


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)



REVUE DOCUMENTAIRE SUR LES CADRES POLITIQUES, JURIDIQUES ET ÉTHIQUES DE L'INTELLIGENCE ARTIFICIELLE (IA), TECHNOLOGIES ÉMERGENTES ET DONNÉES AUX NIVEAUX INTERNATIONAL, CONTINENTAL, RÉGIONAL ET NATIONAL

Rédigé par :

Fatou FOFANA, Juriste,

Mamadou NIANG, Statisticien

Tamba ATHIE, Juriste

Cheikh FAYE, ingénieur statisticien, coordonnateur du projet

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

Juillet 2024

TABLE DES MATIÈRES

LISTE DES SIGLES ET ABBREVIATIONS	3
I INTRODUCTION	7
1. Rappel du Contexte	7
2. Définition	7
3. Objectifs de la revue documentaire du cadre politique, législatif, réglementaire et éthique de l'IA	8
4. Résultats attendus	8
II UNE MEILLEURE COMPRÉHENSION DE L'IA ET SES DIFFÉRENTES APPLICATIONS À PARTIR DE LA LITTÉRATURE EXISTANTE	9
A. Définition de la notion de l'IA	9
B. Quelques exemples d'usages de l'IA	10
C. IA et respect des droits et libertés fondamentaux	12
III EXPLOITATION ET SYNTHÈSE DES TEXTES POLITIQUES, JURIDIQUES ET ÉTHIQUES RELATIFS À L'IA AUX NIVEAUX INTERNATIONAL, CONTINENTAL ET RÉGIONAL	14
A. Au niveau international	14
B. Au niveau européen	17
C. Au niveau continental	20
IV EXPLOITATION ET SYNTHÈSE DES TEXTES POLITIQUES, LÉGAUX, RÉGLEMENTAIRES ET ÉTHIQUES DES QUATRE PAYS CIBLES (SÉNÉGAL, BENIN, BURKINA FASO ET CÔTE D'IVOIRE) ET QUELQUES PAYS CHOISIS POUR LEUR EXPÉRIENCE SUR L'IA	24
A. Exploitation et Synthèse des textes politiques, juridique et institutionnel des quatre pays cibles (Sénégal, Benin, Burkina Faso, Côte d'ivoire)	24
1 Sénégal	24
1.1 Cadre politique	24
1.2 Cadre juridique	25
1.3 Cadre institutionnel	27
2. Côte d'ivoire	28
2.1 Cadre politique	28
2.2 Cadre juridique	29
2.3 Cadre institutionnel	32
3. Benin	32
3.1 Cadre politique	32
3.2 Cadre juridique	33
3.3 Cadre institutionnel	36
4. Burkina Faso	37

4.1 Cadre politique	37
4.2 Cadre juridique	38
4.3 Cadre institutionnel	40
B. Exploitations et des synthèses des textes politiques, législatifs et éthiques d'autres pays (France, Canada, Maroc, Kenya, Ile Maurice)	40
1. France	40
2. Canada	42
3. Ile Maurice	43
4. Maroc	45
5. Kenya	46
V CONCLUSION	48
VI BIBLIOGRAPHIE	49

LISTE DES SIGLES ET ABREVIATIONS

AIDA	Commission spéciale sur l'intelligence artificielle à l'ère du numérique
APDP	Autorité de Protection des données à caractère personnel
ARTCI	Autorité de Régulation des Télécommunications de Côte d'Ivoire
CDP	Commission des données personnelles
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
DPO	Délégué à la protection des données à caractère personnel
IA	Intelligence artificielle
IoT	Internet of things (en français « Internet des objets »)
LOSI	Loi d'orientation sur la Société de l'Information
MOOC	Massive Open Online Course
OCDE	Organisation de Coopération et de Développement Economiques
ODD	Objectifs de développement durable
SAAD	Systèmes Algorithmique d'Aide à la Décision
SNCS	Stratégie Nationale de Cybersécurité du Burkina Faso
TIC	Technologies de l'Information et de la Communication
UA	Union Africaine
UE	Union européenne
UIT	Union Internationale des Télécommunications
UNESCO	Organisation des Nations Unies pour l'Education, la Science et la Culture

La présente revue documentaire a pour objet de disposer d'informations exhaustives sur le cadre politique, juridique et éthique de l'intelligence artificielle, des technologies émergentes, et données, principalement dans les quatre pays cibles du projet à savoir le Bénin, le Sénégal, le Burkina Faso et la Côte d'Ivoire.

A titre comparatif, cette étude sera également étendue dans d'autres pays d'Afrique et au niveau international.

Au niveau africain, un tour sera fait sur le cadre institutionnel et juridique de quelques pays à savoir l'Ile Maurice, le Maroc, le Kenya au vu des avancées importantes notées dans ces pays en matière d'IA.

Au niveau européen, l'accent sera porté sur la France, au vu de sa proximité juridique avec les pays d'Afrique notamment avec les pays cibles du projet.

En guise de benchmarking, il serait également pertinent voir primordial de s'intéresser aux pionniers en matière d'IA. Ainsi, en Amérique, le choix sera porté sur le Canada qui fait partie des premiers pays à disposer d'un instrument stratégique sur les systèmes d'intelligence artificielle.

Après avoir posé des éléments de définition des systèmes d'IA et donner des exemples de ses applications notamment dans les domaines de la santé, de l'éducation, de l'agriculture (II), secteurs clefs et prioritaires des quatre pays cibles du projet, il sera fait une synthèse des textes politique, juridique et éthique au niveau international (III) et une synthèse des textes politique, juridique et éthique au niveau des quatre pays cibles et des autres pays choisis (IV).

1. Rappel du Contexte

Les systèmes d'intelligence artificielle (IA) sont des outils qui occupent de plus en plus notre quotidien et ils peuvent également devenir des outils essentiels du développement. Ils ne constituent pas une fin en soi, mais ils doivent être considérés comme un moyen, un outil pour concourir à la résolution des difficultés dans des domaines comme l'agriculture, l'éducation, la santé et l'environnement. Lorsqu'ils sont utilisés à bon escient, ils peuvent donner toute la mesure de leur immense potentiel au service du développement social et économique. Toutefois, l'IA peut causer des impacts économiques et sociétaux négatifs tels que la transcendance des droits fondamentaux, la dégradation de l'environnement, du climat et des écosystèmes, l'exacerbation des inégalités économiques et sociales, le bouleversement du marché de l'emploi et l'abaissement de la qualité de vie.

