital humain et
- l'accroissement de la coopération internationale.

Cette stratégie s'appuie sur des principes tels que l'obligation mise à la charge des utilisateurs des services liés à la technologie des systèmes d'information de mettre en œuvre les bonnes pratiques de sécurité, la mise en œuvre de la stratégie conforme au respect des droits de l'homme et des libertés fondamentales notamment la protection des données à caractère personnel. La stratégie prône également la coopération et la collaboration avec les parties prenantes du secteur de la cybersécurité tant au niveau national qu'international. L'autorité de régulation des télécommunications de la Cote d"ivoire (ARTCI) est en charge de la lutte contre la cybercriminalité.

4. Stratégie nationale de cybersécurité du Sénégal 2022

En 2017, le Sénégal a également adopté la Stratégie nationale de la Cybersécurité dont le terme est prévu en 2022 (2017-2022)[37].

Cette stratégie a objectifs majeurs :

- le renforcement du cadre juridique et institutionnel de la cybersécurité au Sénégal,
- le renforcement des infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal,
- la promotion d'une culture de la cybersécurité au Sénégal, le renforcement les capacités et les connaissances techniques en cybersécurité dans tous les secteurs,
- la participation aux efforts régionaux et internationaux de cybersécurité.

Cette stratégie est arrivée à terme en 2022, un bilan à mi-parcours en 2020 montre un taux de réalisation très faible soit 4,1% dans la mise en œuvre de cette stratégie. Par exemple sur les objectifs n° 2, 3 et 4 aucun résultat n'a été atteint, même si des actions ont été entreprises et sont en cours de réalisation[38]. Seul l'objectif stratégique n°1 a connu des réalisations. Il faudra alors en tirer des leçons en vue de l'élaboration d'une nouvelle stratégie.

L'IA est autant un avantage qu'une menace pour la cybersécurité. En effet, l'IA, du fait de ses capacités, peut être utilisée notamment dans la gestion des menaces et incidents informatiques, la gestion des données mais est aussi susceptible de constituer une arme pour les actes de cybercriminalité. Les stratégies nationales des quatre pays cibles ont quasiment prévu les mêmes mesures génériques de cybersécurité. Ces mesures sont le renforcement du cadre juridique et institutionnel de la cybersécurité ; la lutte contre la cybercriminalité, la protection des systèmes et des infrastructures informatiques, le renforcement du capital humain et la protection des données personnelles. Ces mesures appréhendent bien évidemment les systèmes de l'IA.

37 Stratégie nationale de la cybersécurité du Sénégal SNC2022, http://www.numerique.gouv.sn/mediatheque/documentation/strat%C3%A9gie-nationale-de-cybers%C3%A9curit%C3%A9-snc2022

38 Stratégie nationale de la cybersécurité du Sénégal SNC2022, Analyse de la mise en œuvre de 2018 à 2020, El hadji Daouda DIAGNE, Spécialiste en cybersécurité

Toutefois, une meilleure prise en compte de cette technologie dans les stratégies nationales de cybersécurité nationale pourrait davantage favoriser son développement dans le domaine de la cybersécurité tout en encadrant les menaces potentielles. Le Benin semble avoir saisi cet enjeu de l'IA sur la cybersécurité, puisque dans sa stratégie nationale de cybersécurité, il a relevé la nécessité de s'adapter et d'appréhender les nouvelles tendances relatives aux nouvelles technologies notamment de l'IA et de se prémunir de ses risques[39].

B. L'émergence et le développement du numérique, une priorité pour les quatre pays cible

Le numérique constitue un levier de développement d'un pays à travers l'offre de biens et de services numériques, créant ainsi un cercle vertueux appelée l'économie numérique. Conscients de cela, les pays cibles du présent projet ont élaboré des documents stratégiques allant dans le sens du développement numérique et de l'accroissement de la contribution de l'économie numérique dans le développement des pays.

1. Stratégie nationale de développement numérique du Burkina Faso 2018-2027

Basée sur une période de dix (10) ans, la stratégie nationale de développement de l'économie définit l'ambition du Burkina en matière de transformation numérique et marque la volonté du pays d'inscrire les technologies et le numérique comme facteur stimulant de développement de l'ensemble de l'économie et de la société. Ainsi à l'horizon 2027, le Burkina Faso espère disposer d'une économie numérique compétitive impactant positivement, durablement et de façon inclusive à son développement[40].

Cette stratégie se fonde sur des principes directeurs au nombre de huit (08) parmi lesquels on peut citer :

1. Neutralité technologique : Ce principe directeur se réfère au fait que la réglementation de l'offre de services numériques ne doit pas consacrer de discrimination entre les différentes technologies susceptibles d'être utilisées pour rendre le service attendu.
2. Inclusion : Ce principe désigne l'ensemble des politiques et mesures concrètes mises en œuvre afin d'édifier une société de l'information ou une économie numérique dans laquelle tout burkinabè où qu'il soit, aura la possibilité créer, d'obtenir d'utiliser et de partager l'information et le savoir dans laquelle chaque communauté pourra ainsi réaliser l'intégralité de son potentiel dans la promotion de son développement durable et l'amélioration de la qualité de vie.
3. Egalité de genre : Ce principe directeur s'inscrit en cohérence avec la Politique Nationale de Genre (PNG) qui vise à infléchir les politiques publiques et sectorielles dans la perspective de construire une société débarrassée de toutes les formes d'inégalités et d'iniquités de genre et qui assure à l'ensemble de ces citoyens et citoyennes les sécurités essentielles pour épanouissement social, culturel, politique et économique.
4. Protection de la diversité culture et de l'éthique : L'édification d'une économie numérique inclusive doit être fondée sur le respect de l'identité culturelle, de la diversité culturelle et linguistique, des traditions et des religions. Elle doit promouvoir ce respect et le dialogue entre les cultures tant au sein du Burkina Faso que vis-à-vis de l'extérieur
5. La confiance : le renforcement du climat de confiance par des mesures garantissant notamment la sécurité de l'information et des données, la sécurité des réseaux, l'authentification, ainsi que la promotion de la vie privée de l'usager est un préalable au développement effectif de l'économie numérique.

En plus de ces principes directeurs, la stratégie repose sur deux orientations stratégiques à savoir :

- le développement de l'infrastructure et la généralisation de l'utilisation numérique ;
- la promotion de la bonne gouvernance dans le domaine de l'économie.

39 Stratégie nationale de sécurité numérique du Benin, page 10,
40 Stratégie nationale de développement numérique https://dgtic.mdenp.gov.bf/wp-content/uploads/2020/03/Strat%C3%A9gie_Nationale_de_D%C3%A9veloppment_de_Economie_Num%C3%A9rique_2018-2020.pdf

En termes d'objectifs, la stratégie se décline en sept (07) objectifs: (i) la mise en place d'une gouvernance efficace et efficiente, (ii) le développement d'un environnement propice à l'instauration de la confiance numérique, (iii) le déploiement d'une infrastructure large bande de qualité sur l'ensemble du pays, (iv) le positionnement des TIC comme un levier durable de la transformation de l'administration publique et des autres secteurs , (v) le développement de l'expertise numérique nationale, (vi)l'intégration du numérique dans le secteur éducatif et (vii) le développement d'une économie numérique équitable et inclusive.

2. Stratégie de développement numérique de la Côte d'Ivoire 2021-2025

La Côte d'Ivoire a adopté également en 2021, la stratégie de développement numérique pour accélérer la transformation numérique en vue de faire du pays, un hub et leader en matière d'innovation. Comme pour la stratégie sur la cybersécurité, 2025 est l'échéance prévue pour la stratégie du développement numérique.

Cette stratégie repose sur sept (07) piliers :

- **Pilier 1 :** les infrastructures numériques dont l'objectif est de mettre en place une infrastructure numérique capable de fournir un accès abordable et inclusif aux services numériques à haut et très haut débit sur le territoire national
- **Pilier 2 :** les services numériques avec comme objectif la mise en place d'une administration connectée et la diffusion des services numériques inclusifs dans les secteurs économiques prioritaires,
- **Pilier 3 :** les services financiers numériques visant à accroître la contribution des services financiers numériques à l'inclusion financière des populations et au développement du commerce électronique ;
- **Pilier 4 :** les compétences numériques avec comme objectif le développement des compétences numériques par le renforcement de la formation professionnelle et l'opérationnalisation des compétences requises pour impulser la créativité et les innovations
- **Pilier 5 :** l'environnement des affaires dans le secteur de l'économie numérique avec comme ambition la création d'un environnement des affaires propice à l'investissement, à l'entreprenariat et à l'innovation dans l'économie numérique
- **Pilier 6 :** l'Innovation avec comme objectif de rendre opérationnel la stratégie nationale de l'innovation dans le domaine du numérique
- **Pilier 7 :** la cybersécurité et la confiance numérique dont l'objectif vise à renforcer la cybersécurité en sécurisant les infrastructures techniques afin d'assurer leur disponibilité et garantir l'intégrité, la confidentialité et l'authenticité des données qui circulent dans le cyberespace ivoirien.

3. Stratégie Sénégal Numérique 2016-2025

Le Sénégal s'est doté d'une stratégie nationale du Numérique pour la période 2016-2025. Cette stratégie vise notamment à impulser la croissance économique du pays, généraliser l'usage du numérique, améliorer le climat des affaires et générer un volume important d'emplois directs et indirects dans le domaine du numérique.

Suite à des lenteurs constatées dans sa mise en œuvre, la stratégie a fait l'objet d'une actualisation en 2019. La stratégie actualisée se décline sur quatre (04) axes :

- Accès ouvert et abordable aux services numériques ;
- Administration connectée au service des citoyens et des entreprises ;
- Promotion de l'industrie numérique innovante et créatrice de valeur ;
- Diffusion du numérique dans les secteurs économiques prioritaires.

Les prérequis identifiés par la stratégie sont :

- le cadre juridique et institutionnel avec la mise à jour du cadre juridique liée aux secteurs du numérique ;
- le capital humain avec le renforcement de la formation professionnelle ;
- le cadre de confiance avec le renforcement de la cybersécurité.

En définitive, il ressort que les technologies émergentes notamment les systèmes d'IA sont prises en compte moyennement dans la stratégie de développement numérique du Sénégal, et de manière plus importante dans celle de la Côte d'ivoire. Concernant le Sénégal, l'IA est appréhendé en filigrane dans le prérequis 2 : « Capital humain », avec la mise en place de module de formation en IA, big data, cloud et IOT (internet of things)[41].

La Côte d'ivoire considère l'IA comme une opportunité dans le développement des infrastructures télécoms et l'accroissement de la confiance numérique[42]. Dans le domaine de l'innovation, l'utilisation de l'IA est envisagée comme catalyseur de la transformation numérique de l'industrie agricole et dans la gestion durable des villes (Smart cities). A cet effet, la Côte d'ivoire prévoit l'élaboration et la mise en œuvre d'une stratégie nationale pour le développement des technologies de la 4ème révolution industrielle (5G, intelligence artificielle…)[43] et la création d'un centre de recherche en intelligence artificielle spécialisé sur l'agriculture.44.

La stratégie nationale de développement numérique du Burkina Faso est restée muette sur les questions de l'IA. Elle mentionne juste la prise en compte du déploiement futur des technologies comme l'internet des objets, dans la réglementation dans le domaine numérique.[45]

C. Absence de politiques et stratégies propres à l'émergence de l'Intelligence artificielle

1) Des stratégies ou des politiques coordonnées sur l'IA au niveau des quatre pays cibles et l'Afrique en général à construire

Vu l'ampleur de l'utilisation des SIA dans de divers secteurs, de nombreux pays ont élaboré des stratégies nationales coordonnées spécifiques fournissant un cadre global à même de guider les politiques gouvernementales. En 2020 déjà, près de vingt-sept (27) pays dans le monde ont élaboré des stratégies nationales sur l'IA et 18 autres pays avaient entamé le processus d'élaboration[46].

Sur le continent africain, seuls sept (07) pays ont élaboré et publié une stratégie nationale sur l'intelligence artificielle. Il s'agit du Benin, de l'Egypte, de l'ile Maurice, de l'Ouganda, du Rwanda, du Sénégal et de la Sierra Léone[47]. En Afrique l'Ouest, seuls trois pays (Sénégal-Benin-Sierra Léone) sur seize pays ont élaboré une stratégie sur l'IA. Le faible taux de documents politiques sur l'IA atteste que l'IA est insuffisamment par les pays africains de manière générale et de ouest africains en particulier.

Néanmoins, il faut relever des initiatives sont en cours dans la région ouest africaine. La Côte d'ivoire a entamé le processus d'élaboration de stratégie sur l'IA en lançant un appel national à contribution[48]. Il en est de même pour le Nigéria[49] et le Ghana.

En dehors de l'Afrique de l'Ouest, d'autres initiatives sont à souligner au niveau continental. Par exemple, Maroc a créé un centre international d'intelligence artificielle[50], et lancé lancement d'un programme d'appui à la recherche en intelligence artificielle et ses applications, élaboré un projet de feuille de route nationale de

41 Stratégie nationale du Numérique 2025, Plans d'actions actualisés, http://www.numerique.gouv.sn/sites/default/files/Strat%C3%A9gie%20Numerique-SN2025-%20Plan%20d%27actions%20actualis%C3%A9.pdf
42 Stratégie de développement du numérique cote d'ivoire 2021-2025, page 14
43 Stratégie de développement du numérique Cote d'ivoire 2021-2025, page 57
44 Stratégie de développement du numérique cote d'ivoire 2021-2025, page 59
45 Stratégie nationale de développement numérique du Burkina Faso 2018-2027, page 26
46 L'ère de l'IA dans le monde, rapport sur les stratégies nationales et régionales en matière d'IA, https://cifar.ca/wp-content/uploads/2020/11/l-ere-de-l-ia-deuxieme-edition-f.pdf
47 Législations (africadataprotection.org)
48 Ministère de la Transition Numérique et de la Digitalisation :: Dossiers || C?0?0te d'Ivoire (telecom.gouv.ci)
49 Le Nigeria prépare une stratégie nationale d'IA et s'ouvre à l'expertise internationale - We are Tech
50 https://www.um6p.ma/fr/le-centre-international-dintelligence-artificielle-du-maroc

l'IA[51]. La Tunisie élabore actuellement sa stratégie nationale dans ce domaine[52]. Le Kenya a mis en place un groupe de travail de onze (11) personnes pour l'élaboration d'une stratégie afin d'encourager les technologies émergentes telles que l'IA et la block Chain[53]..

L'Union africaine a également entamé le processus d'élaboration d'une stratégie continentale d'IA qui se veut éthique et économiquement fructueuse pour le continent. Cette stratégie s'adresse aux secteurs clés susceptibles de bénéficier de la technologie notamment l'éducation, les soins de santé, l'agriculture et la finance[54]. L'adoption de cette stratégie est prévue en 2024.

Le BENIN et le SENEGAL, leaders en Afrique de l'Ouest

Le Benin et le Sénégal font figure de proue dans le continent africain de manière générale et dans la zone ouest africain particulièrement dans l'élaboration de politique en matière d'IA.

En effet, le Benin est le premier pays ouest africain à avoir élaboré une stratégie sur l'IA55 Fixée sur la période 2023-2027, le Benin ambitionne de réaliser sa vision qui est de faire rayonner dans cinq (05) ans le pays par l'intelligence artificielle, un levier de croissance des secteurs stratégiques, dans une approche opportuniste. La stratégie est déclinée en trois orientations stratégiques :

- Orientation stratégique 1 : Organisation et consolidation de l'embryon d'écosystème existant et valorisation de ses résultats ;
- Orientation stratégique 2 : Développement et soutien accru à l'écosystème de l'IA ; Orientation stratégique 3 : Valorisation de l'écosystème, de la connaissance et du savoir-faire béninois.

La stratégie vise également quatre objectifs :

- la mise en œuvre des cas d'usage de l'IA et les initiatives à fort impact ;
- le renforcement des capacités humaines sur l'IA et la gestion des métadonnées ;
- la garantie d'un meilleur soutien au développement du capital humain, à la recherche, à l'innovation, au secteur privé et à la coopération dans le domaine de l'IA,
- la mise à jour le cadre institutionnel et règlementaire pour l'IA et la gestion de mégadonnées.

La stratégie béninoise de l'IA donne le cadre pour le projet ambitieux du Benin de faire de l'IA responsable comme un moteur de développement.

Le Sénégal a élaboré sa stratégie nationale de l'IA en 2024. Cette stratégie, qui s'inscrit dans le cadre plus large du Plan Sénégal émergent (PSE) et de la stratégie nationale pour le développement numérique, a pour vision : « *une IA éthique et de confiance, catalyseur du Plan Sénégal émergent, de l'emploi des jeunes, de la performance de l'économie, de la transformation publique, de la souveraineté et de l'attractivité du Sénégal » à l'horizon 2028*[56]. Cette stratégie s'articule sur quatre objectifs majeurs : (1) faire de l'IA, locomotive de l'économie numérique, un catalyseur du PSE au service du développement du pays, (2) orienter l'IA au Sénégal de façon prioritaire vers l'amélioration des conditions de vie de la population et les ODD, en d'autres termes, IA for Good, (3) faire de l'IA une opportunité pour le Sénégal d'être moteur d'un partenariat technologique régional et sous régional, (4) s'assurer que l'IA soit digne de confiance. Ces objectifs sont déclinés en quatre orientations stratégiques : (1) le Capital humain, (2) l'IA from lab to market , (3) Sénégal moteur du hub IA ouest africain, (4) l'IA en toute confiance, une affaire de tous et 56 actions prioritaires.

Une feuille de route prioritaire structurée en vague a été élaborée pour la mise en œuvre des actions prévues telles que la mise en place une chaire interuniversitaire « Intelligence artificielle et souveraineté numérique », la création d'un campus IA, la mise en place un programme spécial des startup act dédiés à l'IA, élaborer un guide de la régulation de l'IA sur la base des standards nationaux, africains et internationaux.

51 https://aujourdhui.ma/economie/lintelligence-artificielle-priorite-du-chantier-de-la-transformation-digitale
52 L'ère de l'IA, rapport sur les stratégies nationales et internationales, https://cifar.ca/wp-content/uploads/2020/11/l-ere-de-l-ia-deuxieme-edition-f.pdf
53 L'ère de l'IA, rapport sur les stratégies nationales op cité
54 L'IA était en tête de l'ordre du jour du sommet de l'Union africaine (yahoo.com)
55 Stratégie nationale d'intelligence artificielle et les méga données (2023-2027) strategie-nationale-d'intelligence-artificielle-et-des-megadonnees-2023-2027.pdf
56 Enabel_Strategie IA Senegal_V1.indd (ai4d.ai)

Dans une perspective de synergie et en raison du lien intime entre les systèmes de l'IA et les données, la stratégie sur l'IA s'accompagne de la stratégie nationale des données, également élaborée en 2024.

D. Nécessité d'élaborer des stratégies et politiques spécifiques pour le développement d'une IA favorable au bien-être de tous

Comme en matière de cybersécurité, l'IA mériterait une meilleure prise en compte des Etats du fait de son importance actuelle dans l'économie mondiale. En effet, en plus de permettre des gains importants de compétitivité ou de productivité dans tous les secteurs de l'économie et des services publics, l'IA devrait générer près de 90 milliards de dollars de bénéfice mondial à l'horizon 2025[57]..L'impact de l'IA se ressent dans tous les secteurs de l'économie tels les secteurs prioritaires de l'agriculture, de la santé, l'éducation et les transports. Par conséquent, il parait important que les pouvoirs publics élaborent une politique en la matière afin d'encadrer le développement et l'utilisation de l'intelligence artificielle afin d'en tirer le maximum de bénéfices pour la société et l'économie. Pour assurer l'efficacité et l'efficience des stratégies nationales sur l'IA, il semble important de prendre en compte les préoccupations et réalités endogènes et d'éviter des copier- coller des stratégies nationales existantes dans d'autres pays.