En Afrique, les nouvelles technologies et l'intelligence artificielle se développent de plus en plus. Ainsi, au Sénégal, il a été mis en place un centre de données (« data center ») pour le stockage d'une masse de données et la production de grandes quantités d'informations. Le Bénin s'est doté d'une infrastructure identique¹ alors que l'utilisation grandissante d'internet et la fréquentation des réseaux sociaux en Afrique, permet un accès à une plus grande quantité de données personnelles (Global Digital), il s'avère nécessaire de mettre en place des dispositions réglementaires, législatives et politiques afin de parvenir à une applicabilité technique et sociétale sécurisée de l'IA.

La revue documentaire vise à générer des connaissances sur les cadres politiques, juridiques en lien avec l'IA dans quatre (4) pays d'Afrique francophone afin d'informer les politiques et les stratégies pour une IA responsable.

2. Définition

Le cadre politique peut se définir comme tous les instruments de politiques publiques et stratégiques mis en œuvre par un Etat, une organisation régionale et internationale sur un sujet donné. Quant au cadre juridique il s'agit de toutes les lois et règlements en vigueur dans un Etat permettant d'encadrer un domaine. L'éthique peut être définie comme la morale, les valeurs et les règles de conduite d'une société donnée.

Le cadre politique, juridique et éthique de l'AI peut donc se définir comme tous le instruments politiques et stratégiques, les lois et règlements et les règles éthiques afférents à l'intelligence artificielle adoptés au niveau national notamment dans les pays cibles du projet, régional et international.

¹ <http://www.osiris.sn/Benin-premiers-tests-techniques.html>

3. Objectifs de la revue documentaire du cadre politique, législatif, réglementaire et éthique de l'IA

L'objectif principal de la revue consiste à faire une recherche et étude des différents textes politiques, juridiques et éthiques internationaux, continentaux, régionaux, et nationaux, à l'intelligence artificielle et aux technologies émergentes

De façon spécifique, il s'agira :

- Comprendre et de cerner la notion de l'IA ainsi que ses différentes applications ;
- Faire un état des lieux des cadres politiques, juridiques et éthiques relatifs à l'IA, tant au niveau national, régional, continental et qu'international ;
- Sélectionner les documents les plus pertinents en lien avec la thématique abordée ;
- Exploiter les différentes informations contenues dans les documents sélectionnés ;
- Synthétiser les informations recueillies.

4. Résultats attendus

Les résultats attendus sont les suivants :

- Une meilleure compréhension de l'IA et ses différentes applications ;
- Exploitation et synthèse des textes politiques, juridiques et éthiques relatifs à l'IA aux niveaux international, continental et régional ;
- Exploitation et Synthèse des textes politiques, légaux, réglementaires et éthiques des quatre pays cibles (Sénégal, Benin, Burkina Faso et Côte d'Ivoire) et quelques pays choisis pour leur expérience sur l'IA.

A. Définition de la notion de l'IA

Le monde fait face à ce qu'on peut considérer comme une quatrième révolution industrielle avec comme locomotive, le numérique. Ce dernier est marqué par de profondes mutations résultant notamment des systèmes d'Intelligence artificielle (IA) et autres technologies émergentes.

La notion d'IA est apparue dans les années 1950 avec les auteurs tels que John McCarthy, Marvin L. Minsky, Nathaniel Rochester et Claude E. Shannon qui proposaient de mener une « étude de l'intelligence artificielle (...) »².

Mais, que recouvre vraiment cette notion ? Il faut d'abord noter que l'expression « intelligence artificielle » vient de la traduction en anglais de « Artificiel Intelligence ». Or, le mot « Intelligence » n'a pas forcément la même signification en anglais qu'en français, ce qui renforce le flou et l'incompréhension de cette notion. L'intelligence renvoie en anglais aux capacités mentales ou à des informations³ alors qu'en français l'intelligence est relative à la « *faculté de comprendre, de connaître* ou « *l'ensemble des fonctions mentales ayant pour objet la connaissance rationnelle* »⁴.

Le mot « artificiel » quant à lui, est défini comme ce « qui est le produit de l'activité, de l'habileté humaine »⁵. Le regroupement de ces deux mots composant l'expression « intelligence artificielle », n'éclaire pas davantage sur cette notion.

Il faut dire qu'il n'existe pas de définition universelle de la notion d'intelligence artificielle.

Plusieurs définitions de l'IA ont été posées par des organisations internationales telles que l'UNESCO, l'OCDE, et le Parlement européen.

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* »⁶.

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 influencer sur des environnements physiques ou virtuels. Différents systèmes d'IA présentent des degrés variables d'autonomie et d'adaptabilité après déploiement* »⁷.

Toujours, dans cette perspective de tentative de définition de cette notion, le Parlement européen, à travers la commission spéciale AIDA⁸, considère que le terme IA est un terme générique qui renferme diverses 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* »⁹. 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* »¹⁰.

2 Etude préliminaire sur l'éthique de l'intelligence artificielle, SHS/COMEST/EXTWG-ETHICS AI/2019/1 https://unesdoc.unesco.org/ark:/48223/pf0000367823_fre

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

4 <https://dictionnaire.lerobert.com/definition/intelligence>

5 <https://dictionnaire.lerobert.com/definition/artificiel>

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

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

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

9 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

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

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* »¹¹. 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* »¹² 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 question¹³. 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)** »¹⁴, 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.

B. Quelques exemples d'usages de l'IA

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 boîtes 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.

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. A titre illustratif des applications de l'IA dans le domaine de la santé, au Sénégal, la start-up XAIL¹⁵, a conçu un système IA permettant une détection précoce du cancer du cerveau à base d'images radiographiques et a même reçu

11 <https://fr.wikipedia.org/wiki/Algorithme>

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

13 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

14 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-%20Intelligence%20artificielle%20et%20droits%20fondamentaux%2C%20avril%202022.pdf>

15 Stratégie nationale sur l'Intelligence artificielle, Sénégal

un premier financement de Villgro Africa.¹⁶ 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 support¹⁷.

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)¹⁸ et conformément au consensus de Beijing sur l'intelligence artificielle et l'éducation adopté en 2019¹⁹.

En effet, on note depuis quelques années l'apparition des MOOC (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'IA²⁰

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 étudiants²¹. L'IA va donc contribuer à ajouter une dimension très importante à l'éducation via la personnalisation. 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 accroître la production agricole. Actuellement, le monde est résolument tourné vers le e-agriculture²² 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 maîtrise 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 tâches nécessitant impérativement l'intervention humaine.