Les pouvoirs publics pourront s'appuyer sur les recommandations de l'UA émises dans le cadre de sa stratégie de transformation numérique pour l'Afrique (2020-2030) pour une utilisation optimale des technologies émergentes telles que l'intelligence artificielle, la Blok Chain (chaîne de blocs), l'Internet des objets[58].

Ces mesures préconisées sont entre autres

- la nécessité de de promouvoir des politiques et règlements qui tiennent compte des technologies émergentes en matière de protection des citoyens, d'équité des marchés et d'application
- la nécessité de repenser les approches réglementaires et adopter des modèles souples et collaboratifs pour relever les défis posés par les technologies émergentes et la quatrième révolution industrielle,
- la nécessité d'établir des mécanismes de coordination entre les secteurs concernés
- la nécessité de mettre en place de groupes de travails nationaux pour la recherche sur les technologies émergentes sécurisées et proposer des lignes directrices qui éduqueront les utilisateurs d'internet sur la manière d'identifier les dispositifs sécurisés
- la nécessité d'encourager les secteurs public et privé à embrasser les technologies émergentes.

57 https://www.myriadconsulting.fr/blog/2022/strategie-nationale-intelligence-artificielle/

58 Projet de stratégie de transformation numérique pour l'Afrique (2020-2030) https://au.int/sites/default/files/newsevents/workingdocuments/37470-wd-annexe_2_ie25274_f_digital_transformation_startegy.pdf

1. Tableau SWOT des politiques et stratégies liées à l'Intelligence artificielle, les données et technologies émergentes des quatre pays cibles du projet

Forces	**Faiblesses**
· *Existence de stratégie nationale sur la cybersécurité* · *Existence de politique et stratégie dans le domaine du développement numérique ;* · *Prise en compte relative des technologies émergentes telles que l'IA dans les stratégies existantes ;* · *Une stratégie nationale sur l'IA déjà élaborée et publiée dans deux des pays cibles du projet (Sénégal et Benin) ;* · *Une stratégie nationale de la donnée élaborée au Sénégal* · *Existence d'un cadre stratégique de la donnée au niveau continental*	· *Retard dans la réalisation des objectifs déclinés dans les stratégies nationales du numérique ;(Exemple Sénégal)* · *Faiblesse de la prise en compte des technologies émergentes dans les stratégies en vigueur dans le domaine du numérique des pays cibles* · *Quasi inexistence de stratégie coordonnée nationale sur l'IA pour favoriser et encadrer son développement ;* · *Inexistence de stratégie continentale, régionale sur l'IA*
Opportunités	***M*enaces**
· *Volonté politique des pays cible d'élaborer les stratégies nationales sur l'IA* · *Emergence des initiatives sur l'IA telles que la mise en place de modules de formation sur les technologies émergentes,* · *Mise en place de centre de recherche sur l'IA et l'érection de Datacenters* · *Possibilité d'utilisation des SIA par les pouvoirs publics pour une administration forte ;* · *Projet d'élaboration de stratégie continentale d'IA en cours*	· *Utilisation accrue des SIA sans aucun cadre légal approprié tant au niveau national qu'au niveau communautaire* · *Caractère transnational des SIA* · *Utilisation massive des réseaux sociaux utilisant les SIA par les populations des pays cibles* · *Récurrence des défis éthiques liés aux systèmes de l'IA*

II. ETAT DES LIEUX DU CADRE JURIDIQUE RELATIFS A L'IA, LES DONNEES ET TECHNOLOGIES EMERGENTES DES QUATRE PAYS CIBLES

A. Un arsenal juridique important dans le domaine du Numérique

Outre les stratégies et les politiques, les pays cibles disposent dans le domaine du numérique d'un arsenal juridique assez fort. Bien qu'il n'existe pas une législation spécifique à l'IA dans les pays cibles, le SIA, n'est pas hors du champ juridique, certains de ses aspects se trouvent appréhender par le cadre juridique existant dans le domaine du Numérique.

i. La répression de la cybercriminalité

La cybersécurité et la lutte contre la cybercriminalité ne font pas l'objet que de politique et de stratégies. Il existe en fait un cadre juridique contraignant en la matière. Au niveau international, **la Convention sur la cybercriminalité, ouverte à la signature à Budapest**, Hongrie, en novembre 2001, est considérée comme l'accord international le plus pertinent sur la cybercriminalité et la preuve électronique. La Convention de Budapest prévoit (i) l'incrimination d'un certain nombre de comportements allant de l'accès illégal et l'atteinte à l'intégrité des données et des systèmes jusqu'à la fraude liée à l'informatique et à la pornographie enfantine ; (ii) des outils de droit pénal pour enquêter dans des affaires de cybercriminalité et recueillir et sécuriser les preuves électroniques concernant tout crime ; et (iii) une coopération internationale efficiente. La Convention concilie la vision d'un Internet libre où les informations peuvent circuler, être accessibles et partagées librement, et la nécessité d'une réponse efficace de la justice pénale dans des affaires d'abus criminels de l'Internet. Seuls le Sénégal et le Bénin parmi les pays cibles ont ratifié la Convention de Budapest. La Côte d'Ivoire et le Burkina Faso sont invités à adhérer à cette Convention sur la cybercriminalité.

Au niveau continental, la **Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel, appelée Convention de Malabo** est le texte de référence. Ce texte prévoit notamment que « l*es Etats parties adoptent des mesures législatives et/ou réglementaires qu'il jugera efficace en considérant comme infractions criminelles des actes qui affectent la confidentialité, l'intégrité, la disponibilité et la survivance des systèmes technologies de l'information et de la communication et les données traités* [59]». En outre, il est demandé aux Etats parties d'ériger en infractions pénales, les atteintes aux systèmes informatiques, les atteintes aux données informatiques, celles portant sur le contenu et aux mesures de sécurisation des échanges électroniques. Aux termes de la convention, il faut entendre par système informatique « *tout dispositif électronique, magnétique, optique, électrochimique ou tout autre dispositif de haut débit isolé ou interconnecté qui performe la fonction de stockage de données ou l'installation de communications*. *Ces communications sont directement liées à ou fonctionnent en association avec d'autre(s) dispositif(s)* » et les données informatiques : « *toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique* ».

Le SIA pouvant être considéré comme un système information et utilisant des données informatiques pour son fonctionnement tombe sur l'emprise de la réglementation juridique en matière de cybersécurité et de cybercriminalité. Le SIA n'est pas à l'abri d'actes de cybercriminalité c'est pourquoi l'aspect sécurité doit être pris en compte dès la conception du système. Le SIA peut être victime d'empoisonnement des données c'est-à-dire une altération des jeux de données utilisé pour l'entrainement du système dans le but de fausser le fonctionnement et les résultats. Outre l'empoisonnement des données, des vols de données constituant à la reconstitution du code source à des fins personnelles peuvent subvenir.

La Convention est ouverte à tous les Etats membres de l'Union Africaine, pour signature, ratification et adhésion, conformément à leurs procédures constitutionnelles respectives. La ratification des quinze Etats membres est devenue effective depuis le 8 juin 2023[60]. Ce qui fait que cet instrument est le texte de référence au niveau continental.

59 Article 25 de la convention africaine sur la protection des données à caractère personnel et la cybersécurité

60 Les quinze premiers Etats ayant ratifiés la Convention sont : Mauritanie, Togo, Zambie, Sénégal, Rwanda, Namibie, Niger, Île Maurice, Mozambique, Guinée, Ghana, République Démocratique du Congo, Cap-Vert, Angola, Côte d'Ivoire.

Au niveau communautaire, les Etats membres de la CEDEAO ont adopté la Directive C/DIR/1/08111 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO matérialisant leur volonté pour l'adoption d'un cadre juridique harmonisé dans la lutte contre la cybercriminalité. Cette Directive a pour objet d'adapter le droit pénal de fond et la procédure pénale des Etats Membres de la CEDEAO au phénomène de la cybercriminalité61 et elle s'applique à toutes les infractions relatives à la cybercriminalité dans l'espace CEDEAO, ainsi qu'à toutes les infractions pénales dont la constatation requiert la collecte d'une preuve électronique[62]. Cette Directive a défini dans son chapitre II les critères des infractions spécifiques aux technologies de l'information et de la communication avant de mettre en exergue les mesures d'adaptation des infractions classiques aux technologies de l'information et de la communication dans son chapitre III.

Au niveau des pays cibles, tous ont adopté une législation en matière de cybercriminalité.

En effet, le Sénégal, dès 2008 dans le cadre d'un dispositif législatif appelé « Paquet numérique », a adopté la **loi n° 2008-11 du 25 janvier 2008 sur la Cybercriminalité**. Ce texte a connu une modification avec la révision du Code pénal par la **loi n° 2016-29 du 08 novembre 2016**. Ces infractions prévues par la loi sont notamment relatives :

- À la confidentialité, l'intégrité et à la disponibilité des systèmes informatiques avec des peines allant d'un an à cinq ans d'emprisonnement et d'un million à dix millions d'amende63 ;
- Aux données informatiques telles l'interception, l'effacement, l'altération ou la modification frauduleuse des données avec des peines allant d'un à cinq ans d'emprisonnement et de cinq cent mille à dix millions FCFA64 ;
- Aux droits de la personne au regard du traitement des données à caractère personnel régis par les dispositions 432-17 à 432-31 de la loi ;
- A la pornographie infantile et aux activités des prestataires techniques de services de communication au public par voie électronique.

Les atteintes liées aux droits d'auteur et droits voisins par voie informatique sont prévus **par la loi 2008-09 du 25 janvier 2008 sur le droit d'auteur et les droits voisins** aux articles 143 et 145.

Il y a lieu de noter que le Sénégal ne dispose pas encore d'une structure nationale de lutte contre la cybersécurité, à l'image de l'office Office central de répression de la cybercriminalité (OCRC) .

Le Bénin a opéré une véritable révolution juridique avec son code numérique qui fait l'objet de la **loi 2017-20 du 13 juin 2017**. Ce Code qui regroupe toutes les matières relevant du numérique abroge ainsi toutes les dispositions législatives contraires notamment : la loi 2009-09 du 24 mai 2009 portant protection des données à caractère personnel, la loi 2014-14 du 14 juillet 2014 relative aux communications électroniques et à la poste, à l'exception des dispositions relatives au secteur postal.

En matière de cybersécurité, le Benin dispose d'un cadre juridique complet et répressif en matière de cybersécurité qui est traité au livre 6 du Code du numérique.

Le Code numérique prévoit un régime général de responsabilité qui s'applique aux opérateurs fournisseurs d'accès à internet, les fournisseurs de service en ligne et les éditeurs de service en ligne dont les manquements font l'objet de sanctions pénales. Un régime spécifique de responsabilité s'applique au fournisseur de cache, aux fournisseurs de liens hypertextes, de fournisseurs de moteurs de recherche et des activités d'hébergement. Dans le cadre de la lutte contre la cybercriminalité, le livre 6 prévoit diverses infractions parmi lesquelles on peut citer :

Les atteintes liées au système informatique telles que l'accès et le maintien illégal punis d'un à cinq ans et de cinq cent mille à deux millions de FCFA d'amende ou soit l'un un l'autre des peines. En cas de suppression, de modification et des données contenues dans le système informatique, les peines sont doublées et en cas de violation d'une mesure de sécurité, la réclusion criminelle de dix à vingt ans peut être prononcée et une amende de cinq millions à cinq cent millions de FCFA[65].

61 Article 2 de la Directeur C/DIR/1/08111 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO
62 Article 3 de la Directive C/DIR/1/08111 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO
63 Art 431-8 à 431-10 de la loi de 2008-11 sur la cybersécurité
64 Art 431-11 à 431-16 de la loi 2008-11 sur la cybersécurité
65 Art 507 du code du numérique

Les atteintes aux données informatiques telles que l'interception, la divulgation, l'altération ou le détournement des données est punie de deux ans à cinq ans et/ou une amende de cinq cent mille FCFA à deux millions de FCFA. En cas de transfert sans autorisation les peines sont portées de cinq à dix ans et d'une amende de cinq millions à cent millions et les peines sont doublées si ce transfert a été commis avec une intention frauduleuse ou en rapport avec un système informatique connecté avec un autre système informatique [66].

Les atteintes liées à l'intégrité du système sont punies d'une peine d'emprisonnement de deux ans à cinq ans et/ou d'une amende de cinq millions à cinq cent millions FCFA. En cas de dommages des données dans le système, les peines prévues sont de cinq ans à dix ans d'emprisonnement et/ou une amende de cinq millions à cinq cent millions. La perturbation grave du système empêchant totalement ou partiellement son fonctionnement normal est puni à la réclusion criminelle de dix ans à vingt ans et une amende allant de cinq millions à cinq cent millions (500 .000 000) de FCFA67. Quant aux atteintes à l'intégrité des données, l'endommagement, l'effacement, l'altération, la suppression et la détérioration des données des données informatiques sont punies de six mois à cinq ans d'emprisonnement et ou d'une amende de cinq cent mille à deux millions. Si cela a été fait avec une intention de nuire, la peine d'emprisonnement est fixée à deux (02) ans à cinq (5) ans et d'une amende de cinq cent mille à deux millions[68] .

Le livre 6 prévoit la création de l'Agence nationale de la sécurité des systèmes informatiques dénommée ***« ANSSI-BENIN »*** en charge de la sécurité informatique et des réseaux. L'ANSSI-BENIN a pour missions notamment de veiller à l'exécution des orientations nationales et de la stratégie générale de l'État en matière de sécurité des systèmes d'information et des réseaux, suivre l'exécution des plans et des programmes relatifs à la sécurité des systèmes d'information et des réseaux dans les secteurs public et privé et à assurer la coordination entre les divers intervenants dans ce domaine , apporter son concours aux services de l'État en matière de sécurité des systèmes d'information et des réseaux ; effectuer un contrôle général de la sécurité des systèmes d'information et des réseaux relevant des divers organismes publics et privés identifiés par voie règlementaire, centraliser les demandes d'assistance à la suite des incidents de sécurité sur les systèmes d'informations et les réseaux, assurer la veille technologique dans le domaine de la sécurité des systèmes d'information et des réseaux , établir et maintenir une base de données des vulnérabilités, élaborer des recommandations sur la sécurité des systèmes d'information et des réseaux et veiller à leur mise en œuvre dans les organismes public[69]. Le code du numérique prévoit également la création de l'office Office central de répression de la cybercriminalité (OCRC) qui a pour compétence les infractions spécifiques à la criminalité liées aux technologies de l'information et de la communication. L'OCRC a pour entres autres attributions[70] :

- de veiller à la prise de mesures préventives contre la cybercriminalité ;
- d'animer et de coordonner, au niveau national, la mise en œuvre opérationnelle de la lutte contre les auteurs et complices d'infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication ;
- d'effectuer conformément au code de procédure pénale les enquêtes sur les infractions visant ou utilisant les systèmes informatiques ainsi que les modes de traitement, de stockage et de communication de l'information ;
- d'apporter son concours technique aux autres services de sécurité à l'occasion des enquêtes en cours nécessitant ses compétences techniques ou son expertise.

Le Bénin a prévu des dispositions très sévères en matière de cybersécurité afin de dissuader des actes de cybercriminalité. Au-delà des infractions, des organes ont été créés pour assurer le contrôle et prévenir les actes malfaisants et assurer la lutte contre les autres, ce qui renforce davantage le cadre juridique.

A l'instar du Sénégal et du Bénin, le Burkina Faso a prévu des dispositions légales pour lutter contre la cybercriminalité. Toutefois, le Burkina Faso ne dispose pas en soi d'une loi spécifique en matière de cybersécurité, les dispositions relatives aux atteintes en matières informatiques et au moyen des technologies de l'information et de la communication sont intégrées **dans la loi n° 025-2018/AN du 31 mai 2018 portant**

66 Art 508 du code du numérique
67 Art 509 du code du numérique
68 Art 510 du code du numérique
69 Art 606 du code du numérique
70 Art 610 du code du numérique

code pénal modifié au niveau du titre VII. Comme pour le Sénégal et le Bénin, le législateur burkinabé a prévu les infractions liées aux systèmes informatiques et celles liées aux données informations[71]. De plus, le code pénal burkinabé sanctionne également les manquements aux obligations légales dans la mise en œuvre et l'utilisation d'un système de traitement automatisé de données à caractère personnel.

Concernant les atteintes aux systèmes informatiques, l'accès et le maintien sans droit et de manière intentionnelle à tout ou partie d'un système informatique, est puni à une peine d'emprisonnement de deux (02) mois à deux (02) années et d'une amende de deux cent cinquante mille (FCFA à six cent mille FCFA[72]. S'il en résulte la suppression, la modification, ou l'altération des données contenues dans le système ou soit l'altération du fonctionnement du système, la peine est portée à deux mois à trois ans et l'amende de six cent mille (600.000) FCFA à deux millions (2 000 000) FCFA. Quant à l'entrave intentionnelle et sans droit du fonctionnement du système informatique par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques, il est prévu une peine d'emprisonnement de trois (03) à cinq ans et d'une amende de deux cent cinquante mille (250.000) à un million cinq cent mille (1 500 000) FCFA. Les mêmes peines sont prévues en cas d'introduction directe ou indirecte des données informatiques dans un système fait de manière intentionnelle et sans droit[73].

Sur les atteintes aux données informatiques, le code pénal prévoit une peine d'un à cinq ans d'emprisonnement et d'une amende de cinq cent mille (500 000) à deux millions (2 000 000) de FCFA, en cas d'interception intentionnelle et sans droit, par des moyens techniques, des données informatiques, lors des transmissions non publiques à destination à l'intérieur d'un système informatique. L'endommagement, l'effacement, la détérioration, l'altération, la modification et la suppression de données informatiques est punie à un an à dix ans d'emprisonnement et une amende de deux millions (2 000 000) à dix millions de FCFA. Si l'altération, la détérioration, la modification et la suppression des données informatiques engendre des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles, il est prévu une peine d'emprisonnement d'un an à dix ans et une amende d'un million à cinq millions de FCFA. Il est prévu des mêmes peines en d'utilisation des données obtenues de la façon ci-dessus[74].

Toute personne qui sans droit, produit, vend, obtient pour utilisation, importe, diffuse ou met à disposition sous quelque forme un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions relatives aux atteintes aux systèmes et données informatiques prévues par le code ou un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions relatives aux systèmes et données informatiques prévues par le code pénal.

Sur l'utilisation de système automatisé de traitement de données personnels, le code pénal burkinabé sanctionne d'une peine de trois mois à cinq ans et d'une amende de cinq cent mille à deux millions le non-respect des formalités préalables à la mise en œuvre mis à la charge du responsable de traitement de données en cas de traitement automatisé d'informations nominatives[75]. Le manquement par le responsable d'un traitement automatisé de données personnelles à son obligation d'information vis-à-vis de la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est sanctionné d'une peine d'emprisonnement d'un mois à deux ans et d'une amende de deux cent cinquante (250 000) à un million de FCFA[76].

En application de ces dispositions, on peut dire le Burkina Faso dispose d'un cadre juridique assez complet et moderne en matière de cybersécurité. Toutefois, les sanctions prévues par la loi ne semblent pas très dissuasives contre les pratiques malveillantes de cybercriminalité.

En matière de lutte contre la cybersécurité, la Côte d'Ivoire n'est pas en reste. Il a adopté en 2013 un paquet de lois dans le domaine du numérique dont **la loi n° 2013-451 du 19 juin 2013 relative à la lutte contre**

71 Art 700-1 du code pénal: données informatiques s'entendent : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;
72 Art 711-1 et 711-2 du Code pénal
73 Art 711-3 et 711-2 du code pénal
74 Art 711-5 et 711-8 du code pénal
75 Art 712-4 du code pénal burkinabé
76 Art 712-5 du code pénal burkinabé

la cybercriminalité. Cette loi prévoit des infractions spécifiques aux TIC dont les atteintes aux systèmes informatiques, les atteintes aux données informatiques, la pornographie infantile, la protection des données à caractère personnel et les atteintes aux droits de propriété intellectuelle.

Concernant les atteintes aux systèmes informatiques, telles l'accès, le maintien frauduleux système informatique sont punis 'une peine d'emprisonnement d'un à deux ans et d'une amende de dix à quarante millions de FCFA.

L'entrave aux fonctionnements dudit système informatique est punie d'une peine d'un à cinq millions avec une amende de dix à quarante millions de FCFA. Il en est de même pour l'introduction frauduleuse de données dans le système informatique[77].

Les atteintes aux données : l'interception frauduleuse ou la tentative d'interception de données informatiques est punie d'une peine de cinq à dix ans avec une amende allant de quarante millions à soixante millions de FCFA. Les mêmes peines sont applicables en cas d'altération, modification ou suppression ou tentative d'un de ces faits des données informatiques. Il en est de même en cas de production et de fabrication d'un ensemble de données par l'introduction, la modification, l'altération ou la suppression frauduleuse de données informatiques engendrant des données contrefaites dans l'intention qu'elles soient prises en compte ou utilisés à des fins légales.

Les personnes qui participent à une association formée ou une entente en vue de préparer ou de commettre des atteintes contre le système informatique et données informatiques sont punies à des peines allant de dix à vingt ans et une amende de soixante-quinze millions à cent millions de FCFA[78].

La pornographie infantile à travers les systèmes informatiques est fortement réprimée par la loi avec des peines varient de cinq à dix d'emprisonnement et une amende allant de cinq à cent millions de FCFA[79] .

L'utilisation sous quelque forme que ce soit des données à caractère personnel sans consentement préalable écrit aux fins de prospection directe et l'utilisation de procédés illicites à des fins d'envoi de messages électroniques non sollicités sur la base de collecte de données à caractère personnelle sont punies d'un à cinq ans d'emprisonnement et d'un million à dix millions d'amende[80].

Les infractions relatives aux atteintes aux droits d'auteur sont également prévues par la loi. Ainsi, sous réserve des exceptions prévues par la loi, la représentation et la reproduction d'une œuvre à travers un système informatique d'une œuvre sans l'autorisation de l'auteur ou de ses ayants droits sont punies d'une peine d'emprisonnement d'un à dix ans et une amende cinq millions à dix millions de FCFA.[81]

Le cadre juridique existant en matière de cybercriminalité dans les quatre pays cibles appréhendent les systèmes de l'IA. Toutefois, il y a lieu de renforcer ce cadre et d'élaborer des dispositions obligeant les concepteurs des SIA de prévoir des mesures techniques de protection notamment, celle imposant le respect du principe de Privacy by Design (PbD) qui place la protection des données personnelles et de la vie privée comme priorité absolue dès la conception d'une application. Une modification des législations s'impose dans cette perspective. De plus, il faut également mettre en place les organes chargés de la sécurité des systèmes informatiques et de renforcer ceux déjà existants.

ii. Le cadre juridique sur la protection des données à caractère personnel

La collecte et le traitement de données à caractère ne sont nouveaux en Afrique notamment Afrique de l'ouest. Toutefois, le développement du numérique en Afrique et l'émergence de nouveaux acteurs de l'internet ont apporté de profondes mutations sur l'utilisation et le traitement des données à caractère personnel. En effet, l'Afrique représente en 2021 près de 10, 9% des internautes mondiaux soit 507,9 millions d'internautes sur le continent dont 42% en Afrique de l'ouest[82]. Sur cette population africaine d'internautes près de 277 200 000 sont des utilisateurs de réseaux sociaux dont 16% en Afrique de l'ouest[83].

77 Art 4 à Art 7 de la loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité
78 Art 8 à Art 12 de la loi sus citée
79 Art 15 à Art 18 de la loi
80 Art 21 et Art 22
81 Art 33 de la loi de 2013 relative à la lutte contre la cybercriminalité
82 https://cmdafrique.net/2021/01/27/chiffres-internet-afrique-2021/
83 https://cmdafrique.net/2021/01/27/chiffres-reseaux-sociaux-afrique-2021/

Par ailleurs, l'Afrique dont la population a majorité analphabète générant une quantité importante de données personnelles, constitue un grand vivier pour les géants du numérique tels que les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) dont le modèle économique est fondé essentiellement sur la collecte et le traitement de données personnelles.

Par ailleurs, l'utilisation massive des données à caractère personnel est exacerbée par l'apparition de SIA qui nécessite une quantité importante de données dont personnelles pour son développement.

L'encadrement juridique de la protection des données à caractère personnel en Afrique notamment en Afrique de l'ouest est récent. Les premières législations en la matière datent d'une vingtaine d'années. Sur 55 pays, 39 disposent en 2023 une législation sur la protection des données à caractère personnel parmi lesquels 11 pays de l'Afrique de l'Ouest (Bénin, Burkina Faso, Ghana, Guinée, Mali, Côte d'Ivoire, Niger, Nigéria, Sénégal, Togo, Mauritanie,).

La protection des données à caractère personnel trouve sa source au niveau international d'abord à travers l'article 12 de **la Déclaration universelle des droits de l'homme** qui stipule que : *« Nul ne sera l›objet d›immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes »*.

Ensuite, il y'a la convention pour la protection des personnes à l'égard du traitement des données à caractère personnel **(Convention 108+ modernisée)** mise en place par les membres du Conseil de l'Europe et de l'Union européenne avec comme objectif de protéger toute personne physique quelle que soit sa nationalité ou sa résidence à l'égard du traitement des données à caractère personnel contribuant ainsi au respect de ses droits fondamentaux et de ses libertés fondamentales notamment du droit à la vie privée.84

Au niveau africain, la Convention de Malabo vise à mettre en place, dans chaque État partie, un dispositif permettant de lutter contre les atteintes à la vie privée susceptibles d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des données à caractère personnel. Elle garantit, en proposant un type d'ancrage institutionnel, que tout traitement, sous quelque forme que ce soit, respecte les libertés et droits fondamentaux des personnes physiques tout en prenant également en compte les prérogatives des États, les droits des collectivités locales, les intérêts des entreprises sur la base des meilleures pratiques reconnues au niveau international. Cette convention assure le respect de certains principes de base gouvernant le traitement des données à caractère personnel et qui garantissent le respect de la vie privée des personnes tels que les principes du consentement, de transparence, de confidentialité, de sécurité dans le traitement des données à caractère personnel, etc.[85] A cela s'ajoute au niveau régional, **l'acte additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel de la CEDEAO** qui vise à harmoniser le cadre juridique et institutionnel de la protection des données à caractère personnel, ses formalités, ses principes directeurs, les droits de la personne dont les données font l'objet d'un traitement, et les obligations du responsable de traitement de données. La CEDEAO demande à chaque Etat membre de mettre en place un cadre légal de protection de la vie privée et professionnelle consécutive à la collecte, au traitement, à la transmission, au stockage à l'usage de données à caractère personnel et la création d'une autorité de protection des données à caractère personnel.

Au niveau national, les quatre pays cibles aient tous élaboré une loi sur la protection des données à caractère personnel.

A la faveur de **la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel**, le Sénégal fait partie des premiers pays de l'Afrique de l'Ouest à adopter un dispositif permettant de lutter contre les atteintes à la vie privée susceptibles d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des données à caractère personnel.

Cette loi s'applique aux traitements de données effectués aussi bien par le secteur public que le secteur privé qu'importe que le traitement soit automatisé ou pas. Elle s'applique au traitement mis en œuvre par un responsable de traitement sur le territoire national ou tout lieu ou la loi sénégalaise s'applique ou quand le responsable de traitement a recours à des moyens de traitement situés sur le territoire sénégalais à

84 16808b3726 (coe.int)
85 Article 13 de la convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel

l'exclusion des moyens utilisés à des fins de transit86. Le champ d'application territorial de la loi mériterait une plus grande précision. Il n'est pas précisé notamment ce qu'il faut entendre par « recours à des moyens de traitement ».

Que faut-il entendre par données à caractère personnel au sens de la loi sénégalaise ? Au sens de la loi, les données à caractère personnel s'entendent *« toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique*[87]». Cette définition est assez restrictive particulièrement pour les données permettant l'identification d'une personne, il aurait fallu l'adjonction de l'adverbe « notamment « pour montrer que le caractère non limitatif de l'énumération.

Par traitement de données, *« : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction des données à caractère personnel*[88] ». Cette définition a été reprise par les autres pays cibles dans leurs législations.

Tout traitement doit se fonder sur une base légale. La loi a dégagé cinq bases légales [89] qui peuvent justifier un traitement de données que : le consentement[90], le respect d'une obligation légale[91], l'exécution d'une mission d'intérêt public[92], l'exécution d'un contrat[93] et la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée.

En plus de la base légale, le traitement doit obéir aux principes dégagés par la loi tels que le principe de loyauté[94], le principe de finalités,95 le principe de minimisation, le principe de conservation limitée des données et le principe de transparence[96].

La loi pose également le principe de prohibition de la collecte et du traitement de données sensibles telles de l'origine raciale, ethnique, ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée.

Les traitements de données sont soumis à l'accomplissement de formalités préalables suivant les régimes de protection édictées par la loi que sont : la déclaration, l'autorisation et l'avis. A cet effet, la loi instaure une autorité indépendante, la Commission de Protection des Données (CDP) chargée de l'application et du contrôle de conformité conformément à l'article 16 de la loi. Le décret d'application n°2008-721 du 30 juin 2008 fixe les règles d'organisation et de fonctionnement de cet organe.

86 Art 2 de la loi de 2008
87 Art 4 de la loi de 2008
88 Art 4 de la loi de 2008
89 Art 33 de la loi
90 Art 4 de la loi définit le consentement comme : toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel, accepte que ses données à caractère personnel fassent l'objet d'un traitement manuel ou électronique ; expresse signifie par écrit ou déclaration orale devant témoin
91 L'obligation légale doit être définie par le droit national en l'occurrence le droit sénégalais et doit instituer une obligation impérative de traitement des données
92 L'exécution d'une mission de service public concerne les traitements mis en œuvre les autorités publiques pour l'exécution d'une mission de service public
93 Le traitement est nécessaire à l'exécution d'un contrat entre l'organisme responsable des traitements et les personnes concernées
94 Art 34 : La collecte, l'enregistrement, le traitement, le stockage et la transmission des données à caractère personnel doivent se faire de manière licite, loyale et non frauduleuse.
95 Art 35 : les données doivent être collectées pour des finalités déterminées, explicites, légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités
96 Art 37 : Le principe de transparence implique une information obligatoire de la part du responsable du traitement portant sur les données à caractère personnel.

Conformément à la loi, des droits sont conférés à la personne concernée par le traitement de données ainsi qu'il suit : le droit à l'information[97], le droit d'accès98, le droit d'opposition[99] et le droit de rectification et de suppression[100]. A côté de ces droits, pèsent sur le responsable de traitement les obligations de confidentialité[101], de sécurité[102], de conservation[103] et de pérennité [104] . La loi pose le principe de prohibition de prospection directe basée sur l'utilisation de données personnelles d'une personne qui n'a pas exprimé son consentement. Dans le même sillage, **la loi n° 2008-08 du 25 janvier 2008 sur les activités de transactions électroniques** pose le même principe. Ce principe est assorti d'exception[105]. En tout état de cause, la prospection directe est interdite si les coordonnées valables ne sont pas indiquées au destinataire lui permettant de solliciter l'arrêt des communications sans frais autres que ceux liés à la transmission de celle-ci.

Dans le cadre du respect des droits fondamentaux, la loi de 2008 sur la protection des données à caractère personnel interdit qu'une décision de justice soit prise sur le seul fondement de traitement automatisé de données à caractère personnel destiné à évaluer les aspects de personnalité ou le profilage de la personne mise en cause. Par rapport aux SIA, sur la base de cette interdiction, le juge ne pourra pas se baser sur le seulement fondement les résultats d'un SIA permettant d'évaluer les aspects de personnalité pour prononcer une décision de justice.

La loi permet le transfert de données à caractère personnel[106], encore faudrait-il que le pays tiers assure un niveau suffisant de protection de la vie privée et des libertés fondamentales. La loi ne dit pas ce qu'il entend par niveau suffisant de protection mais on peut déduire que le pays doit assurer un même niveau de protection que celle accordée par le Sénégal.

La loi sénégalaise sur la protection des données à caractère personnel mériterait une révision pour s'adapter aux technologies émergentes qui ont un impact fort sur la vie privée. A l'état actuel, la loi sénégalaise pose certes, le cadre juridique de protection de données à caractère personnel, mais ce cadre prend moyennement en compte les enjeux liés aux SIA.

Dans le cadre du respect des données à caractère personnel, **la loi n° 2012-03 du 03 janvier 2012 modifiant et complétant la loi n° 2004-21 du 21 juillet 2004** sur les activités statistiques, poses-en son article 6 la confidentialité des données individuelles recueillies. A ce titre, les services et organismes producteurs de statistiques publiques doivent s'assurer lors de la publication ou de la transmission à des tiers des résultats statistiques de ces opérations, qu'aucune identification directe ou indirecte des personnes physiques ou morales concernées n'est possible.

Comme précédemment dit, le **Bénin** a opéré une véritable révolution juridique avec **la loi n° 2017-20 portant Code du Numérique**. S'inspirant largement du Règlement général de protection des données à caractère personnel (RGPD) de l'Union Européenne, considéré comme le texte de référence en matière de protection des données personnelles, le livre 5 du code du numérique abroge et remplace les dispositions de la loi de 2009-09 du 22 mai 2009.

Le livre 5 rappelle les principes fondamentaux qui sous-tendent la protection des données à caractère personnel notamment le rôle de l'informatique qui doit être *« au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques[107]".* Ce principe fondamental peut être transposé aux SIA. Reprenant presqu'in extenso la définition posée par le RGPD, le code du numérique donne une définition très large des données à caractère personnel considérées comme *« toute information de quelque nature que ce soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable, ci-après dénommée personne concernée. Est réputée identifiable, une personne qui peut être identifiée, directement ou indirectement notamment par*

97 Art 58 à Art 61 de la loi 2008
98 Art 62 à Art 67 de la loi 2008
99 Art 68 de la loi de 2008
100 Art 69 de la loi de 2008
101 Art 70 de la loi de 2008 sur la protection des données à caractère personnel
102 Art 71 idem
103 Art 72 idem
104 Art 73 idem
105 Art 16 idem
106 Art 49 idem
107 Art 379 du Code de numérique

référence à un identifiant, tel un prénom ou un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique [108]».

Le dispositif légal couvre un champ d'application très large. Le livre 5 s'applique au traitement automatisé tout ou partie et non automatisé de données contenues ou appelées à figurer dans un fichier effectué par une personne physique, l'Etat, les collectivités locales et les personnes morales de droit public ou droit privé ainsi qu'au traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou de la sureté et les intérêts essentiels de l'Etat[109]. En plus de ce champ matériel large, le livre 5 du code du numérique couvre sur un champ territorial large et s'applique sur le traitement des données effectués dans le cadre des activités d'un responsable de traitement sur le territoire Béninois qu'importe le lieu de traitement. L'établissement du responsable de traitement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable tel que succursale, filiale. Le livre 5 est susceptible de s'appliquer lorsque le responsable de traitement offre des biens et des services aux personnes concernées se trouvant sur le territoire béninois, qu'un paiement soit exigé ou pas, en cas de suivi du comportement dans la mesure où il s'agit d'un comportement ayant lieu dans le territoire béninois et enfin lorsque le traitement est mis en œuvre dans le territoire d'un Etat membre de la CEDEAO.[110]

Comme prévu dans la loi sénégalaise, tout traitement de données à caractère personnel doit se fonder sur une base légale au sens de la loi béninoise. Le livre 5 prévoit également cinq bases légales : le consentement[111], le respect d'une obligation légale, l'exécution d'une mission d'intérêt public, l'exécution d'un contrat et la sauvegarde de l'intérêt ou des droits fondamentaux. Par ailleurs, tout collecte, traitement doit obéir aux différents principes dégagés par la loi que sont : le principe de finalité, le principe de minimisation, le principe de conservation limitée des données,[112] le principe de transparence[113], le principe de confidentialité et de sécurité[114]. La loi béninoise autorise le transfert de données à caractère personnel sous réserve que le pays tiers assure un niveau équivalent. Concernant le niveau de protection, la loi donne un faisceau d'indices sur lesquels on peut se baser. Il s'agit notamment du respect des droits et libertés fondamentales garanti par une loi, l'existence d'organe de contrôle du respect de la protection des données à caractère personnel et les engagements internationaux souscrits en la matière.

La loi prohibe la prospection directe par l'utilisation des données personnelles sans consentement et qu'une décision en justice ait pour fondement le traitement automatisé de données notamment le profilage.[115] Le traitement des données est également soumis à l'accomplissement de formalités préalables suivant soit le régime de déclaration[116], soit de l'autorisation[117] devant l'Autorité de protection des données à caractère personnel (APDP) chargée de la conformité et du contrôle de la loi conformément à ses missions prévues à l'article 483 de la loi. Cette dernière peut également émettre des avis.

Par ailleurs, la loi prévoit l'obligation pour le responsable de traitement de designer un délégué à la protection des données notamment lorsque soit le traitement est fait par un organisme public, soit en raison de la

108 Art 1 du Code du Numérique
109 Art 380 du Code du numérique
110 Art 381 du Code du Numérique
111 Au sens du livre 5, le consentement est défini comme toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire, conventionnel accepte par une déclaration ou un acte positif clair que les données à caractère personnel le concernant fassent l'objet de traitement
112 Art 383 : Les données à caractère personnel doivent être : 1. traitées légitimement ; 2. collectées, enregistrées, traitées, stockées et transmises de manière licite, loyale, transparente et non frauduleuse ; 3. collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicable. Adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ; 5. exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prises afin que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ; 6. conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées. Les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 396, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par les dispositions du présent Livre afin de garantir les droits et libertés de la personne concernée ;
113 Art 384
114 Art 385
115 Art 400 à Art 401
116 Art 405
117 Art 407

quantité de données à traiter, ou bien le traitement exige un suivi régulier.

Les obligations importantes pèsent sur le responsable de traitement de données. Il s'agit en autre de l'obligation d'information envers la personne concernée par le traitement particulièrement en cas d'existence d'une décision automatisée y compris le profilage. Ces informations doivent notamment porter sur la logique sous-jacente du système ainsi que l'importance des donnés et les conséquences prévues.[118]

Appliquer aux SIA, le responsable de traitement utilisant le système d'intelligence artificielle doit informer la personne concernée de la logique des algorithmes. Le responsable de traitement doit également informer la personne concernée de son intention de traitement ultérieur des données pour une autre finalité que celle prévue lors de la collecte. Cela signifie qu'un traitement ne doit concerner qu'une finalité. Ainsi si le responsable de traitement à travers un SIA utilise des données aux fins d'apprentissage de la machine, apriori, il ne pourrait pas utiliser ses mêmes données en phase opérationnel sans consentement de la personne concernée.

Outre l'obligation d'information, incombent également au responsable de traitement, les obligations de confidentialité[119] et de sécurité[120], de conservation[121] et de pérennité[122]. Le Responsable de traitement est également tenu de tenir un registre des activités effectuées sous responsabilité. Cette obligation pèse également sur les sous-traitants.