16 Stratégie nationale, op citée

17 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

18 <https://fr.unesco.org/themes/tic-education/intelligence-artificielle>

19 <https://unesdoc.unesco.org/ark:/48223/pf0000368303>

20 Stratégie nationale op citée

21 Stratégie nationale op citée.

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

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.²³ 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.²⁴

C. IA et respect des droits et libertés fondamentaux

Malgré les 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)²⁵ 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 pas possible notamment pour les acteurs du pouvoir judiciaire 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 entraîne 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 substituer à eux. Il en est ainsi par exemple de l'application permettant de vieillir les personnes disparues accroissant les chances de les retrouver²⁶. 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 reconnaître, un algorithme n'est pas totalement objectif, il n'est que le reflet des choix et des données fournies par son programmeur. 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.²⁷ 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 hommes²⁸. 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 générerait pour l'entreprise, avait exclu ces zones de service de livraison gratuite. Or, ces zones sont majoritairement habitées par des populations défavorisées²⁹.

23 Stratégie nationale op citée

24 Stratégie nationale op citée

25 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-%20Intelligence%20artificielle%20et%20droits%20fondamentaux%2C%20avril%202022.pdf> page 10

26 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

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

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

29 op cité

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 préférences³⁰. L'IA pourrait également constituer 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 contraires³¹. 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 personnes³².

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* »³³. 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* »³⁴. Toutefois, en dépit de ces recommandations, il s'avère nécessaire 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 108³⁵ sur la protection des données à caractère personnel, un texte similaire applicable en matière d'IA³⁶. Au niveau africain, l'Union africaine a adopté une résolution visant 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'UNESCO³⁷.

30 CNIL op cité, page 36

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

32 Op citée

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

34 *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>

35 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>

36 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-%20Intelligence%20artificielle%20et%20droits%20fondamentaux%2C%20avril%202022.pdf>

37 UNESCO, *Evaluation des besoins en Intelligence artificielle en Afrique*, 2021, 86 pages, <https://unesdoc.unesco.org/ark:/48223/pf0000375321>



EXPLOITATION ET SYNTHÈSE DES TEXTES POLITIQUES, JURIDIQUES ET ÉTHIQUES RELATIFS À L'IA AUX NIVEAUX INTERNATIONAL, CONTINENTAL ET RÉGIONAL

Cette section sera consacrée à l'exploitation et à la synthèse des documents pertinents applicable au développement et à l'utilisation des systèmes de l'IA recensés aux niveaux international, continental et régional.

A. Au niveau international

- **Textes de l'ONU**

- **Résolution de l'ONU en date du 21 mars 2024** « Saisir les possibilités offertes par des systèmes d'intelligence artificielle sûrs, sécurisés et dignes de confiance pour le développement durable »

L'Assemblée générale de l'ONU, réunie lors de sa soixante-dix huitième session, a adopté par consensus la première résolution onusienne sur l'IA, le 21 mars 2024. Les Etats membres de l'ONU se déclarent résolus à favoriser des systèmes d'IA sûrs, sécurisés et dignes de confiance en vue d'accroître la réalisation du Programme 2030 dans son intégralité tout en comblant le fossé numérique entre les pays et à l'intérieur d'un même pays dans l'optique d'atteindre les objectifs de développement durables dans ses trois dimensions : économique, sociale et environnementale. L'Assemblée générale met l'accent sur la nécessité de mettre en place des principes et des cadres réglementaires et de gouvernance par les Etats membres conformément à leurs propres politiques et priorités internes, permettant de régir des systèmes d'IA sûrs, sécurisés, dignes de confiance pouvant créer un écosystème favorable à tous les niveaux et dignes de confiance. L'Assemblée générale invite à une coopération Nord-Sud et une assistance technique au pays en développement pour favoriser un accès inclusif et équitable aux avantages procurés par les systèmes de l'IA sûrs et dignes de confiance. L'Assemblée générale souligne l'importance de protéger et de promouvoir les droits humains et des libertés fondamentales tout au long du cycle de vie des systèmes de l'IA. A ce titre, l'Assemblée générale demande aux Etats membres de s'abstenir ou de cesser d'utiliser les systèmes d'IA non respectueux des droits humains ou présentant des risques importants pour les droits humains. Enfin, l'Assemblée générale reconnaît l'importance capitale des données dans la mise au point et le fonctionnement des systèmes de l'IA et de la nécessité d'avoir une gouvernance des données inclusive, juste, responsable et efficace pour mettre les potentialités des systèmes de l'IA au service du développement durable. Dans ce cadre, les Etats membres sont invités à échanger les meilleures pratiques en matière de gouvernance des données et faciliter la coopération en ce sens.

- **Recommandation de l'UNESCO sur l'éthique de l'intelligence artificielle, novembre 2021.**

L'UNESCO a adopté, le 23 novembre 2021, la **Recommandation sur l'éthique de l'intelligence artificielle** (IA), premier instrument normatif mondial sur le sujet. La 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 Pays les moins avancés (PMA).

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 :
- Sécurité et sécurité :
- Équité et non-discrimination :
- Durabilité :
- Droit au respect de la vie privée et protection des données :
- Surveillance et décision humaines :
- Transparence et explicabilité :
- Responsabilité et redevabilité ;
- Sensibilisation et éducation :
- Gouvernance et collaboration multipartites et adaptatives :

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.

- **Consensus de Beijing sur l'intelligence artificielle**

Le Consensus de Beijing sur l'intelligence artificielle et l'éducation a été adopté en 2019 à Beijing en Chine dans le Cadre de la Conférence internationale sur l'intelligence artificielle et l'éducation par les ministres et les représentants internationaux représentant plus de 100 États membres de l'UNESCO, des organisations, d'organismes des Nations unies, d'établissements universitaires, de société civile et de secteur privé. Ainsi, dans le cadre du programme de développement durable à l'horizon 2030 (Programme 2030) et en particulier l'objectif de développement durable 4 (ODD 4) et ses cibles, tout en reconnaissant l'importance de l'IA dans le secteur éducatif, l'évolution rapide de cette technologie et la place centrale de l'humain dans le développement de cette technologie, il est recommandé aux gouvernements des États membres de l'UNESCO, d'envisager de mettre en œuvre conformément à leur législation, leurs politiques publiques et leurs pratiques, les mesures en vue de prendre en compte les possibilités et les défis que représente l'IA dans le domaine de l'éducation. Ces mesures sont les suivantes :

- Planifier l'IA dans les politiques de l'éducation ;

- Mettre l'IA au service de la gestion et de la mise en œuvre de l'éducation ;
- Mettre l'IA au service de l'autonomisation des enseignants et de leur enseignement ;
- L'IA au service de l'apprentissage et de l'évaluation des acquis ;
- Développer les valeurs et compétences nécessaires dans la vie et au travail à l'ère de l'IA ;
- L'IA comme moyen d'offrir à tous des possibilités d'apprentissage tout au long de la vie ;
- Promouvoir une utilisation équitable et inclusive de l'IA dans l'éducation ;
- Promouvoir une IA respectueuse de l'équité entre les genres et propice à l'égalité des genres ;
- Veiller à une utilisation éthique, transparente et vérifiable des données et des algorithmes de l'éducation ;
- Faire un Suivi, évaluation et recherche de l'IA
- Financement, partenariats et coopération internationale par une évaluation et surveillance des incidences de la fracture créée par l'IA, la coordination des actions collectives par une utilisation équitable de l'IA, le renforcement de la coopération internationale orientée vers les besoins nationaux et la création de plateforme facilitant les échanges internationaux sur les cadres réglementaires.