De plus, avec l'apparition des nouvelles technologiques, comme l'intelligence artificielle qui peut avoir un fort impact sur les droits fondamentaux et les libertés physiques, le responsable est tenu de faire une analyse d'impact notamment en cas d'évaluation systématique et approfondi d'aspects personnels concernant les personnes physiques fondée sur un traitement automatisé, y compris le profilage, la surveillance système à grande échelle d'une zone accessible au public[123]. Si l'analyse d'impact montre que le traitement de données présenterait un risque élevé non pris en compte par le responsable de traitement, ce dernier doit impérativement consulter préalablement au traitement l'APDP.

A côté des obligations du responsable, des droits ont été conférés par la loi aux personnes concernées par le traitement. Ces droits sont les suivants : le droit d'accès[124], le droit à la portabilité des données[125], droit d'interrogation[126], droit d'opposition[127], droit de rectification et de suppression,[128] le droit à l'oubli[129], le droit d'introduire une réclamation auprès de l'APDP, le droit à un recours juridictionnel et droit à réparation.

La loi prévoit des sanctions administratives et pénales très lourdes en cas de violation des dispositions légales. A cet effet, l'APDP peut procéder à un avertissement ou une mise en demeure avant de prononcer des sanctions pécuniaires pouvant aller de Cinq millions à Cent millions de FCFA. De plus, l'APDP peut prononcer d'autres sanctions comme une injection de cessation de traitement, un retrait défini ou temporaire d'autorisation de traitement ou un verrouillage des données. Ces sanctions administratives sont sans préjudice des sanctions pénales prévues par la loi.

Le Bénin dispose d'un cadre juridique moderne et très protecteur à l'égard des données à caractère personnel. Ce cadre prend largement en compte les technologies émergentes comme l'IA notamment les effets négatifs qui peuvent en résulter sur les droits des personnes et les libertés fondamentales.

La Côte d'Ivoire s'est également dotée d'un cadre législatif de protection des données à caractère personnel **avec la loi n° 2013-450 du 19 juin 2013**. Au sens de cette loi, on entend par données à caractère personnel « *toute information de quelque nature que ce soit et indépendamment de son support y compris le son et l'image relative à une personne physique identifiée ou identifiable directement ou indirectement par référence*

118 Art 415
119 Art 425
120 Art 426
121 Art 433
122 Art 434
123 Art 428
124 Art 434
125 Art 437
126 Art 438
127 Art 439
128 Art 440
129 Art 441

à un numéro d'*identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique,* génétique*, psychique, culturelle, sociale ou* économique [130]».

En comparaison avec la définition béninoise, celle ivoirienne est moins large. Comme pour la loi sénégalaise, il aurait fallu l'insertion de l'adverbe « *notamment* » avant de débuter l'énumération. Toutefois, la définition posée par la loi ivoirienne est plus large que celle donnée par la loi sénégalaise dans la mesure où elle inclut dans la catégorie des données à caractère personnel tout ce qui est son et images tels que comme les audio et vidéos. Concernant le champ d'application, cette loi s'applique à tout traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier mis en œuvre sur le territoire national par une personne physique, l'Etat, les collectivités territoriales et les personnes morales de droit public ou droit privé ainsi que le traitement de données concernant la défense, la recherche et la poursuite d'infractions pénales ou la sureté de l'Etat entre également dans le champ d'application de la loi[131]. L'application territoriale de la loi semble exclure les traitements effectués hors du territoire ivoirien sur des personnes se situant dans le territoire.

A l'instar du Sénégal et du Bénin, la loi ivoirienne conditionne le traitement de données personnelles à l'accomplissement de formalités préalables suivant les régimes de protection suivants : la déclaration[132], l'autorisation[133] et l'avis[134]. Ces formalités sont adressées à l'Autorité de protection des données chargée de la conformité et d'assurer que l'usage des TICS ne porte atteinte aux libertés et la vie privée, en l'occurrence l'Autorité en charge de la Régulation des télécommunications et des technologies de l'information et de la Communication (ARTCI). Les modalités relatives aux dépôts des formalités sont régies par le Décret n° 2015 -79 du 04 Février 2015. La loi accorde des pouvoirs de sanctions à cette autorité telles que l'avertissement, la mise en demeure, l'interruption de mise en œuvre de traitement, le verrouillage des données, le retrait provisoire et définitif de l'autorisation et de sanction pécuniaire dont le montant ne peut excéder dix millions. En cas de récidive dans les cinq ans, la sanction pécuniaire est portée au maximum à 100.000.00 FCFA ou s'agissant d'une entreprise, 5% du chiffre d'affaires dans la limite de 500.000.000 FCFA. Aux termes de l'article 12 de la loi, le responsable de traitement doit désigner un correspondant à la protection disposant des qualités requises qui sera l'interlocuteur sur toutes les questions relatives au traitement de données effectués. A ce titre, il est tenu de tenir un registre des traitements.

La loi exige une base légale pour tout traitement de données à caractère personnel. Les bases légales prévues par la loi ivoirienne sont les mêmes prévues par les lois sénégalaise et béninoise sur la protection des données. De plus, tout traitement doit être guidé par les principes suivants : le principe de finalité ; le principe de minimisation, le principe de conservation limitée des données[135], le principe de transparence[136], le principe de confidentialité[137]. Sous peine de sanctions pénales pouvant aller de dix à vingt ans d'emprisonnement et d'une amende de vingt millions à quarante millions, le traitement de données sensibles (origine raciale, ethnique, filiation, vie sexuelle, données génétiques …) est interdit. Cette interdiction est assortie d'exceptions prévues à l'article 21 de la loi. Il en est de même pour la prospection directe sans consentement préalable de la personne concernée[138]. En ce sens, **la loi 2013-546 du 30 juillet 2013 relative aux transactions électroniques** dans le cadre de la publicité électronique, la loi ivoire proscrit sous peine de sanction pénale d'un à cinq et d'une amende d'un million à dix millions, la prospection directe par envoi de message au moyen d'automate d'appel ou d'émission de sms, télécopieur, courrier électronique, ou tout autre moyen de communication électronique utilisant sous quelque forme que ce soit les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes[139]. Néanmoins, la prospection directe est autorisée si les coordonnées du destinataire sont recueillies en toute connaissance de cause directement auprès de lui ou si la prospection est adressée aux abonnés ou clients d'une personne physique ou morale qui a recueilli les coordonnées en tout état de cause pour des produits ou services analogues. Tout comme la loi sénégalaise, la loi ivoirienne impose l'indication de coordonnées

130 Art 1
131 Art 3
132 Art 5
133 Art 6
134 Art 9
135 Art 16
136 Art 18
137 Art 19
138 Art 22
139 Art 14

valables pour permettre aux destinataires de s'opposer à la réception de la prospection.

La loi de 2013 de la Côte d'Ivoire sur la protection des données à caractère personnel pose également le principe d'interdiction de prise de décision de justice, administrative basée uniquement sur le traitement automatisé des données à caractère personnel destiné à évaluer les aspects de la personnalité ou définir un profil[140].

Le transfert de données à caractère personnel vers un pays tiers est autorisé par la loi sous réserve que le ce pays assure un niveau de protection supérieur ou équivalent de la vie privée[141].

Concernant les droits accordés aux personnes concernées par la loi, ils ne diffèrent pas beaucoup de ceux accordés par la loi sénégalaise et béninoise. On retrouve le droit d'accès[142], le droit à l'information, le droit d'opposition,[143] le droit de rectification et suppression[144], le droit à l'oubli[145], le droit à la portabilité des données[146]. Corolairement aux droits accordés aux personnes concernées par le traitement, pèsent sur le responsable de traitement des obligations d'information,[147] de confidentialité[148] et sécurité. A ce titre, il est tenu de tenir un rapport annuel pour le compte de l'autorité de protection[149].

La loi ivoirienne sur la protection des données à caractère personnel a le mérite de poser le cadre juridique de la protection des données à caractère personnel. Toutefois, datant de 2013, ce cadre connait des limites dans la prise en compte des effets découlant de l'utilisation des technologies émergentes comme les SIA. Une révision de la loi s'avère être nécessaire.

Avec la loi n°10-2004/AN du 20 avril 2004, **le Burkina Faso** fut l'un des pays de la région ouest africaine à disposer d'un cadre légal pour la protection des données à caractère personnel. Mais, avec le développement technologique, cette loi a montré ses limites dans la protection efficace des données à caractère personnel. Suite à son adhésion à la convention 108 sur la protection des données à caractère personnel, le Burkina a modifié son cadre légal pour s'aligner aux standards internationaux avec **la loi n°001-2021/AN du 30 mars 2021 portant protection des personnes à l'égard du traitement des données à caractère personnel**.

Visant à protéger les droits et libertés fondamentaux des personnes physiques en matière de traitement de leurs données à caractère personnel, cette loi s'applique aux traitements de données à caractère personnel contenues ou appelées à figurer dans un fichier, automatisés en tout ou en partie, ainsi qu'aux traitements non automatisés de données à caractère personnel et aux traitements de données à caractère personnel relatives aux communications électroniques. La loi a également vocation à s'appliquer lorsque le responsable de traitement est établi sur le territoire burkinabé ou s'il est établi hors du territoire met en œuvre des opérations de traitement sur le territoire national à l'exclusion des données de transit[150].

La définition de la notion de donnée à caractère personnel se rapproche de celle posée par la loi ivoirienne et sénégalaise. Ainsi au sens de la loi, les données à caractère personnel « *toutes informations relatives à une personne physique identifiée ou identifiable directement ou indirectement notamment par référence* à un ou des éléments propres à son identité physique*, physiologique, génétique psychique, culturelle, sociale et économique* [151]». La loi burkinabé n'inclut pas expressément le son et l'image comme la loi ivoirienne ou béninoise.

La loi de 2021 pose le principe du respect des droits fondamentaux en ce sens où les TIC doivent être au service de la personne humaine et ne doivent pas porter atteinte ni à l'identité humaine, ni à la vie privée et aux libertés individuelles et collectives.

140 Art 25
141 Art 26
142 Art 29
143 Art 31
144 Art 33
145 Art 35
146 Art 38
147 Art 41
148 Art 39
149 Art 40
150 Art 3
151 Art 5

Partant de ce principe fondamental, la loi est guidée par les principes directeurs suivants :

- Le principe de transparence caractérisé par l'information, le consentement et la mise en place de régime de protection avec l'accomplissement de formalités préalables (avis, autorisation, déclaration[152]) ;
- Le principe de finalité, de pertinence et de proportionnalité des données traitées ;
- Le principe de conservation des données ;
- Le principe de sécurité et de confidentialité.

En outre, tout traitement doit se baser une base légale. La loi burkinabé ne fait pas dans l'originalité et pose presque les mêmes bases légales prévues dans les lois sénégalaise, ivoirienne et béninoise[153].

La loi interdit également la prospection directe sans consentement par l'utilisation de données caractère personnel et la prise de décision de justice basé sur le traitement automatisé de données donnant une définition de profil ou de la personnalité de la personne concernée[154]. De plus, **la loi n° 045-2009/AN du 10 novembre 2009, le Burkina Faso adopté un cadre juridique relatif aux transactions électroniques** proscrit également de la prospection directe sous réserve des exceptions légales[155].

La loi burkinabé sur la protection des données à caractère personnel accorde des droits également aux personnes concernées par le traitement. Ces droits sont relatifs à l'information[156], l'accès[157], la contestation[158], l'opposition[159], rectification[160] et le droit à l'oubli[161]. Concernant le droit de contestation, le législateur burkinabé apporte une innovation de taille en faisant référence explicitement à l'intelligence artificielle. Ainsi selon l'article 19 de la loi, « *toute personne a le droit de connaitre et de contester les informations et les raisonnements utilisés dans les traitements automatisés ou non dont les résultats lui sont opposés et lors que cela relève de l'IA, les critères et la nature des données à caractère personnel fondant le traitement qui lui sont indiqués dès la collecte* ».

En d'autres termes, en cas d'utilisation de SIA, il faut indiquer dès la collecte, les critères et la nature des données collectées à la personne concernée ainsi que le raisonnement utilisé par l'algorithme pour lui permettre de le contester.

A cela s'ajoute, L'article 31 al 7 soumet à l'autorisation de la CIL « *les traitements d'aide à la décision administrative ou privée, impliquant une appréciation sur un comportement humain, donnant une définition du profil ou la personnalité de l'intéressé ou reposant sur des techniques d'intelligence artificielle à des fins prédictives* ».

En outre la loi pose le principe de la désignation facultative par le responsable de traitement d'un délégué à la protection des données à caractère personnel chargé de contrôler la conformité aux obligations légales.[162] Le transfert de données vers un pays tiers est autorisé si ce dernier assure un niveau adéquat de protection.

A noter que la loi de 2021 a élargi les pouvoirs et attributions de l'autorité en charge de la conformité et de l'application de la loi, la Commission de l'Informatique et des Libertés (CIL) qui peut désormais prononcer des sanctions administratives dont l'amende forfaitaire[163]. Ces sanctions administratives sont toutefois sans préjudice des sanctions pénales.

Par ailleurs, **la loi n° 012-2007/ AN Du 31 mai 2007 sur les activités statistiques** pose le secret statistique et au secret professionnel. En ce sens, les organismes relevant du système national de statistique sont tenus

152 Art 26
153 Art 13
154 Art 14 et Art 15
155 Art 49
156 Art 16
157 Art 17
158 Art 19
159 Art 20
160 Art 22
161 Art23
162 Art 29
163 Art 63 : la CIL peut prononcer à l'encontre des contrevenants, sans préjudices des poursuites pénales des sanctions administratives : avertissement, mise en demeure, injonction de cesser le traitement, le verrouillage de certaines données à caractère personnel, l'amende forfaitaire et le retrait d'autorisation

à la confidentialité à l'égard des données individuelles recueillies. Ces données ne pourront être divulguées en aucune manière sans autorisation explicite accordée par les personnes concernées.

La loi burkinabé sur la protection des données à caractère personnel constitue une avancée significative et prend en compte de manière explicite les technologies de l'IA. Mais, législateur burkinabé aurait pu aller plus loin dans la réforme pour davantage protéger les données personnelles face aux enjeux des systèmes d'IA et des technologies émergentes en imposant des analyses d'impact par exemple pour le traitement ayant de risques très élevés sur la vie privée.

En définitive, seul le Bénin parmi les pays cibles dispose d'un cadre propice à la régulation de l'IA.

iii. La protection des droits fondamentaux-Non-discrimination-Equité

L'un des risques les plus récurrents qui pourrait survenir avec le SIA est la reproduction de biais conduisant à la discrimination avec comme conséquence la rupture de l'équité ou d'égalité. En effet, les données utilisées pour les SIA ne sont que la représentation de la réalité et constitue le produit d'un arbitrage humain. En ce sens, elles ne sont jamais objectives et constituent la résultante des choix opérés par une personne. Ces choix pouvant être conditionnés par diverses considérations [164] aboutissant à la reproduction de biais discriminatoire. Imaginons qu'un modèle de présélection à de logements sociaux comme le programme de 100.000 logements piloté par le gouvernement sénégalais soit entrainé sur la base des décisions humaines discriminatoires en faveur des hommes. Ce modèle risque de produire des résultats discriminatoires en faveur des hommes et permettra à ces derniers d'avoir accès de manière favorable aux logements même si les femmes remplissent les mêmes critères.

La non-discrimination est un droit fondamental garanti par l'article 2 de la Déclaration universelle des droits de l'homme qui dispose que « ***Chacun peut se prévaloir de tous les droits et de toutes les libertés proclamées dans la présente Déclaration, sans distinction aucune, notamment de race, de couleur, de sexe, de langue, de religion, d'opinion politique ou de toute autre opinion, d'origine nationale ou sociale, de fortune, de naissance ou de toute autre situation*** ». Ce principe est réaffirmé par l'article 2 de la Charte africaine des droits de l'homme et des peuples en les termes suivants : « ***Toute personne a droit à la jouissance des droits et libertés reconnus sans distinction aucune notamment de race, d'ethnie, de couleur, de sexe, de langue, de religion, d'opinions politiques…***. »

Au niveau national, le Sénégal réaffirme dans le préambule de sa constitution son adhésion à la déclaration universelle des droits de l'homme et à la charte africaine des droits de l'homme et du peuple. La constitution sénégalaise pose en son article 7 le principe d'égalité entre homme et femme. De plus, la loi d'orientation de la société de l'Information n° 2008-10 du 25 janvier 2008 prévoit en son article 3 que « *la société de l'information est une société à dimension humaine, inclusive et solidaire, ouverte, transparente et sécurisée, qui œuvre en vue de l'accélération du développement économique, social ainsi que culturel, de l'élimination de la pauvreté et de la modernisation de l'Etat* ». A cela s'ajoute l'article 6 de ladite loi qui dispose que « *le principe de sécurité des systèmes de la société de l'information garantit les droits fondamentaux des personnes et les droits sur les biens et sauvegarde l'ordre public ainsi que les valeurs fondamentales de la société de l'information dans un environnement transparent et prévisible qui reflète la situation réelle du pays ».*

L'attachement à la Déclaration universelle des droits de l'homme et la charte africaine des droits de l'homme et des peuples est réaffirmé également dans le préambule de la constitution du Bénin[165], de la Côte d'Ivoire[166] et du Burkina Faso[167].

La constitution du Bénin affirme d'ailleurs à son article 7 que « ***Les droits et les devoirs proclamés et garantis par la Charte Africaine des Droits de l'Homme et des Peuples adoptée en 1981 par l'Organisation de l'Unité Africaine et ratifiée par le Bénin le 20 janvier 1986 font partie intégrante de la présente Constitution et du Droit béninois ».***

164 Etude préliminaire sur l'éthique de l'intelligence artificielle, SHS/COMEST/EXTWG-ETHICS AI/2019/1
165 https://cdn.accf-francophonie.org/2019/03/benin-constitution-1990.pdf
166 https://www.centif.ci/images/lois/caf6428781fcfabd787165779f7f08a0.pdf
167 https://adsdatabase.ohchr.org/IssueLibrary/BURKINA%20FASO_Constitution.pdf

L'article 396 du livre 5 du Code du numérique dispose du principe que l'informatique est au service de l'homme et qu'elle ne doit porter ni atteinte à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

L'article 1 de la constitution Burkinabé interdit *« Les discriminations de toutes sortes, notamment celles fondées sur la race, l'ethnie, la région, la couleur, le sexe, la langue, la religion, la caste, les opinions politiques, la fortune et la naissance »*. Tout comme la législation béninoise sur la protection des données à caractère personnel, la loi burkinabé de 2021 sur les données personnelles pose le principe du rôle de la société de l'information qui ne doivent ni porter atteinte à l'identité humaine, ni à la vie privée, ni aux libertés individuelles, ni aux droits humains.[168]

En résumé, comme les quatre pays cibles offrent des garanties constitutionnelles pour le respect des droits fondamentaux comme la non-discrimination, l'égalité, la protection de la vie privée. Face aux nouveaux enjeux sur les droits fondamentaux découlant des nouvelles technologies telles que le SIA, il faudra nécessairement élaborer les dispositions spécifiques pour encadrer les éventuelles dérives. Le droit accuse toujours un retard sur la technologie.

iv. Le cadre juridique relatif à la propriété intellectuelle

Tout comme en matière de données personnelles, de cybersécurité, et des droits humains, l'IA soulève des questions juridiques en matière de propriété intellectuelle. En effet, l'IA est capable de générer des créations assimilables à des créations intellectuelles qui constituent l'objet de la protection par la propriété intellectuelle. En témoigne, la vente aux enchères de plus de 400000 dollars d'un tableau dénommé « Edmond de Balamy » généré par une IA[169] ou bien la reproduction et la vente dans le metaverse des sacs physiques de Birkin de la marque Hermes[170], ou le titre de musique « Daddy's car » produite par la machine Flow machines de Sony[171], ou encore des nombreuses demandes de brevet pour des inventions générées par l'IA.