- **Les Orientations de l'OMS, Éthique et gouvernance de l'intelligence artificielle pour la santé**

L'Organisation mondiale de la Santé à l'instar de l'UNESCO, a publié un document d'orientation posant six principes éthiques pour servir de base aux gouvernements, aux concepteurs de technologies, aux entreprises, la société civile et aux organisations intergouvernementales pour mettre l'IA au service de la santé d'une manière conforme à l'éthique.

Les principes éthiques sont les suivants :

- Protéger l'autonomie de l'humain : l'utilisation de l'IA ne porte pas atteinte à l'autonomie de l'être humain. Dit autrement, l'humain doit être maître des systèmes de soins de santé et des décisions médicales ;
- Promouvoir le bien-être et la sécurité des personnes et l'intérêt public : les concepteurs doivent satisfaire aux exigences en matière de sécurité, d'exactitude, et d'efficacité pour des utilisations ou des indications bien définies ;
- Garantir la transparence, l'explicabilité et l'intelligibilité : faire en sorte de rendre les technologies de l'IA soient plus transparentes et les rendre plus explicables afin qu'elles soient intelligibles ou compréhensibles pour les développeurs, les professionnels de la santé, les patients, les utilisateurs, et les législateurs ;
- Favoriser la responsabilité et la responsabilisation : indiquer clairement et de manière transparente aux humains les tâches que les systèmes peuvent effectuer et les conditions dans lesquelles ils peuvent produire les résultats souhaités ;
- Garantir l'inclusion et l'équité : l'intelligence pour la santé doit être conçue de manière à encourager une utilisation et un accès appropriés et équitables les plus larges possibles, indépendamment de l'âge, du sexe, de race, genre, revenu, appartenance ethnique, orientation sexuelle, des capacités ou caractéristiques protégées par les codes des droits de l'homme ;
- Promouvoir une IA réactive et durable : Les concepteurs, développeurs, et des utilisateurs doivent évaluer de manière continue, systématique, et transparente les applicables IA lors de leur application effective. Les gouvernements et entreprises anticipent les perturbations sur le lieu de travail, notamment en formant les agents de santé pour qu'ils s'adaptent à l'utilisation de l'IA et els pertes d'emploi pouvant découler de l'utilisation des systèmes automatisés.

- **Texte de l'OCDE**

- **Recommandation de l'OCDE sur l'IA**

La Recommandation de l'OCDE sur l'intelligence artificielle a été adoptée 2019. Elle vise à stimuler l'innovation et renforcer la confiance dans l'IA en promouvant une approche responsable au service d'une IA digne de confiance tout en garantissant les droits humains et les valeurs démocratiques. La recommandation a été révisée en 2024 pour tenir en compte les évolutions rapides de l'IA et des actions des pouvoirs publics en la matière.

La Recommandation pose cinq principes qui sont complémentaires. Les membres adhérents à la Recommandation sont invités à promouvoir et à mettre en œuvre ces principes pour une approche responsable de l'IA. Ces principes sont les suivants :

- **Principe 1 : Croissance inclusive, développement durable et bien-être** : Ce Principe souligne le potentiel de contribution à la croissance et la prospérité qu'aurait une IA digne de confiance à différents niveaux – individuel, sociétal, planétaire – et de faire progresser les objectifs de développement mondiaux tels que les objectifs de développement durable (ODD).
- **Principe 2 : Valeurs centrées sur l'humain et équité** : Les systèmes d'IA doivent être conçus de façon à respecter l'État de droit, les droits de l'Homme, les valeurs démocratiques et la diversité, tout en prévoyant les garde-fous nécessaires à assurer le caractère juste et équitable de la société.
- **Principe 3 : Transparence et l'explicabilité** : Ce principe porte sur la transparence et la divulgation responsable d'informations concernant les systèmes d'IA afin de garantir que les utilisateurs soient en mesure de comprendre et de mettre en question les résultats produits par les systèmes d'IA.
- **Principe 4 : Robustesse, sûreté et sécurité** : Les systèmes d'IA doivent fonctionner de façon robuste, sûre et sécurisée tout au long de leur cycle de vie, et les risques potentiels devraient être continuellement évalués et gérés.
- **Principe 5 : Responsabilité** : Les organismes et individus amenés à développer, déployer et utiliser les systèmes d'IA devraient être tenus responsables de leur bon fonctionnement, en adéquation avec les Principes de l'OCDE pour l'IA fondés sur des valeurs.

En plus de ces principes, il est recommandé aux membres adhérents dans le cadre de leur politiques nationales et la coopération internationale, d'investir dans la recherche et le développement en matière de l'IA, favoriser un écosystème inclusif propice de l'IA, façonner un cadre d'action et de gouvernance interopérable favorable de l'IA, renforcer les capacités humaines et préparer la transformation du marché du travail et favoriser la coopération internationale au service d'une IA responsable.

B. Au niveau européen

- **Textes du Conseil de l'Europe**
- **Convention de Budapest sur la cybercriminalité**

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 infantile ; (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 efficace. 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. Les restrictions sont définies de manière étroite puisque seules certaines infractions spécifiques constitutives d'un crime passible de la justice pénale font l'objet d'enquêtes et poursuites et que les données spécifiées nécessaires comme preuves dans des procédures pénales spécifiques sont garanties sous réserve des protections liées aux droits de l'homme et à l'État de droit.³⁸

- **Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108 +)**

Reconnaissant la nécessité de promouvoir les valeurs fondamentales du respect de la vie privée et de la protection des données à caractère personnel à l'échelle mondiale, favorisant ainsi la libre circulation de l'information entre les peuples, les États membres du Conseil de l'Europe et l'Union européenne ont mis en place une convention ayant pour de protéger les données à caractère personnel.³⁹ C'est ainsi que la présente convention est adoptée. Le but de la présente Convention est de protéger toute personne physique, quelle que soit sa nationalité ou sa résidence, à l'égard du traitement des données à caractère

38 [1] <https://rm.coe.int/t-cy-2020-16fr-bc-benefits-rep-prov-1/16809efc6c#:~:text=La%20Convention%20de%20Budapest%20pr%C3%A9voit,enqu%C3%AAter%20dans%20des%20affaires%20de>

39 [16808b3726 \(coe.int\)](https://rm.coe.int/16808b3726)

personnel, contribuant ainsi au respect de ses droits de l'homme et de ses libertés fondamentales et notamment du droit à la vie privée.