Qu'est-ce que c'est la propriété intellectuelle ? La propriété intellectuelle est définie comme l'ensemble des règles juridiques applicables aux créations intellectuelles ou immatérielles[172]. Elle se subdivise en deux branches : la propriété littéraire et artistique (PLA) communément appelée les droits d'auteurs et droits voisins qui protège les œuvres littéraires et artistiques, et la propriété industrielle regroupant le brevet, les signes distinctifs comme la marque, le dessin et modèle industriel, les noms commerciaux, les indications géographiques…, le certificat d'obtention végétale et les schémas de configuration.

Concernant la PLA, les pays cibles ont mis en place un dispositif légal protégeant les œuvres de l'esprit entendues comme toutes les créations littéraires, artistiques ou scientifiques.

Ainsi, au Sénégal, la PLA est régie par la loi n°2008-09 du 25 janvier 2008 relative aux droits d'auteurs, en Côte d'ivoire, la loi n°2016-555 du 26 juillet 2016 relative au droit d'auteur et aux droits voisins, au Burkina Faso, la loi n° 032-99 AN du 22 décembre 1999 et au Benin par la loi n°2005-30 du 05 avril 2006 relative au droit d'auteur et droits des voisins. Ces lois présentent de nombreuses similitudes en ce sens qu'elles posent les mêmes conditions de forme et de fond pour la protection. Elles octroient des droits d'ordre patrimonial et moral aux moraux et prévoient des limitations et exceptions à l'exercice de ces droits. Elles posent également des sanctions en cas d'atteinte aux droits d'auteur.

Pour bénéficier de la protection, ces lois sur le droit d'auteur posent l'exigence d'une mise en forme ou d'une matérialisation pour qu'une œuvre puisse bénéficier de la protection. La simple idée sans expression perceptible est exclue de la protection[173]. Cela signifie qu'il faut que l'idée de départ de l'auteur soit exprimée d'une façon ou d'une autre. Or, à priori, l'IA qui constitue une machine n'a pas en soi d'idée comme un humain pourrait l'avoir. Par conséquent, l'œuvre générée par l'IA ne provenant pas d'idée précise de la machine ne saurait bénéficier de la protection par le droit d'auteur au sens de ces lois précitées.

168 Art 6 de la loi n°001-2021/ AN du 30 mars 2021 portant protection des personnes à l'egard du traitement des données à caractere personnel
169 https://newconceptartphotoselling.com/blog/23159-laffaire-du-portrait-dedmond-bellamy/
170 https://www.journalduluxe.fr/fr/business/decision-metabirkin-revolution-droit-nfts-anna-klein
171 https://siecledigital.fr/2016/09/29/daddys-chanson-realisee-ia-style-beatles/
172 https://www.dictionnaire-juridique.com/definition/propriete-intellectuelle.php
173 Voir l'article 5 de la loi 2016-555 du 26 juillet 2016 (Cote d'ivoire), l'article 3 de la loi 032-99 AN du 22 décembre 1999 (Burkina Faso), l'article 2 de la loi 2008-09 du 25 janvier 2008 (Sénégal) et article 2 de la loi 2005-30 du 05 avril 2006 (Benin)

De surcroit, pour qu'une œuvre puisse bénéficier des droits d'auteur, il faut nécessairement qu'elle soit originale. C'est une condition de fond. Au titre des lois sur le droit d'auteur des pays cibles, l'originalité de l'œuvre s'entend de l'empreinte de la personnalité de l'auteur. En d'autres termes, il faut que l'œuvre porte la marque ou le reflet de l'auteur. Pour l'œuvre générée par l'IA, cette condition est difficilement réalisable dans la mesure où la machine ne peut pas être considérée comme un humain. De plus, les lois sur les droits d'auteur des pays cibles considèrent comme auteur d'une œuvre « la personne physique ayant créée une œuvre »[174]. La conséquence est que l'IA étant une machine ne saurait bénéficier de la qualité de l'auteur.

La conclusion est qu'à l'état actuel des législations sur le droit d'auteur au niveau des pays cibles, pour qu'une œuvre générée par l'IA puisse bénéficier de la protection, il faut démontrer l'intervention humaine ayant abouti à la création de l'œuvre à l'aide de la machine[175].

Les lois sur les droits d'auteurs octroient aux auteurs des droits de propriété qui sont deux ordres : les droits patrimoniaux et les droits moraux. Les seconds qui sont rattachés à la personne de l'auteur ont un caractère inaliénable, imprescriptible et perpétuel. Ces droits sont constitués du droit à la paternité et au respect de l'œuvre, du droit à la divulgation et droit de repentir. Il serait inconcevable à l'état du droit positif au niveau des pays cibles, que ces droits qui sont d'essence humaine, puissent être octroyés à une machine.

Relativement à la propriété industrielle, elle est régie par l'Accord de Bangui instituant l'Organisation africaine de la propriété intellectuelle (OAPI) de 1977 révisé en 1999 et en 2015. Cet accord comporte dix annexes qui portent chacune à l'exception de l'annexe 8[176], sur un droit de propriété intellectuelle. Cet accord constitue la loi nationale de ses Etats membres y compris les quatre pays cibles.[177] Dans le cadre de cette étude, nous n'aborderons que l'annexe 1 de l'accord relative au brevet d'invention. En effet, depuis quelques années, il est constaté l'émergence de demande de brevet en lien avec l'IA dans le monde. Ainsi, se dessinent de nombreux enjeux sur la question du brevet dans le domaine de l'IA. Ces questions portent de manière non limitative sur la protection par le brevet de la technologie de l'IA et de l'invention générée par l'IA.

Sur la question de la brevetabilité de l'IA, l'article 1-3 de l'Annexe 1 de l'Accord de Bangui révisé ne considère pas comme des inventions les découvertes, les théories scientifiques, les méthodes, mathématiques, les programmes d'ordinateurs etc. Or, les algorithmes de l'IA sont généralement assimilés aux formules mathématiques ou à des programmes d'ordinateur[178]. Sur la base de l'article précité, la demande de brevet portant sur l'IA en tant qu'algorithme ou programme d'ordinateur ne pourrait donc pas aboutir. Toutefois, la technologie IA peut être protégée par le brevet à condition qu'elle puisse produire un effet technique c'est-à-dire qu'elle soit utilisée pour une application technique[179].

La protection des inventions générées par l'IA soulève également plusieurs problèmes juridiques. Le premier porte sur la qualité d'inventeur de l'IA. Si le législateur OAPI dans l'article 1 de l'Annexe 1 de l'Accord de Bangui Révisé a pris le soin de définir l'invention comme étant « une *idée qui permet dans la pratique la solution d'un problème particulier dans le domaine de la technique* »[180], il n'en a pas fait de même pour l'inventeur. Il se borne à dire à l'article 9 alinéa 1 de l'Annexe 1 a que l'inventeur est le titulaire du brevet à l'article 9. Toutefois, à la lecture de l'alinéa 2 du même article, il ressort que le législateur attribue la qualité d'inventeur à la personne disposant d'une capacité juridique. Par conséquent, l'IA étant une machine ne pourrait recevoir la qualité d'inventeur. Cette vision est partagée par plusieurs pays. Dans la saga DABUS, l'Office Européen des Brevets (OEB) a refusé de conférer la qualité de l'inventeur à l'IA DABUS[181]. Actuellement, seul l'Afrique du Sud a franchi le pas en acceptant de considérer comme inventeur l'IA DABUS dans la demande de brevets[182].

Le second point concerne les critères de brevetabilité de l'invention. L'article 2 de l'annexe 1 de l'Accord de Bangui Révisé prévoit que l'invention ne peut faire l'objet de brevet que si elle est nouvelle, qu'elle

174 Voir les lois précitées à l'article 1 et 12 des lois précitées
175 Et si Terminator devenait artiste, Erwin SOTIRI, Ruben Mendes, éditions légitech
176 Cette annexe porte sur la concurrence déloyale
177 L'OAPI compte 17 états membres : Bénin, Burkina Faso, Cameroun, Centrafrique, Comores, Congo, Côte d'Ivoire, Gabon, Guinée, Guinée Bissau, Guinée Equatoriale, Mali, Mauritanie, Niger, Sénégal, Tchad, Togo
178 Intelligence artificielle et Brevets, Camille AUBIN, 2018
179 https://www.ieepi.org/paroles-dexperts-protection-brevet-des-inventions-intelligence-artificielle/
180 Article 1 de l'Annexe 1 de l'Accord de Bangui Révisé
181 https://www.ipsilon-ip.com/dabus.html
182 https://www.planeterobots.com/2021/10/18/dabus-la-qualite-dinventeur-reconnue-

implique une activité inventive et qu'elle est susceptible d'une application industrielle. Si les conditions de nouveauté et d'application industrielle ne posent pas en principe de difficulté, il en est autrement pour l'activité inventive. Le critère de l'activité inventive suppose que l'invention ne soit pas évidente par rapport à l'état de la technique pour un homme du métier ayant des connaissances et une habilité moyenne[183]. Le critère de non évidence renvoie aux activités humaines inventives[184] et non aux activités d'une machine. Ainsi, pour une invention générée par l'IA, la référence à l'homme du métier risque de soulever des difficultés concernant l'examen de l'activité inventive.

Par ailleurs, il ressort que l'IA se fonde sur des données pour créer des œuvres ou générer des inventions au moyen de technique telle que l'apprentissage automatique. Ces données d'entrainement peuvent constituer des œuvres protégés par le droit d'auteur ou des inventions protégées par le brevet. L'utilisation de telles données sans autorisation peuvent constituer des atteintes aux droits de propreté intellectuelle du titulaire.

Malheureusement, ces questions sont peu prises en charge par le cadre législatif existant dans les pays cibles aussi bien en droit d'auteur qu'en matière de propriété industrielle.

Pour conclure, les quatre pays cibles disposent de législation en matière de propriété intellectuelle qui protège l'innovation et la création. Toutefois, ce cadre prend en compte insuffisamment les problématiques de l'IA. Il s'avère nécessaire de réviser le cadre juridique plus particulièrement les lois sur la propriété littéraire et artistique en vigueur afin de prendre en compte ses nouveaux enjeux soulevés par l'IA en particulier l'IA générative

B. Limites du cadre juridique existant dans l'appréhension de l'IA et ses effets

i. Faiblesse du cadre juridique en vigueur dans l'encadrement de l'IA

Le cadre juridique lié aux technologies émergentes, l'IA et données existant dans les pays cibles a montré ses limites.

En effet, en matière de protection à caractère personnel, à part le Bénin qui dispose d'un cadre protecteur et très avant-gardiste dans le contexte ouest africain et du Burkina Faso qui a opéré une révision législative en 2021, des limites subsistent dans les lois sur la protection des données à caractère personnel du Sénégal et de la Côte d'Ivoire pour prendre en compte les enjeux importants liés aux atteintes aux droits de la vie privée comme l'obligation d'information sur le modèle algorithmique utilisé en cas de traitement de données automatisées ou bien l'obligation d'analyse d'impact en cas de traitement de données susceptible d'avoir un fort impact sur les droits fondamentaux.

Par ailleurs, l'autre faiblesse constatée est le manque de moyens des autorités de protection des données personnels pour assurer pleinement leur mission de veille, de contrôle de conformité et de sanction. Au Sénégal par exemple des acteurs que ce soit public comme privé continuent de collecter des données personnelles en dehors de tout accomplissement de formalités préalables sans encourir aucune sanction parce que l'autorité de protection n'a pas assez de moyens pour faire des opérations de contrôle et de vérification. Il est nécessaire d'avoir dans nos pays des autorités de protection à l'image de la CNIL (Commission nationale informatique et Libertés) de la France qui a récemment condamné la société CLEARVIEW IA qui aspirait des photographies provenant de nombreux sites web dont les réseaux sociaux pour offrir cette base de données aux services de police afin d'identification des auteurs et victimes d'infractions. L'enquête de la CNIL suite à des plaintes a permis de constater que cette société faisait le traitement illicite sans base légale et ne prenait pas en compte de manière effective les droits des personnes. Ainsi après une mise en demeure resté infructueuse, la société CLEARVIEW a été condamnée à vingt millions d'euros d'amende sous astreinte.[185]

Par ailleurs, il se pose également une méconnaissance de la législation des données à caractère personnel par la population. Les autorités de protection devraient dans le cadre de leur mission, accentuer les opérations de sensibilisation.

183 Article 4 de l'annexe 1 de l'Accord de Bangui révisé

184 Dialogue de l'OMPI sur la propriété intellectuelle et l'intelligence artificielle, Organisation mondiale de la Propriété intellectuelle (OMPI), décembre 2020, https://www.wipo.int/edocs/mdocs/mdocs/fr/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1_rev.pdf

185 https://www.cnil.fr/fr/reconnaissance-faciale-sanction-de-20-millions-deuros-lencontre-de-clearview-ai

Dans le cadre de la cybersécurité, bien que le cadre juridique en place s'adapte aux SIA, l'absence de mise en place d'autorité de contrôle demeure une faiblesse notamment pour certains pays. Le choix politique peut être le renforcement des pouvoirs des autorités de protection des données ou la mise en place d'un organe dédié.

Concernant la lutte contre les biais générés par le SIA, le cadre juridique en vigueur ne nous semble peu efficace pour y lutter. Il faudrait élaborer des dispositions spécifiques pour encadrer ses dérives.

Sur la question la propriété intellectuelle, il est nécessaire de réviser le cadre juridique en vigueur pour intégrer les nouveaux enjeux soulevés par l'IA afin de mieux encadrer les atteintes aux droits de propriété intellectuelle.

ii. Réglementation insuffisante en matière d'ouverture des données publiques

Les données publiques ouvertes renvoient aux informations que les organismes publics recueillent, produisent ou achètent et qui sont mises à disposition gratuitement en vue de les réutiliser à d'autres fins. Toutefois, l'ouverture de données publiques n'est pas totalement une réalité dans les quatre pays. En effet, seules certaines catégories de données publiques sont amenées à être publiées. Il s'agit notamment des données statistiques et des données environnementales.

La loi sénégalaise n°2012-03 du 03 janvier 2012 modifiant et complétant la loi n°2004-21 du 21 juillet 2004 sur les activités statistiques en son article 5 pose le principe d'accès à titre gratuit ou onéreux par tout utilisateur aux informations traitées dès leur disponibilité.

L'article 5 de **la loi ivoirienne n°2013-537 du 30 juillet 2013 portant organisation et fonctionnement du système de statistique** pose le principe de l'ouverture des données statistiques.

Outre les données statistiques, **l'article 77 de la burkinabé 045-2009 du 10 novembre 2009 sur les transactions électroniques,** dispose que l'administration publique veille à ce que tous les documents relatifs à l'environnement soient mis à la disposition du public dans la mesure du possible par voie électronique.

Cependant, l'administration détient une quantité de données importantes pas nécessairement statistiques, qui doivent être mises à la disposition de tous. L'ouverture de toutes les données de l'administration doit être un gage de transparence administrative et de bonne gouvernance. A titre d'exemple, la France a adopté en 2016 la loi pour une République numérique[186] visant à l'ouverture des données publiques et d'intérêt général et le libre accès de la recherche publique qui devient le principe et non l'exception. Sur la base de cette loi, l'Etat, les administrations publiques, les établissements publics, les collectivités locales doivent publier en ligne en mode ouvert les principaux documents qu'ils détiennent y compris les codes sources, les bases de données, et les données qui présentent un intérêt économique, social, sanitaire ou environnemental sous réserve de la vie privée et de la sécurité des systèmes d'information des administrations. La mise à disposition des données permettrait de développer une économie numérique tout en garantissant la transparence dans l'exécution de l'action publique. L'ouverture des données publiques nécessite le renforcement des autorités de protection des données personnelles pour contrôler et encadrer les éventuelles atteintes à la vie privée.

Dans le cadre de la stratégie nationale des données, le Sénégal envisage de mettre en place un cadre juridique adaptée à l'ouverture et à l'accessibilité des données et une plateforme nationale d'ouverture des données[187].

C. Nécessité de renforcement du cadre juridique pour une meilleure prise en compte de l'IA

Le cadre juridique en vigueur relatif aux SIA nécessite d'être renforcé pour qu'il soit plus efficace. Le renforcement passe par la révision des textes en vigueur notamment les lois relatives à la protection des données à caractère personnel. Parmi les lois étudiées, celles qui nécessitent une révision sont sans aucun doute la loi sénégalaise et la loi ivoirienne. En ce sens il faut noter que le Sénégal a entamé depuis 2019 une réforme en cours pour réviser ladite loi. Le nouveau projet de loi aborde les nouvelles questions telles que la biométrie, les méga données, l'intelligence artificielle et le cloud[188]. En plus de la révision des lois

186 https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-27/premiere-lecture

187 Synthèse de la Stratégie Nationale des Données du Sénégal. | Ministère de la Communication, des Télécommunications et du Numérique (numerique.gouv.sn)

188 https://cipesa.org/2020/01/le-senegal-va-reviser-la-loi-sur-la-protection-des-donnees-personnelles/

nationales, l'acte additionnel de la CEDEAO doit être également révisé pour tenir en compte ces nouvelles problématiques. Il en est de même de la Convention de Malabo.

Par ailleurs, il nous parait nécessaire d'initier une réflexion sur l'adoption d'une réglementation africaine ou communautaire spécifique à l'image du e Règlement européen sur l'IA ou le projet de loi canadienne C-27 qui comporte une loi sur l'IA. En effet, le Règlement européen sur l'IA vise à garantir les normes élevées en matière d'éthique et protection des droits fondamentaux tout en assurant le développement des SIA dans le marché européen. A ce titre, le règlement se fonde sur trois approches :

- Un champ d'application très large matérialisé par la définition des SIA proposée, la prise en compte de l'ensemble des acteurs impliqués (privés et publics) ;
- La prise en compte des risques avec l'interdiction des SIA présentant des risques trop importants à proscrire[189], des SIA à hauts risques à encadrer[190] et les SIA à risques faibles avec des exigences limitées ;
- L'exigence de transparence notamment pour l'IA générative telle le chatGPT ;
- La mise en place d'un cadre juridique favorable à l'innovation par l'adoption de bac à sables réglementaires.

Ce Règlement s'applique sans préjudice des dispositions relatives à la protection des données à caractère personnel en l'occurrence le RGPD qui demeurent applicables même si des adaptations ont été fait dans le projet de règlement[191].

Au niveau africain, l'UA peut adopter un instrument normatif pour appréhender l'IA.

Au niveau régional la CEDEAO pourrait élaborer une réglementation spécifique sur l'IA et la législation communautaire pourrait prendre la forme d'une directive ou d'un autre instrument plus contraignant sur la base des orientations déclinées par l'UA dans une perspective d'harmonisation des règles.

Pour l'élaboration de cette réglementation, des recommandations du Comité Ad hoc du Conseil de l'Europe sur l'IA peuvent constituer une source d'inspiration. Ce dernier recommande entre autres de proposer une définition des systèmes d'IA dans les législations, de mettre l'accent sur la prévention et la réduction des risques des systèmes d'IA susceptibles de porter atteinte aux droits de l'homme. Dans ce cadre, certains usages portant gravement atteinte aux droits de l'homme devraient être interdites comme la notation sociale, les programmes de surveillance de masse à des fins répressives. De plus, une analyse des risques devrait être faite de manière systématique sur certains usages de l'IA.

De plus, la Résolution sur la nécessité d'élaborer une étude sur les droits de l'homme et des peuples et l'intelligence artificielle (IA), la robotique et d'autres technologies nouvelles et émergentes en Afrique - CADHP/Rés.473(XXXI) 2021 pourrait servir de cadre de référence. En tout état de cause, cette réglementation communautaire doit être assez souple et évolutive au risque d'une obsolescence assurée face aux développements rapides des systèmes d'IA.

189 Les SIA portant sur la manipulation mentale, l'abus de faiblesse avec l'exploitation des personnes vulnérables (enfant, handicap,) le storting social c'est-à-dire la notation sociale et identification biométrique en temps réel dans les lieux publics à des fins répressives sont interdits par le règlement

190 SIA utilisés dans des certains secteurs industriels et les secteurs biométriques, environnement, éducation formation professionnelle, emploi et gestion de la main d'œuvre, accès et droit aux services privés, gestion de la migration, administration de la justice, système d'aide aux autorités répressives autorisés sous réserve de respecter un certain nombre d'obligation telles que la mise en place d'un système de gestion des risques, contrôle humain etc.

191 Traitement de données sensibles sous réserve des garanties appropriées en vue de lever tout biais du SIA

Tableau SWOT du cadre juridique lié à l'Intelligence artificielle, les données et technologies émergentes des quatre pays cibles

Forces	**Faiblesses**
• *Existence d'une législation sur la protection des données à caractère personnel avec un accent sur les technologies émergentes ;* • *Existence d'Autorités de protection des données à caractère personnel* • *Existence d'une législation sur la cybersécurité permettant la protection des technologies émergentes ;* • *Cadre juridique de protection des droits fondamentaux ;* • *Cadre juridique sur la propriété intellectuelle*	• *Faible prise en compte de certains risques de l'IA sur la protection de la vie privée et des données personnelles dans les législations sur la protection des données personnelles (Sénégal, Côte d'Ivoire)* • *Faiblesse des moyens financiers et humains des autorités de protection des données à caractère personnel* • *Absence de législation sur l'ouverture de toutes les données publiques* • *Retard dans la mise en place d'autorité de contrôle en matière de cybersécurité (Sénégal)* • *Faible protection contre les biais et les atteintes aux droits fondamentaux* • *Absence d'instrument normatif pour une IA éthique et responsable,* • *Les risques de violation des droits de propriété intellectuelle insuffisamment prises en compte par les lois sur la propriété intellectuelle*
Opportunités	**Menaces**
• *Révision des législations sur la protection des données à caractère personnel pour prendre en compte des enjeux liés à l'IA sur la vie privée dans certains pays cibles ;* • *L'ouverture des données publiques en cours de réflexion,* • *Réflexion sur une réglementation communautaire et africaine (CEDEAO, UA) sur les SIA* • *Renforcement des autorités de protection des données à caractère personnel* • *Volonté manifestée par le Sénégal et le Benin, dans leurs stratégies nationales de l'IA, de règlementer l'IA*	• *Fortes atteintes aux droits fondamentaux par l'usage des SIA ;* • *Risques de reproduction de biais discriminatoire par les SIA ;* • *Risque d'attaques cybercriminelles sur les SIA* • *Risque d'atteintes aux droits de propriété intellectuelle notamment avec l'IA générative*

4. LE CADRE ETHIQUE DE L'IA EN AFRIQUE DE L'OUEST

a. L'éthique de l'IA

Le cadre éthique de l'IA en Afrique de l'Ouest est à construire.

Certes, la Constitution des pays cibles du projet offre des garanties constitutionnelles quant au respect des droits et libertés fondamentales tels que la non-discrimination, l'égalité et le respect de la vie privée. Ces garanties bien s'appliquant aux SIA déployés, sont insuffisantes pour encadrer efficacement l'IA afin qu'elle soit responsable et au service de la société.

Par ailleurs, certains pays comme le Sénégal[192], le Benin[193] ont légiféré dans le domaine de l'éthique de la recherche en Santé. La Recherche en santé s'entend des recherches épidémiologiques, les recherches cliniques, les recherche en médecine traditionnelle et les recherches sur les systèmes de santés. Ces législations énoncent des principes éthiques dans ce domaine qui sont notamment les suivants : le consentement libre et éclairé, le respect de la dignité humaine et des droits de l'homme, le respect de l'autonomie et la responsabilité individuelle, le respect de l'intégrité physique et morale, l'égalité, la justice et l'équité, la non-discrimination et la non stigmatisation, le respect de la vie prie et de la confidentialité. Par ailleurs, tous les pays cibles du projet ont mis en place un Comité d'éthique national pour la Recherche en Santé. En principe, ces principes s'appliquent sur les SIA déployés dans ce domaine bien précis.

Au niveau international, il a été adopté le 23 novembre 2021, un instrument normatif mondial sur ce sujet : La Recommandation sur l'éthique de l'intelligence artificielle de l'UNESCO. Cette Recommandation se considère comme une boussole éthique et un socle normatif mondial destinés à protéger mais aussi à promouvoir les droits humains et la dignité humaine, en vue de l'instauration d'un solide respect de l'État de droit dans le monde.

La Recommandation a pour objet de servir de base afin de mettre les systèmes d'IA au service de l'humanité, des individus, des sociétés, de l'environnement et des écosystèmes, ainsi que de prévenir les préjudices. Elle a également pour vocation de favoriser l'utilisation pacifique des systèmes d'IA.

Les objectifs de la Recommandation sont :

(a) offrir un cadre universel de valeurs, de principes et d'actions pour guider les États dans la formulation de leur législation, de leurs politiques ou d'autres instruments concernant l'IA, conformément au droit international ;

(b) guider les actions des individus, des groupes, des communautés, des institutions et des entreprises du secteur privé afin de garantir la prise en compte de l'éthique à tous les stades du cycle de vie des systèmes d'IA ;

(c) protéger, promouvoir et respecter les droits de l'homme et les libertés fondamentales, la dignité humaine et l'équité, y compris l'égalité des genres ; protéger les intérêts des générations présentes et futures ; préserver l'environnement, la biodiversité et les écosystèmes ; et respecter la diversité culturelle à tous les stades du cycle de vie des systèmes d'IA ;

(d) favoriser un dialogue multipartite, pluridisciplinaire et pluraliste ainsi que la recherche du consensus au sujet des questions éthiques en lien avec les systèmes d'IA ;

(e) promouvoir un accès équitable aux progrès et aux connaissances dans le domaine de l'IA, ainsi que le partage des bienfaits qui en découlent, en accordant une attention particulière aux besoins et contributions des pays à revenu intermédiaire inférieur (PRITI), notamment aux PMA, aux PDSL et aux PEID.

La Recommandation comprend des valeurs et principes devant être respectés par tous les acteurs du cycle de vie des systèmes d'IA. Les **valeurs éthiques** sont : (i) Respect, protection et promotion des droits de l'homme, des libertés fondamentales et de la dignité humaine ; (ii) Un environnement et des écosystèmes qui prospèrent ; (iii) Assurer la diversité et l'inclusion, et (iv) Vivre dans des sociétés pacifiques, justes et interdépendantes.

La Recommandation de l'éthique de l'IA comporte dix **principes éthiques** qui sont :

- Proportionnalité et innocuité : Toujours justifier la décision de recourir à des systèmes d'IA et, en cas de risque grave, que ce soit l'homme qui prenne la décision finale. Il faut aussi que la méthode d'IA retenue soit adaptée et proportionnée pour atteindre un objectif légitime, qu'elle ne porte pas atteinte aux valeurs humaines fondamentales, qu'elle soit adaptée au contexte et repose sur des bases scientifiques rigoureuses ;
- Sûreté et sécurité : Les systèmes d'IA doivent être sûrs, c'est-à-dire fonctionner comme prévu, et être sécurisés, c'est-à-dire qu'ils ne puissent pas être compromis par des parties non autorisées. Il faut alors prévenir et éliminer, tout au long du cycle de vie des systèmes d'IA, les préjudices non désirés et les vulnérabilités aux attaques afin de garantir la sûreté et la sécurité des personnes, de

192 Loi n°2009-17 du 09 mars 2009 portant code éthique pour la recherche en santé
193 Loi n°2010-40 di 08 décembre 2010 portant code éthique et déontologique pour la recherche en Santé

l'environnement et des écosystèmes. Cela nécessite l'élaboration de cadres d'accès aux données qui soient respectueux de la vie privée et qui favorisent un meilleur entraînement et une meilleure validation des modèles d'IA utilisant des données de qualité ;

- Équité et non-discrimination : S'assurer que les bénéfices des technologies de l'IA soient disponibles et accessibles à tous, notamment aux groupes vulnérables, afin de promouvoir la justice sociale, garantir l'équité et lutter contre les discriminations en tous genres, aux niveaux national, régional et international ;
- Durabilité : Evaluer continuellement l'impact humain, social, culturel, économique et environnemental des technologies de l'IA sur la durabilité en tant qu'ensemble d'objectifs d'une société en constante évolution, tels qu'ils sont actuellement définis dans les objectifs de développement durable (ODD) des Nations Unies ;
- Droit au respect de la vie privée et protection des données : Respecter et protéger la vie privée tout au long du cycle de vie des systèmes d'IA. Il faudra pour cela mettre en place des cadres adéquats de protection des données comportant des mécanismes juridiques, organisationnels et procéduraux respectant les principes et les normes internationaux en matière de protection des données à caractère personnel. L'impact des algorithmiques sur la vie privée nécessitent des évaluations adéquates qui incluent également des considérations sociétales et éthiques. Les acteurs de l'IA sont responsables de la protection des informations personnelles, de la conception à l'évaluation d'impact des systèmes d'IA en passant par leur mise en œuvre.
- Surveillance et décision humaines : A tout stade du cycle de vie des systèmes d'IA, la responsabilité éthique et juridique doit pouvoir être imputée à des personnes physiques ou morales existantes, donnant ainsi lieu à la surveillance humaine individuelle ou publique ;
- Transparence et explicabilité : La transparence est nécessaire pour que les règlementations nationales et internationales en matière de responsabilité puissent être appliquées. Aussi, les individus devraient-ils être pleinement informés lorsqu'une décision affectant leur sécurité ou leurs droits humains est fondée sur des algorithmes d'IA ou prise par ceux-ci. Dans ces circonstances, ils devraient avoir la possibilité d'exiger ou de demander des explications à l'acteur de l'IA ou aux institutions du secteur public concernés ;
- Responsabilité et redevabilité : Les acteurs de l'IA et les États ont la responsabilité éthique et juridique de respecter, protéger et promouvoir les droits de l'homme et les libertés fondamentales, et favoriser la protection de l'environnement. Il faut aussi mettre en place des mécanismes appropriés de surveillance, d'évaluation de l'impact, de contrôle et de diligence requise pour assurer la redevabilité des systèmes d'IA et de leur impact ;
- Sensibilisation et éducation : Afin de garantir une participation publique efficace de sorte que tous les membres de la société puissent prendre des décisions éclairées concernant leur utilisation des systèmes d'IA et soient protégés contre toute influence indue, il faudra assurer la sensibilisation du public et sa compréhension des technologies de l'IA et de la valeur des données à travers une éducation ouverte et accessible, l'engagement civique, l'acquisition de compétences numériques et la formation à l'éthique de l'IA, notamment en faveur des médias;
- Gouvernance et collaboration multipartites et adaptatives : Les États, conformément au droit international et la souveraineté nationale, doivent réglementer les données générées sur leur territoire ou transitant par celui-ci, en vue du respect et de la protection des droits humains, notamment de la vie privée.

La Recommandation donne onze (11) domaines stratégiques d'application des valeurs et principes éthiques ci-dessus. Ces domaines stratégiques sont : (i) : évaluations de l'impact éthique ; (ii) gouvernance et gestion éthiques ; (iii) politiques en matière de données ; (iv) développement et coopération internationale ; (v) environnement et écosystèmes ; (vi) égalité des genres ; (vii) culture ; (viii) éducation et recherche (ix) communication et information (x) économie et travail ; (xi) santé et bien-être social.

Les États membres sont appelés à assurer de manière crédible et transparente le suivi et l'évaluation des politiques, programmes et mécanismes relatifs à l'éthique de l'IA en combinant des approches quantitatives et qualitatives. L'UNESCO est disposée à les appuyer dans ce suivi et évaluation, notamment dans le domaine méthodologique.

En termes d'utilisation, les États membres de l'UNESCO sont appelés à respecter, promouvoir et protéger les valeurs, principes et normes éthiques de l'IA énoncés dans la Recommandation. Ils doivent prendre toutes les mesures pour donner effet aux recommandations stratégiques qu'elle contient.

b. Nécessité de lignes directrices éthiques pour une IA digne de confiance en Afrique

Le développement et l'utilisation de systèmes d'IA doivent être basés sur la **confiance et la responsabilité.** L'IA, sur tout le continent, doit être **responsable et digne de confiance.** Dans son **Acte constitutif** (Art.4) et sa **Charte des droits de l'homme et des peuples (Art. premier à Art. 26), l'Union Africaine** (UA) fournit les principes et les droits fondamentaux de toute personne et tout peuple vivant sur son espace.

Concernant la technologie et les données, l'UA a adopté un ensemble de textes juridiques pouvant servir de base à l'encadrement de l'intelligence artificielle sur le continent. Il y a notamment la **Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel** adoptée en juin 2014 à Malabo qui cependant peut être mise à jour pour mieux prendre en compte l'IA.

Au niveau **régional**, le cadre juridique global a fixé les règles claires concernant la sécurité des réseaux et des systèmes d'information ainsi que pour la protection des données à caractère personnel. Il y a notamment **avec la CEDEAO** de la Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité, de la Directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace, de l'Acte additionnel A/SA 1/01/07 du 19 janvier 2007 relatif à l'harmonisation des politiques et du cadre réglementaire du secteur des Technologies de l'Information et de la Communication et de l'Acte Additionnel A/SA.1/01/10 du 16 février 2010, relatif à la protection des données à caractère personnel.

Cependant, **spécifiquement sur l'IA**, il n'y a pas encore de stratégie, ni de texte juridique au niveau continental, régional ou national. Cette absence de textes est aussi observée sur le volet éthique qui, à n'en pas douter, est indispensable pour renforcer la confiance dans le développement et l'utilisation de systèmes d'IA. Il s'avère donc crucial de procéder à l'élaboration de projets de lignes directrices de l'éthique de l'IA aux niveaux continental, régional et national. Ces projets de lignes directrices devront s'attaquer aux problèmes d'ordre éthique en se basant sur la Charte des droits de l'homme et des peuples de l'Union Africaine, le traité de la CEDEAO ainsi que les constitutions nationales et les législations nationales portant sur code éthique.

L'élaboration de ce projet de lignes directrices tiendra compte des valeurs et principes édictés par l'UNESCO dans sa **Recommandation sur l'éthique de l'intelligence artificielle** qui a offert un cadre normatif mondial sur le sujet. Elle devra rassembler toutes les parties prenantes concernées par l'IA afin d'aboutir à des principes éthiques multidimensionnels et consensuels.

Le projet de lignes directrices prendra en compte les préoccupations, appels et exhortations de la **Commission africaine des droits de l'homme et des peuples** (CADHP) qui, notamment dans sa Résolution CADHP/Rés.473(XXXI) 2021[194] :

- **Appelle** les États à veiller à ce que le développement et l'utilisation de technologies de l'intelligence artificielle, de la robotique et d'autres technologies nouvelles et émergentes soient compatibles avec les droits et les devoirs inscrits dans la Charte africaine des droits de l'homme et des peuples et d'autres instruments régionaux et internationaux des droits de l'homme afin de maintenir la dignité humaine, la vie privée, l'égalité, la non-discrimination, l'inclusion, la diversité, la sécurité, l'équité, la transparence, la responsabilité et le développement économique comme principes sous-jacents devant guider le développement et l'utilisation de l'IA ;
- **Exhorte** les États à s'assurer que toutes les technologies de l'IA, importées d'autres continents, soient rendues applicables au contexte africain ou adaptées pour correspondre aux besoins de l'Afrique et qu'ils prennent sérieusement en considération les valeurs et les normes africaines dans la formulation des cadres de gouvernance de l'IA pour prendre en compte l'injustice épistémique prévalant actuellement dans le monde ;
- **Exhorte** les États à garantir la transparence dans l'utilisation des technologies de l'IA et que les décisions les concernant soient rendues rapidement compréhensibles pour les personnes concernées ;

194 https://www.achpr.org/fr_sessions/resolutions?id=504

- **Appelle** les États à œuvrer dans le sens d'un cadre de gouvernance juridique et éthique global pour les technologies de l'IA afin d'en garantir la conformité avec la Charte africaine et d'autres traités régionaux ;
- **Appelle** l'Union africaine et les organismes régionaux à inscrire d'urgence dans leurs agendas la question des technologies de l'IA en vue d'élaborer un cadre régional réglementaire qui permettra de mettre en place des technologies qui répondent aux besoins des populations du continent ;
- **Appelle** les États à s'assurer que toutes les technologies de l'IA qui ont des conséquences de longue portée pour les humains doivent rester sous un contrôle humain effectif, en vue de garantir que la menace qu'elles représentent pour les droits fondamentaux de l'homme est écartée. La norme émergente relative au maintien d'un contrôle humain effectif des technologies de l'IA doit être codifiée en tant que principe des droits de l'homme ;
- **S'engage** à entreprendre une étude afin d'affiner des lignes directrices et des normes sur les questions relatives aux technologies de l'IA et leur impact sur les droits de l'homme en Afrique en collaboration avec un Groupe africain d'experts sur l'intelligence artificielle et les nouvelles technologies.

Ainsi, le projet de lignes directrices portera sur des domaines tels que la gestion des systèmes d'IA importés, la sécurité, la sûreté, la surveillance, l'équité, l'inclusion sociale, la transparence, la responsabilité, la redevabilité et le développement économique. D'une manière plus générale, il examinera l'impact de l'IA sur les droits fondamentaux des personnes et des peuples, y compris l'égalité des peuples, le respect de la vie privée, la dignité, la protection des consommateurs et la non-discrimination.

Le projet de lignes directrices s'appuiera sur les travaux du Groupe d'experts de l'Union africaine sur la cybersécurité[195] et exploitera d'autres activités similaires. Les entreprises, les établissements universitaires, les centres de recherches et d'autres organisations de la société civile seront invités à donner leurs points de vue sur les valeurs et principes éthiques pertinents, mais aussi l'application des cadres juridiques sur les données et les technologies émergentes.

Le projet de lignes directrices éthiques de l'IA mettra à profit les travaux réalisés par certains organismes internationaux comme l'Union Européenne[196], l'OCDE[197] et pays comme le Canada, la Suède, ... En Afrique, des ONG et auteurs ont mené des réflexions touchant le sujet qui pourront être pris en considération. Il s'agit par exemple de WATHI[198], du CRDI[199],...

195 Le Groupe d'experts de l'Union africaine sur la cybersécurité tient sa première réunion inaugurale | Union africaine
196 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60427
197 https://legalinstruments.oecd.org/api/print?ids=648&lang=fr
198 https://www.wathi.org/
199 Les Enjeux Éthiques d'Internet en Afrique de l'Ouest: Vers un Modèle Éthique d'Intégration (idrc.ca)

Tableau SWOT du cadre éthique lié à l'Intelligence artificielle, les données et technologies émergentes des quatre pays cibles

Forces	**Faiblesses**
• *Existence de législations instituant un Code d'Ethique pour la Recherche en Santé au Sénégal, Benin, ;* • *Existence de Comité National d'Ethique pour la Recherche en Santé (CNERS) dans tous les pays cibles ;* • *Existence de Comité d'éthique de la recherche dans les universités (UCAD...) au Sénégal* • *Les activités statistiques sont basées sur le respect de principes éthiques professionnelles ;*	• *Inexistence de document national sur l'éthique de l'IA dans les pays cibles* • *Inexistence de document communautaire sur l'éthique de l'IA à la CEDEAO ou à l'UA* • *Faiblesse des moyens financiers et humains des autorités de protection* • *Absence de législation sur l'ouverture des données publiques* • *Retard dans la mise en place d'autorité de contrôle en matière de cybersécurité (Sénégal)* • *Faible protection contre les biais et les atteintes aux droits fondamentaux*
Opportunités	***M*enaces**
• *Révision des législations sur la protection des données à caractère personnel pour prendre en compte des enjeux liés à l'IA sur la vie privée ;* • *Réglementation nécessaire sur l'ouverture des données publiques* • *Réflexion sur une réglementation communautaire (CEDEAO) sur les SIA* • *Renforcement des autorités de protection des données à caractère personnel*	• *Risques d'atteintes aux droits fondamentaux par l'usage des SIA ;* • *Risques de reproduction de biais discriminatoire par les SIA ;* • *Risque d'attaques cybercriminelles sur les SIA* • *Risque d'atteinte aux droits de propriété intellectuelle*

V. LE CADRE INSTITUTIONNEL DES TECHNOLOGIES EMERGENTES ET DES DONNEES

Selon la Recommandation sur l'éthique de l'IA de l'UNESCO, les étapes du cycle de vie des systèmes d'IA sont notamment la recherche, la conception, le développement, le déploiement, l'utilisation, la maintenance, l'exploitation, la commercialisation, le financement, le suivi et l'évaluation, la validation jusqu'à l'obsolescence et donc la fin de l'utilisation, le démontage et la mise hors service.