La convention fixe à cinq le nombre de ratifications d'États membres du Conseil de l'Europe nécessaires pour son entrée en vigueur.⁴⁰

- **Textes de l'Union Européenne (UE)**
- **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)**

Le parlement européen a adopté en 2024 le Règlement européen établissant des règles harmonisées concernant l'IA, première réglementation sur l'intelligence artificielle. Ce règlement se donne pour objectif d'améliorer le fonctionnement du marché intérieur de l'union en établissant un cadre uniforme, en particulier pour le développement, la mise sur le marché, la mise en service et l'utilisation des systèmes d'IA dans le respect des valeurs de l'union, de promouvoir l'adoption de l'IA axée sur l'humain digne de confiance tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte»), y compris la démocratie, l'état de droit et la protection de l'environnement, de protéger contre les effets néfastes des systèmes d'IA dans l'Union, et de soutenir l'innovation. Le règlement européen sur l'IA garantit la libre circulation transfrontière des biens et services fondés sur l'IA, empêchant ainsi les États membres d'imposer des restrictions au développement, à la commercialisation et à l'utilisation de systèmes d'IA, sauf autorisation expresse du présent règlement⁴¹.

Fondé sur une approche par risque, le règlement européen établit des obligations à la charge des fournisseurs et les utilisateurs en fonction du risque lié à l'IA. Ainsi, plus les risques sont élevés, plus les règles régissant le système sont strictes. Le règlement prévoit plusieurs niveaux de risques. Le premier constitue l'interdiction de certaines pratiques de l'IA considérées comme inacceptables et donc interdites. Ces pratiques sont celles visant à manipuler le comportement de personnes et susceptibles de leur causer un préjudice psychologique ou physique ; celles visant à exploiter la vulnérabilité d'une personne ou d'un groupe de personnes ; la notation sociale ; et l'identification biométrique à distance et en direct dans un espace accessible au public et à des fins d'application du droit.

Le deuxième niveau concerne la mise sur le marché ou en service de « systèmes d'IA à haut risque ». Ces systèmes sont ceux susceptibles d'engendrer un risque pour la santé, la sécurité ou les droits fondamentaux des individus.

La réglementation porte également sur l'utilisation des modèles d'IA général, qui dès lors qu'ils ne présentent pas de risques systémiques, seront soumis à des exigences limitées. Le règlement européen pose des exigences de transparence notamment pour l'IA générative telle le ChatGPT. Ce type d'IA doit se conformer aux exigences de transparence et à la législation de l'UE sur le droit d'auteur.

Pour terminer, le règlement prévoit un cadre juridique favorable à l'innovation par l'adoption de bac à sables réglementaires offrant un environnement contrôlé pour le développement, l'essai et la validation de systèmes d'IA innovants.

- **Règlement (UE) 2016/679 Du Parlement Européen Et Du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)**

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée « Charte ») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données à caractère personnel la concernant. Les principes et les règles régissant la protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant devraient respecter leurs libertés et droits fondamentaux, en particulier leur droit à la protection des données à caractère personnel.

⁴⁰ Article 26 de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108 +)

⁴¹ pdf (europa.eu) Législation sur l'intelligence artificielle (IA): le Conseil donne son feu vert définitif aux premières règles mondiales en matière d'IA - Consilium (europa.eu)

La réalisation de cet espace respectueux des droits et libertés des personnes par rapport à leurs données à caractère personnel dépend largement la mise en place d'un cadre juridique harmonisé et innovant. Conscients des enjeux liés aux données à caractère personnel, les dirigeants européens ont senti la nécessité de mettre en place des outils juridiques garantissant les droits fondamentaux des personnes, quelle que soit la nationalité ou la résidence de celles-ci. Ce qui justifie ainsi l'adoption de ce Règlement (UE) 2016/679 Du Parlement Européen Et Du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données qui s'applique directement au niveau des Etats membres de l'Union depuis son entrée en vigueur le 25 mai 2018.

Le présent règlement devrait s'appliquer à tous les aspects de la protection des libertés et droits fondamentaux à l'égard du traitement des données à caractère personnel qui ne sont pas soumis à des obligations spécifiques ayant le même objectif énoncé dans la directive 2002/58/CE du Parlement européen et du Conseil, y compris les obligations incombant au responsable du traitement et les droits des personnes physiques⁴². Ainsi, le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier⁴³.

- **Livre blanc sur l'intelligence artificielle**

L'intelligence artificielle (IA) se développe rapidement. Elle va entraîner des changements dans nos vies en améliorant les soins de santé (précision accrue des diagnostics ou meilleure prévention des maladies, par exemple), en rendant l'agriculture plus efficiente, en contribuant à l'adaptation au changement climatique et à l'atténuation de ses effets, en augmentant l'efficacité des systèmes de production par la maintenance prédictive, en renforçant la sécurité des Européens et de bien d'autres façons que nous commençons à peine à entrevoir. Mais elle s'accompagne aussi d'un certain nombre de risques potentiels, tels que l'opacité de la prise de décisions, la discrimination fondée sur le sexe ou sur d'autres motifs, l'intrusion dans nos vies privées ou encore l'utilisation à des fins criminelles⁴⁴.

Il faut par conséquent adopter une approche européenne commune en matière d'IA pour parvenir à une échelle suffisante et éviter la fragmentation du marché unique. La mise en place d'initiatives à l'échelle nationale pourrait nuire à la sécurité juridique, affaiblir la confiance des citoyens et empêcher l'apparition d'une industrie européenne dynamique. C'est dans cette dynamique que le présent Livre blanc est élaboré. Il expose ainsi des options qui permettront un développement sûr et digne de confiance de l'IA en Europe, dans le plein respect des valeurs et des droits des citoyens européens.

- **Lignes directrices en matière d'éthique pour une IA digne de confiance**

Elaborées par le groupe d'expert indépendants de haut niveau sur l'intelligence artificielle constitué par la commission européenne, les lignes directrices⁴⁵ visent à promouvoir une IA digne de confiance. Une IA digne de confiance présente les trois caractéristiques suivantes, qui devraient être respectées tout au long du cycle de vie du système : a) elle doit être licite, en assurant le respect des législations et réglementations applicables ; b) elle doit être éthique, en assurant l'adhésion à des principes et valeurs éthiques ; et c) elle doit être robuste, sur le plan tant technique que social car, même avec de bonnes intentions, les systèmes d'IA peuvent causer des préjudices involontaires.