Les acteurs de l'IA visés sont toutes les personnes physiques et morales impliquées dans au moins l'une des étapes du cycle de vie de l'IA. Ce sont alors les entreprises, les universités et instituts de recherche, les entités publiques et privées, les chercheurs, les programmeurs, les ingénieurs, les data scientist, les utilisateurs finaux, les importateurs et exportateurs de systèmes d'IA, etc. Ces acteurs de l'IA se retrouvent donc aux niveaux international, africain, régional et national.

A. Le rôle propulseur des acteurs institutionnels dans le développement de l'IA

Les acteurs institutionnels sont entendus ici comme étant les administrations publiques, les gouvernements ou les décideurs politiques qui se situent aux niveaux continental, régional et national. Les acteurs institutionnels sont au cœur du développement et de l'utilisation de l'IA et y jouent un rôle moteur. Les technologies IA s'étendent dans les économies et les sociétés africaines. L'UA, la CEDEAO et les gouvernements sont de plus en plus actifs, à la fois comme décideurs mais aussi utilisateurs de systèmes d'IA. Si de nombreuses parties prenantes jouent des rôles différents, les pouvoirs publics sont les seuls qui peuvent avoir une vue

d'ensemble de l'IA et de ses répercussions, qui peuvent promouvoir les conditions de son développement et répondre aux défis et aux questions qui découlent de son utilisation.

Les décideurs publics déterminent l'environnement politique, juridique et commercial qui favorise l'innovation, l'investissement et le développement basé sur la technologie. Dans le monde entier, des gouvernements tournés vers l'avenir s'efforcent déjà de promouvoir l'IA et, plus largement, l'économie numérique en prenant des mesures telles que l'élaboration de cadres de protection des données clairs et favorables à l'innovation, la mise en œuvre de politiques de cybersécurité, l'utilisation du cloud computing et la promotion d'une connectivité de haute qualité pour tous.

Selon la Commission Economique pour l'Afrique (CEA) dans « L'intelligence artificielle en Afrique : possibilités à saisir, défis à relever et considérations de politique générale »[200], les gouvernements gèrent à l'échelle nationale des systèmes d'éducation, des instituts de recherche et de nombreuses initiatives de qualification qui préparent les travailleurs à participer à l'économie de l'IA et peuvent contribuer aux progrès de l'IA. Ils sont également les gardiens de quantités considérables de données qui peuvent fournir la matière première aux chercheurs et aux innovateurs pour développer des applications, et ils ont le pouvoir de les rendre disponibles et utiles.

Les gouvernements constituent aussi une plateforme essentielle pour le dialogue avec les parties prenantes et assurent leur coordination. Ils peuvent créer d'importants mécanismes de collaboration et de partage d'informations entre le secteur public, le secteur privé, la société civile et le monde universitaire. Les discussions avec ces parties sont également importantes pour identifier et concevoir des réponses efficaces à certaines des questions de politique générale et des défis sociaux qui découleront de l'IA.

L'IA offre de multiples avantages potentiels tout en posant de grands défis aux nations africaines, aux régions du continent et à l'Union Africaine. A l'heure actuelle, les réponses stratégiques nécessaires ne sont pas à la hauteur des défis, dans aucun niveau, continental, régional ou national.

L'IA est absente des conventions et chartes de l'UA, tandis qu'elle commence de produire des effets non négligeables sur la vie des africains. Les acteurs continentaux comme la Conférence des Chefs d'Etat et de Gouvernement de l'UA (avec la Commission de l'UA et la Commission africaine des droits de l'homme et des peuples), la Conférence des Ministres (avec le Comités techniques spécialisés sur les communications et les technologies de l'information et de la communication) sont ainsi interpelés afin d'apporter une réponse politique et juridique pour le développement et l'utilisation d'une IA éthique, responsable et digne de confiance en Afrique.

Plusieurs actions sont menées par des structures de l'UA portant sur l'IA ou les données parmi lesquelles il y a :

- La Résolution sur la nécessité d'élaborer une étude sur les droits de l'homme et des peuples et l'intelligence artificielle (IA), la robotique et d'autres technologies nouvelles et émergentes en Afrique - CADHP/Rés.473(XXXI) 2021[201] ;
- Le Cadre stratégique en matière des données de l'UA approuvé par décision EX.CL/Déc.1144(XL) du Conseil exécutif lors de sa 40e session ordinaire tenue les 2 et 3 février 2022[202].

Ces actions ne tarderont certainement à se refléter dans les textes juridiques comme les conventions et les chartes afin d'indiquer aux CER et aux Etats membres les politiques, lois et règlements à adopter en matière d'IA.

Au niveau régional, la Communauté économique des États de l'Afrique de l'Ouest - CEDEAO[203] a été créée le 28 mai 1975 à Lagos, au Nigéria. Son siège est à présent à Abuja (Nigeria). Elle est constituée de 15 pays membres : Bénin, Burkina Faso, Cabo Verde, Côte d'Ivoire, Gambie, Ghana, Guinée, Guinée-Bissau, Liberia, Mali, Niger, Nigeria, Sénégal, Sierra Leone, Togo (la Mauritanie a quitté la CEDEAO en 2000. Elle a récemment signé un nouvel accord de membre associé en août 2017). Elle s'étend sur une superficie de 5,2 millions de km^2. La population de la CEDEAO est estimée à 407 millions d'habitants en 2022[204]. La mission de la CEDEAO est de « Promouvoir la coopération et l'intégration des états membres avec pour objectif de créer une union économique et monétaire ouest-africaine ».

200 Nations Unies. Commission Economique pour l'Afrique (2021-08). L'intelligence artificielle en Afrique : possibilités à saisir, défis à relever et considérations de politique générale. Addis Abeba:. © NU. CEA,. https://hdl.handle.net/10855/48011"

201 https://www.achpr.org/fr_sessions/resolutions?id=504

202 https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-FR.pdf

203 A propos de la CEDEAO | Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) (ecowas.int)

204 Communauté économique des États de l'Afrique de l'Ouest 2022 | countryeconomy.com

En matière de structure de gouvernance[205], la CEDEAO est composée de trois grandes instances : l'Exécutif, le Législatif et le Judiciaire. Au sommet de la structure se trouve le président de la Conférence des chefs d'Etat et de gouvernement. Le président de la Conférence est le président en exercice désigné par les autres chefs d'Etat et de gouvernement pour gérer les affaires de l'organisation pour une période d'un an. Le ministre chargé des affaires de la CEDEAO dans le pays du président de la Conférence devient automatiquement le président du Conseil des ministres. Et ce pays préside toutes les autres réunions statutaires (ministérielles, experts, comme les comités techniques) de la CEDEAO pendant l'année en cours.

L'Exécutif de la Communauté est dirigé par le président de la Commission de la CEDEAO qui est nommé par la Conférence pour une période non renouvelable de quatre ans. Il est assisté d'un vice-président et de 13 Commissaires. L'organe législatif de la Communauté est le Parlement, qui est dirigé par un président. Les fonctions administratives du Parlement sont gérées par le Secrétaire Général. En attendant les élections au suffrage universel direct, les parlementaires sont détachés des Parlements nationaux au Parlement de la Communauté pour une période de quatre ans. L'organe judiciaire de la Communauté est la Cour de Justice, qui est également dirigée par un président. Les juges sont détachés des Cours suprêmes nationales pour occuper les postes réservés aux pays. La Cour veille à l'interprétation et à l'application des lois, des protocoles et des conventions de la Communauté. Les fonctions administratives de la Cour sont assurées par le Greffier en chef assisté d'autres professionnels.

En ce qui concerne l'intelligence artificielle, les données et les technologies émergentes, il est important de relever l'adoption des trois textes politique et juridiques suivants : (i) la Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité de la CEDEAO ; (ii) l'Acte additionnel A/SA 1/01/07 du 19 janvier 2007 relatif à l'harmonisation des politiques et du cadre règlementaire du secteur des technologies de l'information et de la communication (TIC) et (iii) l'Acte Additionnel relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO de 2010 a été une grande avancée. Pour l'instant aucune initiative sur l'IA.

Au niveau national, l'exemple du Sénégal montre que l'IA est sous la tutelle technique du **ministère** chargée du numérique (ou des communications électroniques, ou de l'économie numérique) qui est **l'Autorité gouvernementale** chargée de mettre en œuvre la politique définie en matière de communications électroniques.

Le **Ministère de l'Enseignement Supérieur de la Recherche et de l'Innovation – MESRI** (http://mesr.gouv.sn/) joue un rôle important, comme au Sénégal, de fournisseur de plateformes notamment d'un Supercalculateur de 537 Teraflops opérationnel et d'un Centre de calcul mis en place.

Outre les directions logées dans les ministères, il existe des **agences ou sociétés nationales** dotées de la personnalité morale et de l'autonomie de gestion chargée de mettre en œuvre la politique d'informatisation de l'Etat ainsi que la gestion des infrastructures numériques de l'État[206].

Au Sénégal, **l'Agence de l'Informatique de l'Etat – ADIE** (www.adie.sn), qui s'est muée en **Sénégal Numérique - SENUM SA**, joue aussi un rôle prépondérant d'opérateur d'infrastructures publiques. Elle a procédé à la mise en place de 2 Datacenters aptes à héberger les applications IA. Il existe également lePark de Technologie Numérique - centre de services (https://ptn.sn/),. Le réseau de SENUM SA couvre plus de 5000 kms de fibres optiques déployés sur tout le territoire national. Enfin, plusieurs câbles sous-marins atterrissent au Sénégal.

En plus, dans chaque pays cibles, il existe des **Autorités de Régulation des Télécommunications**, en tant qu'autorité administrative indépendante, chargée d'assurer l'application de la législation et de la réglementation applicable au secteur des communications électroniques et de veiller au respect de la loi (Art. 7 Code des communications électroniques du Sénégal207).

Par ailleurs, il existe dans chaque paye une autorité **de protection des données personnelles** chargée de garantir le respect de la vie privée dans le traitement des données à caractère personnel.

La **Loi n°2020-01 du 6 janvier 2020 portant création et promotion de la startup** a été votée au Sénégal. Il en est de même pour la Côte d'ivoire) **avec la loi n°2023-901 du 23 novembre 2023 portant promotion**

205 La CEDEAO… en dates et en chiffres | Webmanagercenter
206 Sénégal numérique : Une Histoire, Un Avenir | Société Sénégal Numérique S.A. (adie.sn)
207 Code des Communications électroniques | ARTP Sénégal

des startups numériques. Un projet de loi similaire est en cours d'élaboration dans les deux autres pays cibles. Au Sénégal, en application des dispositions de l'article 4 de la loi n° 2020-01 du 06 janvier 2020, est pris le Décret n° 2021-1772 du 28 décembre 2021 portant création de la **Commission d'évaluation, d'appui et de coordination,** en abrégé, **« CEAC »** est une autorité administrative rattachée au ministère en charge de l'Economie numérique. La CEAC est chargée du pilotage et de la définition des orientations stratégiques en vue de la promotion des startups ; mais également chargée de l'élaboration et de la coordination de la mise en œuvre d'une stratégie nationale de promotion des startups articulée aux politiques et stratégies pertinentes au Sénégal.

Cette architecture institutionnelle en matière d'IA est à peu de chose près la même dans les quatre pays cibles.

B. Les acteurs privés, levier d'innovation en matière d'IA

Par acteurs privés, il est entendu les acteurs non politiques i.e. tous ceux ne faisant pas partie des acteurs institutionnels ci-dessus définis. Le diagnostic des acteurs privés de l'IA portera sur les quatre pays cibles. A cet effet, des enquêtes quantitatives et qualitatives sont en cours et n'ont pas encore produit leurs résultats. En attendant, le diagnostic portera sur le Sénégal à partir d'un tableau cartographique obtenu de l'Université[208].

L'exploitation du tableau montre que les acteurs privés de l'IA sont dans les secteurs suivants : les académies d'enseignement supérieur, la société Civile, les organisations patronales, les associations, le secteur privé, les opérateurs de télécommunications et multinationales, et les Organisations Non Gouvernementales (ONG).

Dans le secteur des **académies** d'enseignement supérieur, les acteurs privés de l'IA sont :

- **l'Université Cheikh Anta DIOP - UCAD** (https://www.ucad.sn/) qui, dans son rôle de fournisseur de compétences et de recherche, organise un Master en Data Science et Intelligence Artificielle, gère un projet de développement d'un kit de formation à la Data Science pour maitriser la productivité agricole, et administre un Projet AI for Covid19 Program ;
- **l'Université Gaston BERGER – UGB** (https://www.ugb.sn/) qui gère un Projet AI for cardio pour le suivi et la prévention des maladies cardiovasculaires en Afrique et aussi un Projet environnemental de Système d'alerte précoce ;
- **l'Université Alioune DIOP Bambey – UADB** (http://www.uadb.edu.sn/) qui organise des formations de Licence et Master en statistiques et informatique décisionnelle, délivre un Certificat en collecte de données. Elle gère aussi un Projet Résilience pour publier les leçons apprises de la covid19 dans le cadre de la transformation digitale des universités ;
- **le Dakar Institute of Technologies – DIT** (https://dit.sn/) organise une formation pour une Licence en Big Data et master IA et une pour un Certificat en Data Sciences ;
- **l'Ecole Supérieure Polytechnique – ESP** (http://www.esp.sn/) organise un Master en IA ;
- **l'Institut Africain des Sciences Mathématiques – AIMS** (https://aims-senegal.org/fr/) qui forme pour un Master Africain en Intelligence Artificielle ;
- **le Centre d'Excellence Africain Mathématiques Informatique et TIC** (www.ceamitic.sn/) actif dans la formation et la recherche ;
- **l'Université Iba Der THIAM** (https://www.univ-thies.sn) qui fait un Master en sciences de données et applications et un autre en IA et smart tech ;
- **l'Université Virtuelle du Sénégal – UVS** (https://www.uvs.sn/) qui organise des formations pour un Master en E-data Analytics, un autre Master en IA, une Licence et Master en Robotique, un Master en calcul et données massives et l'IA et un Certificat en IA et IoT ; et
- **l'Ecole Supérieure Multinationale de Télécommunications - ESMT** (https://www.esmt.sn/) qui forme pour un Master en Data Science et Intelligence Artificielle.

208 Avec Dr. Daouda Diagne

Dans le secteur de la **Société civile, les acteurs privés de l'IA sont :**

- **Jonction** (http://jonction.e-monsite.com/) qui est active dans la promotion des droits du numérique et dans la sensibilisation aux droits du numérique ; et
- **Students Travel And Exposure Senegal – STAESEN** (http://staesen.org) qui, pour son rôle de promotion des droits du numérique, procède par sensibilisation et formation aux droits du numérique.

Dans le secteur des **organisations patronales, les acteurs privés de l'IA sont :**

- **L'Ordre National des Médecins du Sénégal** (https://www.ordremedecins.sn), qui promeut la recherche dans le domaine médical, fait de la recherche en utilisant des systèmes d'IA ;
- **le Conseil National du Patronat** (https://www.cnp.sn/) qui procède à l'accompagnement des entreprises ;
- **l'Organisation des Professionnels des Technologies de l'Information et de la Communication – OPTIC** (http://www.optic.sn/), qui est un regroupement d'entreprises en TIC, procède à la promotion de l'IA ;

Dans le secteur des **associations, les acteurs privés de l'IA sont :**

- **Galsen AI** (https://galsen.ai/), qui intervient dans la vulgarisation de l'IA et son plaidoyer, en procédant à l'initiation de projets à caractère social, l'organisation de formations et la mobilisation de compétences ;
- **L'Association Sénégalaise d'Intelligence Artificielle - ASIA** (https://twitter.com/aisenegal) fait la promotion de la recherche autour de l'IA et effectue des campagnes de développement de l'IA ;
- **L'Association Sénégalaise des Chercheurs en Informatique (ASCII)** (http://www.ascii.org.sn/) organise des activités liées à l'IA et développe de la formation en informatique avec des productions ;
- **Wathi (**https://www.wathi.org/) a procédé au lancement d'une initiative spéciale sur l'IA ;

Dans le secteur privé de l'économie numérique, les acteurs de l'IA sont :

- **Baamtu Datamation (**https://baamtu.com/), dans le domaine de l'automatisation des tâches, développe des applications basées sur l'IA ;
- **le Salon International des Professionnels du Numérique - SIPEN (**https://www.sipen-dakar.com) fait dans l'organisation d'évènements liés à l'IA ;

Dans le secteur des **opérateurs de télécommunications et multinationales, les acteurs de l'IA sont:**

- Orange (http://orange.sn), fournisseur d'infrastructures, dispose d'un Datacenter et des services d'IA ;
- Free (https://www.free.sn/), qui aussi est un Fournisseur d'infrastructures, dispose d'infrastructures 5G et d'un Datacenter ;
- **Arc Informatique https://site.arc.sn/ joue un rôle de fournisseur d'infrastructures et de services d'accès Internet ;**
- **Google AI (**https://ai.google/) fait dans l'accompagnement financier de projets comme le Projet «Jeu de données» ;

Dans le secteur des **Organisations Non Gouvernementales (ONG), les acteurs de l'IA sont :**

- **Deep learning INDABA (**https://deeplearningindaba.com) vulgarise l'IA, en partenariat avec GALSEN IA, en organisant des conférences au niveau national, en procédant par réseautage et en vulgarisant l'entreprenariat social autour de l'IA ;
- **Artificial Intelligence for Development - AI4D (**https://africa.ai4d.ai/fr/) fait dans l'accompagnement financier de projets – Recherche, notamment en mettant en place des laboratoires.

Au total, 27 acteurs privés ont été identifiés comme intervenants dans le domaine de l'IA. Ils sont repartis dans 8 secteurs d'activités. Parmi eux, le secteur des académies d'enseignement supérieur en sort prépondérant avec 10 acteurs privés, soit plus du tiers. Cela témoigne de l'état de développement de l'IA au Sénégal où

elle en est dans une phase de formation et d'implantation.