Les lignes directrices établissent un cadre pour parvenir à la réalisation d'une IA digne de confiance. Ce cadre ne traite pas explicitement de la première caractéristique d'une IA digne de confiance (IA licite). Il vise plutôt à proposer des orientations pour encourager et garantir une IA éthique et robuste (les deuxième et troisième caractéristiques). S'adressant à l'ensemble des parties prenantes, les présentes lignes directrices cherchent, en plus de présenter une liste de principes éthiques, à fournir des orientations sur la manière dont ces principes peuvent être mis en œuvre dans des systèmes sociotechniques.

Les lignes directrices sont destinées à l'ensemble des parties prenantes de l'IA qui conçoivent, mettent au point, déploient, mettent en œuvre, utilisent l'IA ou sont soumises à ses incidences, et notamment aux entreprises, aux organisations, aux chercheurs, aux services publics, organismes gouvernementaux, institutions, organisations de la société civile, particuliers, travailleurs et consommateurs. Elles définissent

42 <http://data.europa.eu/eli/reg/2016/679/oj>

43 Article 2 du Règlement (UE) 2016/679 Du Parlement Européen Et Du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

44 [Livre-blanc-sur-l'intelligence-artificielle.pdf \(auvergnerhonealpes.fr\)](#)

45 Commission européenne, Direction générale des réseaux de communication, du contenu et des technologies, Lignes directrices en matière d'éthique pour une IA digne de confiance, Publications Office, 2019, <https://data.europa.eu/doi/10.2759/74304>

ainsi un cadre pour parvenir à la mise en œuvre d'une IA digne de confiance fondée sur les droits fondamentaux tels que consacrés dans la charte des droits fondamentaux de l'Union européenne (charte de l'UE), et dans le droit international pertinent en matière de droits de l'homme.⁴⁶.

- **Recommandations en matière de politique et d'investissement pour une IA digne de confiance⁴⁷.**

L'intelligence artificielle promet d'améliorer la prospérité et le bien-être des individus, de contribuer à une activité économique mondiale dynamique et durable, de stimuler l'innovation et la productivité, et d'aider à affronter les grands défis planétaires. Ces transformations pourraient avoir des effets disparates d'une société et d'une économie à l'autre et en leur sein, notamment en termes de mutations économiques, de concurrence, de transitions sur les marchés du travail, d'inégalités, et de conséquences sur la démocratie et les droits de l'homme, la protection de la vie privée et la confidentialité des données, et la sécurité numérique. C'est donc en ce sens qu'un ensemble de recommandations de politique et d'investissement a été fait. Il s'agit d'expliquer comment une IA de confiance peut être mise en place, déployée, encouragée et étendue à toute l'Europe en profitant au maximum de ses bénéfices tout en minimisant et en prévenant ses risques

Ces recommandations concrètes au nombre de 33 sont adressées aux institutions européennes et aux États membres vont dans ce sens. Celles-ci se concentrent sur quatre domaines principaux dans lesquels une IA digne de confiance peut avoir un impact bénéfique, en commençant par les humains et la société en général, puis en se concentrant ensuite sur le secteur privé, le secteur public, la recherche et les universités européennes⁴⁸.

Dans le même temps, les principaux outils nécessaires pour faciliter ces impacts ont été examinés, en fonction de la disponibilité des données et de l'infrastructure, des compétences et de l'éducation, d'une gouvernance et d'une réglementation appropriées, ainsi que du financement et des investissements.

C. Au niveau continental

- **Textes de l'Union africaine**

- **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**

En reconnaissant que les technologies telles que l'intelligence artificielle (IA), la robotique et les autres technologies nouvelles et émergentes, présentent à la fois des opportunités et des dangers pour la promotion et la protection des droits de l'homme en Afrique, les dirigeants africains ont réaffirmé l'importance de l'accès à Internet à l'ère du numérique et ses implications pour la réalisation des droits de l'homme inscrits dans la Charte africaine et d'autres instruments des droits de l'homme de l'Union africaine (UA). C'est pourquoi, ces autorités africaines ont appelé les États parties à travers la commission de l'Union Africaine : « 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 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'intelligence artificielle, de la robotique et d'autres technologies nouvelles et émergentes ». Ainsi cette résolution invite les États à entreprendre les études 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 en collaboration avec un Groupe africain d'experts sur l'intelligence artificielle et les nouvelles technologies.⁴⁹ Cette présente recherche s'inscrit en droite ligne avec cette volonté des États parties à faire des études pour une meilleure prise en compte des technologies de l'intelligence artificielle dans les textes juridiques et politiques en Afrique.

46 KK0219841FRN.fr.pdf <https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trust-worthy-artificial-intelligence>

47 <https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trust-worthy-artificial-intelligence>

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

49 Résolution sur la nécessité d'élaborer une étude sur les droits de l'homme et des peuples et l'intelligence artificielle, la robotique et d'autres technologies émergentes, https://www.achpr.org/fr_sessions/resolutions?id=504

- **La Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel ;**

Le développement fulgurant du numérique est souvent accompagné de la violation des droits des personnes du fait de leur utilisation à mauvais escient. C'est pourquoi les autorités africaines ont manifesté l'urgence de mettre en place d'un dispositif juridique permettant de faire face aux dangers et risques nés de l'utilisation de l'informatique et des fichiers sur les individus dans le souci de respecter la vie privée et les libertés.

La convention a pour ambition de répondre aux besoins de législation harmonisée dans le domaine de la cyber sécurité dans les États membres de l'Union africaine ; elle 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 ; tout en prenant en compte les meilleures pratiques reconnues au niveau international.

En clair l'objet de cette convention vise donc à assurer la sécurité et le cadre juridique nécessaires à l'émergence de l'économie du savoir en Afrique.

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.⁵⁰

- **Le Cadre stratégique de l'Union Africaine de la donnée**

L'UA, consciente l'importance capitale de la donnée, pilier de la transformation numérique et levier important dans l'atteinte des objectifs de réalisation de l'Agenda 2063 et des objectifs de développement durable (ODD), a mis en place un cadre stratégique de la donnée⁵¹ adopté en 2022. Ce cadre a pour ambition d'offrir aux pays africains, la possibilité de s'assurer que les lois permettent de manière proactive l'accès des données à des fins d'innovation et de développement et de concurrence. Il fournit aux Etats membres des orientations fondées sur des principes pour faciliter son incorporation au niveau national de façon adaptée à leurs conditions et propose aussi un instrument ou un mécanisme pour intégrer et coordonner les efforts continentaux. Le cadre vise à renforcer les systèmes des données nationaux pour une utilisation efficace des données en créant un environnement favorable qui stimule l'innovation et l'esprit d'entreprise afin de favoriser le développement d'économies fondées sur la valeur des données. Ce cadre s'intéresse à la gouvernance des données qui comprend les données à caractère personnel, non personnel, industriel et public.

Les objectifs généraux du Cadre sont les suivants entre autres :

- Permettre aux Etats de coopérer sur des questions de gouvernance des données pour atteindre les objectifs communs liés au développement durable de leur économies et leurs sociétés ;
- Informer et soutenir l'internationalisation de la stratégie continentale par les pays africains ;
- Veiller à la circulation des données à travers les frontières aussi librement que possible, tout en favorisant une répartition équitable des bénéfices et en traitant les risques liés aux violations des droits de l'homme et autres intérêts légitimes des états
- Favoriser et faciliter le flux des données transfrontalières en augmentant les opportunités commerciales tout en garantissant un niveau adéquat de protection des données personnelles et de vie privée ;
- Faire en sorte que les données puissent circuler à travers les frontières aussi librement que possible, tout en favorisant une répartition équitable des avantages et en traitant les risques liés aux droits de l'homme et à la sécurité nationale ;
- Veiller à ce que les données soient utilisées d'une manière durable qui profite à la société dans son ensemble et ne porte pas atteinte à la vie privée, à la dignité et à la sécurité des personnes ;
- Faciliter les moyens innovants de promouvoir les avantages publics en utilisant les données de

50 Article 13 de la convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel

51 42078-doc-AU-DATA-POLICY-FRAMEWORK-FR.pdf

manière nouvelle, ce qui permettrait aux données en Afrique de réaliser la valeur des données dans la prise de décision, la planification, le suivi et l'évaluation du secteur public.

- **Stratégie de transformation numérique de l'Afrique 2020-2030**

La transformation numérique est une force motrice pour une croissance innovatrice, inclusive et durable. Qu'il s'agisse d'innovations telles que les plates-formes monétaires mobiles ou l'externalisation à grande échelle des processus commerciaux, la numérisation crée des emplois, s'attaque à la pauvreté, réduit les inégalités, facilite la fourniture de biens et de services et contribue à la réalisation de l'Agenda 2063 et des objectifs de développement durable (ODD) des Nations Unies. Consciente de cela, l'Union africaine a élaboré une stratégie de transformation numérique sur la période 2020-2030. La vision de cette stratégie est d'avoir une société et une économie numériques intégrées et inclusives en Afrique qui améliorent la qualité de vie des citoyens africains à l'horizon 2030.

Les objectifs spécifiques déclinés par la STN sont notamment :

- Construire un marché unique numérique sécurisé en Afrique d'ici 2030, où la libre circulation des personnes, des services et des capitaux est assurée et où les particuliers et les entreprises peuvent accéder de manière transparente aux activités en ligne et s'y engager, conformément à la zone de libre-échange continentale de l'Afrique (ZLECAf) ;
- Mettre en œuvre les politiques et les règlements nécessaires pour stimuler et accélérer la transformation numérique pour le développement national, régional et continental ;
- Favoriser la cohérence des politiques et stratégies numériques existantes et futures aux niveaux régional et national et mobiliser une coopération efficace entre les institutions.
- Favoriser l'entrée en vigueur de la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel d'ici à 2020 et adoption par tous les États membres d'un ensemble complet de textes législatifs couvrant les transactions électroniques, la protection des données et la vie privée, la cybercriminalité et la protection des consommateurs ;
- Promouvoir des normes ouvertes et l'interopérabilité pour un cadre de confiance transfrontalier, la protection des données personnelles et la vie privée. • Sensibiliser et équilibrer les questions de cybersécurité et de protection des données personnelles et de la vie privée.
- Développer des compétences numériques inclusives et des capacités humaines dans le domaine des sciences numériques et de l'éducation, tant techniques que professionnelles, pour diriger et alimenter la transformation numérique, y compris le codage, la programmation, l'analyse, la sécurité, la chaîne de blocs, l'apprentissage automatique, l'intelligence artificielle, la robotique, l'ingénierie, l'innovation, l'entrepreneuriat, et la politique et la réglementation technologique.

- **Textes de la CEDEAO**

- **Directive C/DIR/1/08111 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO**

Des défis restent donc à relever au niveau de l'adoption de législations par certains États, la formation des acteurs de mise en œuvre des lois pénales, la modernisation des méthodes et des moyens de recherche des preuves. Les actions communes de lutte aussi bien au niveau du droit pénal de fond que de forme restent des voies privilégiées de lutte contre les cybercrimes dans la région ouest-africaine. C'est pourquoi, les autorités de la sous-région ouest africaine ont matérialisé leur volonté à travers cette Directive pour l'adoption d'un cadre juridique harmonisé dans la lutte contre la cybercriminalité.

La présente 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 cybercriminalité⁵² 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 électronique⁵³. Cette Directive a déterminé 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.

- **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**

52 Article 2 de la Directive C/DIR/1/08111 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO

53 Article 3 de la Directive C/DIR/1/08111 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO

Adopté le 19 janvier 2007, l'Acte additionnel CEDEAO relatif à l'harmonisation des politiques et du cadre réglementaire du secteur des technologies, de l'information et de la communication (TIC) vise à créer un cadre harmonisé pour la politique et la réglementation des TIC. Il fixe les tâches incombant aux Etats membres et à leurs Autorités nationales de régulation respectives en dégagant les principes directeurs de la politique des TIC et les lignes de conduite en matière de régulation. Il établit une série de procédures visant à garantir l'application harmonisée du cadre réglementaires des Etats membres de la CEDEAO⁵⁴.

- **Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO⁵⁵**

L'Acte additionnel relatif à la protection des données à caractère personnel, adopté le 16 février 2010 vise à créer un cadre légal harmonisé dans le traitement des données à caractère personnel dans l'espace CEDEAO. Dans ce cadre, il impose aux Etats membres d'adopter un cadre légal de protection de la vie privée et professionnelle consécutive à la collecte, au traitement, à la transmission, au stockage et à l'usage des données à caractère personnel. Il pose les formalités nécessaires au traitement des données personnelles telles que la déclaration, l'autorisation et l'avis. L'acte additionnel impose aux Etats membres de créer une autorité de protection des données. L'Acte additionnel définit les principes directeurs régissant le traitement des données personnelles tels que le consentement, la légitimité, la licéité et la loyauté, l'exactitude, la transparence, la confidentialité et la sécurité. Il pose les droits des personnes dont les données font l'objet de traitement et les obligations qui pèsent sur le responsable du traitement.