Tableau SWOT du cadre institutionnel lié à l'Intelligence artificielle, les données et technologies émergentes des quatre pays cibles

Forces	**Faiblesses**
• Existence de ministères chargés du numérique ; • Existence d'Autorités de Régulation des Télécommunications, de Commissions des données personnelles et de Commission de promotion et de coordination des startups (Sénégal) ; • L'Enseignement supérieur (universités, écoles supérieures,...) est fortement impliqué notamment comme fournisseur de compétences et de recherche ; • Existence d'agences ou sociétés nationales chargées de mettre en œuvre la politique d'informatisation de l'Etat ainsi que la gestion des infrastructures numériques de l'État ; • La Société civile, les associations et les ONG sont actives dans la sensibilisation et la promotion des droits du numérique, le plaidoyer, les formations et la mobilisation de compétences ; • Les organisations patronales accompagnent des entreprises et promeuvent l'IA ; • Les opérateurs de télécommunications et multinationales fournissent des infrastructures et accompagnent financièrement des projets.	• Inexistence de Commission nationale sur l'IA dans les pays cibles ; • Inexistence d'institution communautaire sur l'IA à la CEDEAO ; • Inexistence d'institution communautaire sur l'IA à l'UA ; • Inexistence de Commission de promotion et de coordination des startups dans trois pays cibles ; • Inexistence de Groupe de travail sur l'IA chargé de proposer des mesures urgentes à prendre pour mettre à profit l'IA en faveur du développement.
Opportunités	**Menaces**
• la Commission de l'UA a élaboré « La stratégie de transformation numérique pour l'Afrique (2020-2030)[209] » • Le Conseil exécutif de l'UA a adopté le Cadre stratégique en matière des données de l'UA • La Commission africaine des droits de l'homme et des peuples a adopté une Résolution sur les droits de l'homme et des peuples et l'IA[210] . • La création d'un groupe de réflexion sur l'IA par l'ONU composé de 38 experts dont un représentant Sénégalais	• Inexistence au niveau de l'UA d'un Groupe d'experts sur l'intelligence artificielle ; • Inexistence au niveau de la CEDEAO d'un Groupe d'experts sur l'intelligence artificielle.

209 https://au.int/sites/default/files/newsevents/workingdocuments/37470-wd-annexe_2_ie25274_f_digital_transformation_startegy.pdf
210 https://www.achpr.org/fr_sessions/resolutions?id=504

II. CONCLUSION ET RECOMMANDATIONS GENERALES

A. Recommandations pour l'élaboration d'une stratégie communautaire et une stratégie nationale sur l'IA

Le constat est là, à part le Benin, les autres pays cible n'ont adopté aucune stratégie sur l'IA. Ce constat est partagé avec tous les pays d'Afrique de l'Ouest. Les questions liées aux SIA sont énoncées de manière brève dans les stratégies de développement du Numérique. Or, vu le développement fulgurant des SIA et son usage dans de nombreux domaines, ces questions doivent constituer une priorité pour les pays cibles. C'est pourquoi nous recommandons, l'élaboration d'un document stratégique national spécifique sur l'intelligence artificielle par les trois pays cible afin d'encadrer le développement et l'utilisation des SIA. Ces documents stratégiques ne doivent pas uniquement constituer à un copier-coller des stratégies existantes en la matière (**même si ces stratégies peuvent être source d'inspiration)** mais devraient prendre en compte les préoccupations et les besoins endogènes de chaque pays. Ces stratégies pour être efficace doivent faire l'objet de financement interne afin d'éviter l'influence des bailleurs. A notre avis, la recherche, la formation et le volet éthique devraient être les objectifs majeurs de ces stratégies.

Au-delà des stratégies nationales, l'élaboration de stratégie communautaire à l'instar de la stratégie régionale de cybersécurité et de lutte contre la cybercriminalité de la CEDEAO s'avère nécessaire. Cette stratégie donnera des orientations et établira un cadre stratégique que les Etats membres pourront prendre en compte dans leurs stratégies nationales.

B. Recommandations pour le renforcement du cadre juridique pour une prise en charge des enjeux liés à l'IA, aux technologies émergentes

L'étude a montré que les quatre pays cible disposent d'un cadre juridique composé de lois et règlements portant sur la cybersécurité et la cybercriminalité, la protection des données à caractère personnel, les transactions électroniques, les activités statistiques et la propriété intellectuelle. Ce cadre juridique s'applique aux SIA mais nécessiterait un renforcement.

Nous recommandons :

- Le renforcement des législations sur la protection des données à caractère personnelles : Les lois ivoiriennes et sénégalaises sur la protection des données à caractère personnel doivent faire l'objet de révision pour prendre en compte plus amplement les enjeux liés à l'intelligence artificielle ce qui n'est pas encore le cas. La loi béninoise en la matière pourrait servir de modèle car elle est la plus aboutie parmi les législations étudiées.
- Le renforcement en moyens humains et financiers des autorités de protection des données personnelles : Des missions de contrôle de conformité ont été conférées par la loi aux autorités de protection de données. Pour leur permettre d'assurer pleinement leur mission, il faut doter ces autorités de ressources humaines de qualité et de moyens financiers. Ces autorités doivent aussi jouer leur rôle dans l'accompagnement pour l'appropriation et la vulgarisation des législations sur la protection des données personnelles.
- Le renforcement des législations en matière de propriété intellectuelles pour mieux prendre en compte les problématiques résultant des technologies émergentes et l'IA générative notamment les atteintes aux droits de propriété intellectuelle ;
- Révision de l'acte additionnel de la CEDEAO sur la protection des données à caractère personnel pour prendre en compte les SIA ;
- La mise en place d'autorités réglementaires nationales en matière de cybersécurité : Depuis l'adoption de la loi sénégalaise de 2008, le Sénégal n'a pas encore mis en place d'autorité de cybersécurité, contrairement aux autres pays cibles du projet (Bénin : ANSSI -BENIN, Burkina Faso : ANSSI Burkina, Côte d'Ivoire : ANSSI CI).
- L'élaboration de réglementation nationale sur l'ouverture de toutes les données publiques dans

les pays cibles pour permettre l'utilisation des données de l'administration et apporter plus de transparence dans l'activité administrative ;

- Réflexion sur l'élaboration d'une réglementation nationale ou régionale sur l'intelligence artificielle. Conformément au document stratégique de l'IA sur la transformation digitale, la réglementation doit reposer sur des modèles souples et évolutifs

C. Recommandation pour le renforcement du cadre éthique pour une IA responsable et digne de confiance

En ce qui concerne l'éthique en matière d'intelligence artificielle, les recommandations proposées peuvent être mises en œuvre aux niveaux continental, régional et national. Les recommandations sont : (i) la création d'un comité d'experts en éthique de l'IA en vue de favoriser la recherche, l'acquisition de connaissances et le dialogue entre les acteurs, et de contribuer à l'établissement d'un cadre politique et juridique approprié pour le développement et l'utilisation d'une IA responsable et digne de confiance ; (ii) développer et mettre à disposition un instrument d'évaluation des risques éthiques pour un système d'IA ; (iii) mettre en place un programme de formation continue, pour les acteurs publics et privés, sur l'importance de l'éthique dans le développement et l'utilisation de l'IA.

D. Recommandations pour le renforcement du cadre institutionnel de l'IA en Afrique de l'ouest

La première étape est de mettre en place un Groupe de travail sur l'IA dont les missions porteront sur la proposition de mesures urgentes à prendre pour mettre à profit l'IA en faveur du développement, notamment l'identification de projets prioritaires compatibles avec l'IA dans les différents secteurs, l'attraction des compétences en IA, le renforcement des capacités,... Une Commission nationale sur l'IA est aussi à mettre en place avec à sa charge la coordination de toutes actions menées dans le secteur de l'IA, mais également de créer et d'animer un réseau entre les investisseurs, les grandes entreprises, les grandes sociétés de télécommunications, les universités et les startups afin d'encourager la collaboration et de faciliter le flux de connaissances et de financement.

II. BIBLIOGRAPHIE

RAPPORTS, ETUDES, ARTICLES

Rapport sur l'intelligence artificielle à l'ère du numérique, Commission AIDA, https://www.europarl.europa.eu/doceo/document/A-9-2022-0088_FR.html

Global Index IA 2022 Reports, https://aiindex.stanford.edu/report

Evaluation des besoins en Intelligence artificielle en Afrique, UNESCO, 2021, https://unesdoc.unesco.org/ark:/48223/pf0000375321

L'ère de l'IA dans le monde, rapport sur les stratégies nationales et régionales en matière d'IA, https://cifar.ca/wp-content/uploads/2020/11/l-ere-de-l-ia-deuxieme-edition-f.pdf

Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique par la loi pour une république numérique. https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

Le résumé en Français du rapport sur l'intelligence artificielle dans la société. https://www.oecd-ilibrary.org/docserver/aa565467fr.pdf?expires=1661270139&id=id&accname=guest&checksum=6E7260C121BD3

Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, CNCDH, 7 avril 2022 , https://www.cncdh.fr/publications/avis-relatif-limpact-de-lintelligence-artificielle-sur-les-droits-fondamentaux-2022-6#.

Etude du Conseil d'Etat français, Intelligence artificielle et action publique : construire la confiance, servir la performance, adoptée le 31/03/2022

Etude préliminaire sur l'éthique de l'intelligence artificielle, SHS/COMEST/EXTWG-ETHICS AI/2019/1

L'intelligence artificielle en Afrique : possibilités à saisi, défis à relever et considérations de la politique généraleAddis Abeba:. © NU. CEA,. https://hdl.handle.net/10855/48011"

Les Enjeux Éthiques d'Internet en Afrique de l'Ouest : Vers un Modèle Éthique d'Intégration (idrc.c

AZOULAY Warren, « Des machines et des hommes. La guerre n'aura pas lieu », Droit et société, 2019/3 (N° 103), p. 595-607

Camille AUBIN, Intelligence artificielle et Brevets, 2018

DUGUET Julien, CHASSANG Gauthier, BéRANGER Jérôme, « Enjeux, répercussions et cadre éthique relatifs à l'Intelligence Artificielle en santé. Vers une Intelligence Artificielle éthique en médecine », Droit, Santé et Société, 2019/3 (N° 3),

Erwin SOTIRI, Ruben Mendes, Et si Terminator devenait artiste, éditions légitech

Kondi Napo SONHAYE, L'Intelligence Artificielle, une opportunité pour l'agriculture au Togo, journals open éditions, https://journals.openedition.org/ctd/7219

CONVENTIONS INTERNATIONALES, RÉGIONALES ET SOUS RÉGIONALES

Convention de Budapest sur la Cybercriminalité

Convention 108 sur la protection des données à caractère personnel

Convention de l'Union africaine sur la Cybersécurité et la protection des données à caractère personnel

Accord de Bangui Révisé, 2015

RECOMMANDATIONS, RÉSOLUTIONS,

Recommandation de l'UNESCO sur l'éthique de l'intelligence artificielle, novembre 2021 ,21 p. https://unesdoc.unesco.org/ark:/48223/pf0000380455_fre/PDF/380455fre.pdf.multi

Résolution de l'UA sur la nécessité d'élaborer une étude sur les droits de l'homme et des peuples et l'intelligence artificielle (IA), la robotique et d'autres technologies nouvelles et émergentes en Afrique - CADHP/Rés.473(XXXI) 2021, https://www.achpr.org/fr_sessions/resolutions?id=504 4

CONSTITUTIONS

Constitution du Sénégal

Constitution du Benin

Constitution de la Cote d'ivoire

Constitution du Burkina Faso

TEXTES LÉGISLATIFS ET RÉGLEMENTAIRES

Loi n° 2008 -10 du 25 janvier 2008 portant loi d'orientation sur la Société de l'Information (LOSI) (Sénégal)

Loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel (Sénégal) ;

Loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques (Sénégal) ;

Loi n° 2008-11 du 25 janvier 2008 sur la Cybercriminalité (Sénégal)

Loi 2008-09 du 25 janvier 2008 sur le droit d'auteur et les droits voisins (Sénégal)

Loi de modification n° 2016-29 du 08 novembre 2016 du Code pénal (Sénégal)

Loi n°2012-03 en date du 03 janvier 2012 modifiant et complétant la loi n° 2004-21 du 21 juillet 2004 portant organisation et fonctionnement des activités statistiques (Sénégal)

La loi n° 2013-546 du 30 juillet 2013 relative aux transactions électroniques (Côte d'Ivoire)

La loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité (Côte d'Ivoire)

La loi n° 2013 – 450 du 19 juillet 2013 sur la protection des données à personnel (Côte d'Ivoire)

Loi n°2013-537 du 30 juillet 2013 portant organisation du système statistique (Côte d'Ivoire)

Loi 2017-20 du 13 juin 2017 portant Code du Numérique (Bénin)

La loi n° 99-014 du 12 avril 2000 portant Organisation et Fonctionnement Conseil National de Statistiques (Bénin)

Loi n°045-2009/AN du 10 novembre 2009 relative à la réglementation des services et des transactions électroniques (Burkina Faso)

Loi n°001-2021/AN du 31 mars 2021 portant protection des personnes à l'égard du traitement des données à caractère personnel (Burkina Faso)

Loi n°12-2007 /AN du 31 mai 2007 sur les activités statistiques (Burkina Faso)

Loi n°025-2018 du 31 mai 2018 portant code pénal (Burkina Faso)

Loi n°2008-09 du 25 janvier 2008 relative aux droits d'auteur et aux droits voisins (Sénégal)

Loi n°2016-555 du 26 juillet 2016 relative au droit d'auteur et aux droits voisins (Côte d'ivoire)

Loi n°032-99 AN du 22 décembre 1999 sur le droit d'auteur et les droits voisins (Burkina Faso)

Loi n°2005-30 du 05 avril 2006 relative au droit d'auteur et droits des voisins (Benin)

Loi n°2009-17 du 09 mars 2009 portant Code Ethique pour la Recherche en Santé (Sénégal)

Loi n°2010-40 du 08 décembre 2010 portant éthique et déontologie pour la recherche en santé (Bénin)

Loi n°2020-01 du 6 janvier 2020 portant création et promotion de la startup (Sénégal)

Loi n°2023-901 du 23 novembre 2023 portant promotion des startups numériques (Cote d'ivoire).

Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle et modifiant certains actes législatifs de l'Union), IA act

Décret d'application n° 2008-721 du 30 juin 2008 portant application de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel (Sénégal)

Décret n° 2015 -79 du 04 Février 2015, Fixant les modalités de dépôt des déclarations, de présentation des demandes, d'octroi et de retrait des autorisations pour le traitement des données à caractère personne (Côte d'Ivoire)

DOCUMENTS POLITIQUES ET STRATÉGIQUES

Stratégie Nationale d'Intelligence Artificielle et des Mégadonnées 2023-2027 | Portail du Numérique - Bénin (gouv.bj) ;

Stratégie nationale sur l'Intelligence artificielle (Sénégal) , synthèse de la stratégie IA du SENEGAL | Ministère de la Communication, des Télécommunications et du Numérique (numerique.gouv.sn)

Stratégie nationale des données (Sénégal), Synthèse de la Stratégie Nationale des Données du Sénégal. | Ministère de la Communication, des Télécommunications et du Numérique (numerique.gouv.sn)

Stratégie nationale du Numérique (2016-2025), Sénégal, http://www.numerique.gouv.sn/sites/default/files/Strat%C3%A9gie%20Numerique-SN2025-%20Plan%20d%27actions%20actualis%C3%A9.pdf

Stratégie nationale de la Cybersécurité (2017-2022), Sénégal, http://www.numerique.gouv.sn/mediatheque/documentation/strat%C3%A9gie-nationale-de-cybers%C3%A9curit%C3%A9-snc2022#:~:text=Minist%C3%A8re%20de%20l'%C3%89conomie%20Num%C3%A9rique%20et%20des%20T%C3%A9l%C3%A9communications,-Menu&text=La%20pr%C3%A9sente%20%C2%AB%20Strat%C3%A9gie%20nationale%20de,aux%20objectifs%20de%20la%20SN2025

Stratégie nationale de Développement numérique 2021-2025, Cote d'Ivoire

Stratégie nationale de l'Innovation (2021-2025), Cote d'Ivoire, https://docplayer.fr/228030345-Strategie-d-innovation-de-la-cote-d-ivoire.html

Stratégie nationale de la cybersécurité (2021-2025), Cote d'Ivoire

Stratégie Nationale de la Sécurité numérique (2020-2022), Bénin, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SNSN_FINAL_SIGNED_ANSSI.pdf

Stratégie nationale de développement de l'économie numérique (2018-2027), Burkina Faso, https://dgtic.mdenp.gov.bf/wp-content/uploads/2020/03/Strat%C3%A9gie_Nationale_de_D%C3%A9veloppment_de_Economie_Num%C3%A9rique_2018-2020.pdf

Stratégie nationale de la cybersécurité (2019-2023), Burkina Faso, https://anssi.bf/fileadmin/user_upload/SNCS_BF.pdf

Stratégie AI for Humanity (2018-2022), France, https://cache.media.enseignementsup-recherche.gouv.fr/file/strategie_IA/60/7/mesri_IA_dep_A4_09_1040607.pdf

Stratégie pancanadienne en matière d'IA (2017-2022), Canada, https://cifar.ca/fr/ia/

Mauritius Artificial Intelligence Strategy (2018-2030, Ile Maurice, https://ncb.govmu.org/ncb/strategicplans/MauritiusAIStrategy2018.pdf

Projet de stratégie de transformation numérique pour l'Afrique (202.-2030) Union Africaine

SITES INTERNETS

https://www.larousse.fr/dictionnaires/anglais-francais/intelligence/589276

https://dictionnaire.lerobert.com/definition/intelligence https://dictionnaire.lerobert.com/definition/artificiel

https://fr.wikipedia.org/wiki/Algorithme

https://penseeartificielle.fr/difference-intelligence-artificielle-machine-learning-deep-learning

https://www.coe.int/fr/web/artificial-intelligence/ai-and-control-of-covid-19-coronavirus

https://feserwam.org/fr/accueil-2/

https://www.actuia.com/actualite/la-commission-europeenne-publie-ses-recommandations-de-politique-et-dinvestissement-pour-une-ia-de-confiance/

http://www.osiris.sn/Adoption-des-Conventions-de.html

https://www.wipo.int/wipo_magazine/fr/2017/05/article_0003.html

Le Groupe d'experts de l'Union africaine sur la cybersécurité tient sa première réunion inaugurale | Union africaine

https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60427

https://legalinstruments.oecd.org/api/print?ids=648&lang=fr

https://www.wathi.org/

https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2021/11/08112021_dp_strategie_nationale_pour_ia_2eme_phase.pdf

https://www.gouvernement.fr/action/pour-une-republique-numerique#

https://cifar.ca/fr/cifarnews/2022/06/22/le-cifar-annonce-les-plans-de-la-deuxieme-phase-de-la-strategie-pancanadienne-en-matiere-dintelligence-artificielle/

https://www.osler.com/fr/ressources/reglements/2022/loi-sur-l-intelligence-artificielle-et-les-donnees-du-gouvernement-du-canada -

https://ised-isde.canada.ca/site/innover-meilleur-canada/sites/default/files/attachments/1020_04_19-Website_Placemat_FR_v02.pdf

https://afm.media/2022/01/31/intelligence-artificielle-maurice-se-classe-1ere-en-afrique-et-58e-mondiale/

https://www.um6p.ma/fr/le-centre-international-dintelligence-artificielle-du-maroc

https://aujourdhui.ma/economie/lintelligence-artificielle-priorite-du-chantier-de-la-transformation-digitale

https://www.add.gov.ma/lancement-du-nouveau-portail-national-des-donnees-publiques-ouvertes-open-data#:~:text=Lancement%20du%20nouveau%20Portail%20national%20des%20donn%C3%A9es%20publiques%20ouvertes%20(Open%20Data

https://ideas4development.org/intelligence-artificielle-alliee-du-developpement-durable/

https://www.ieepi.org/paroles-dexperts-protection-brevet-des-inventions-intelligence-artificielle/

https://www.ipsilon-ip.com/dabus.html

https://www.wipo.int/edocs/mdocs/mdocs/fr/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1_rev.pdf

https://newconceptartphotoselling.com/blog/23159-laffaire-du-portrait-dedmond-bellamy/

https://www.journalduluxe.fr/fr/business/decision-metabirkin-revolution-droit-nfts-anna-klein

https://siecledigital.fr/2016/09/29/daddys-chanson-realisee-ia-style-beatles/

https://www.dictionnaire-juridique.com/definition/propriete-intellectuelle.php

Intelligence artificielle et cybersécurité : risques ou opportunités ? - onepoint (groupeonepoint.com)