54 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 (TIC) | CDP

55 CEDEAO - Acte additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO (www.droit-afrique.com) (afapdp.org)

EXPLOITATION ET SYNTHÈSE DES TEXTES POLITIQUES, LÉGAUX, RÉGLEMENTAIRES ET ÉTHIQUES DES QUATRE PAYS CIBLES (SÉNÉGAL, BENIN, BURKINA FASO ET CÔTE D'IVOIRE) ET QUELQUES PAYS CHOISIS POUR LEUR EXPÉRIENCE SUR L'IA

Au niveau national, il sera procédé à l'exploitation et la synthèse des textes politique et juridique relatifs à l'IA, des technologies émergentes et des données des pays cibles du projet. Dans une perspective de benchmarking, une analyse et synthèse des documents politiques, juridiques et éthiques, afférents aux systèmes d'IA, des technologies émergentes et des données, sera fait d'autres pays ((France, Canada, Maroc, Kenya, Ile Maurice), pour voir comment l'IA est appréhendée.

A. Exploitation et Synthèse des textes politiques, juridique et institutionnel des quatre pays cibles (Sénégal, Benin, Burkina Faso, Côte d'ivoire)

1. Sénégal

1.1 Cadre politique

- **Stratégie nationale du 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 » avec comme prérequis : « un cadre juridique et institutionnel » ; le « capital humain » ; « cadre de confiance ». La stratégie actualisée prend en compte moyennement les technologies émergentes et les systèmes d'IA. On le retrouve en filigrane dans le prérequis 2 : « Capital humain », avec la mise en place de module de formation en big data, cloud et IOT (internet of things)⁵⁶.

- **Stratégie de développement de l'Intelligence artificielle**

Le Sénégal a élaboré et publié sa stratégie nationale sur l'IA. Cette stratégie, qui s'inscrit dans le cadre plus large du Plan Sénégal émergent 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 2028⁵⁷. 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 dont le budget s'élève à 6,7 milliards pour les années 2024-2025. Ainsi, il est prévu entre autres de mettre 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.

⁵⁶ Stratégie nationale du Numérique 2025, Plans d'actions actualisé, <http://www.numerique.gouv.sn/sites/default/files/Strat%C3%A9gie%20Numerique-SN2025-%20Plan%20d%27actions%20actualis%C3%A9.pdf>

⁵⁷ 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, le Sénégal a pris l'option d'articuler stratégie sur l'IA à la stratégie nationale sur les données.

- **Stratégie nationale des Données (SND)**

Corrélativement à la stratégie nationale de développement de l'IA, le Sénégal a élaboré en 2023 stratégie sur les données en raison du fait que l'économie numérique mondiale est devenue essentiellement une économie de la donnée. Le Sénégal ambitionne ainsi de « faire de la donnée un moteur de croissance socioéconomique et de souveraineté numérique à l'horizon 2028 au Sénégal ». ⁵⁸ . Cette traduit la volonté du Sénégal de s'appuyer sur la donnée comme levier pour une meilleure inclusion sociale, un développement économique et moteur de la recherche et l'innovation.

La stratégie nationale des données reposent sur quatre orientations stratégiques : (1) Un cadre réglementaire favorable à l'exploitation du potentiel de la donnée au service du développement et de l'innovation, (2) des infrastructures hautement disponibles, performantes, sécurisées et abordables pouvant soutenir l'exploitation de la donnée au service des usages pour un développement socio-économique durable, (3) l'exploitation du potentiel de la donnée au service des usages pour un développement socio-économique durable, (4) Le renforcement des compétences en matière de données et établir une nouvelle culture de la donnée à l'échelle nationale. Il est notamment prévu d'élaborer un cadre de gouvernance des données avec l'élaboration d'une loi sur les données et la création d'une autorité chargée de la donnée, de renforcer le cadre des données ouvertes et la cybersécurité et l'intelligence artificielle. Le Sénégal prévoit également d'accélérer la mise en place d'un cloud national et d'opérationnaliser le supercalculateur. L'agriculture, la santé, l'éducation, l'environnement, le Tourisme, le transport, les statistiques et les mines sont été identifiés comme des secteurs dont l'exploitation des données pourrait contribuer à leur développement. Par ailleurs, des actions de sensibilisation sur l'intérêt et l'importance de la donnée, le renforcement de la formation sur la donnée et le renforcement de la recherche et innovation ont été identifiés.

- **Stratégie nationale de la Cybersécurité (2017-2022)**

Le Sénégal a également adopté la Stratégie nationale de la Cybersécurité (2017-2022) qui a pour objectifs majeurs : le renforcement du cadre juridique et institutionnel de la cybersécurité au Sénégal, la protection 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, et la participation aux efforts régionaux et internationaux de cybersécurité. Cette stratégie est arrivée à terme en 2022 doit être actualisée pour prendre en compte les technologies tels que l'IA qui est autant une menace qu'une opportunité pour la cybersécurité.

1.2 Cadre juridique

Dans le cadre législatif et réglementaire, le Sénégal a adopté en 2008 un paquet de lois dénommé "*paquet numérique*" composé d'un ensemble de lois portant sur le numérique. On peut citer notamment la loi d'orientation à portée générale sur la société de l'information, la loi sur la protection des données à caractère personnel, la loi sur les transactions électroniques la loi sur la cybercriminalité et la loi sur le droit d'auteur et droits voisins. Ces lois sont accompagnées pour la plupart de leurs décrets d'application. Ces lois, certes, ne portent pas spécifiquement sur l'IA, sont susceptibles de s'appliquer à ces systèmes.

- **La loi n° 2008 -10 du 25 janvier 2008 portant loi d'orientation sur la société de l'Information (LOSI)**

Cette loi pose les bases juridiques et institutionnelles de la société de l'information telle voulue par le Sénégal. Elle vise notamment à définir les objectifs et les grandes orientations de la société de l'information au Sénégal et à compléter la législation actuelle en matière de technologies de l'information et de la communication. Au sens de la loi LOSI, une 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** ». ⁵⁹

Dans la société de l'information, chaque individu a le droit et la liberté de créer, d'obtenir, d'utiliser et de partager l'information et le savoir dans le respect des lois et règlements en vigueur. Tous les individus, les

58 Résumé de Stratégie Nationale des Données du Se_230724_172910.pdf (numerique.gouv.sn)

59 Article 3 de la loi LOSI

communautés et les peuples y ont la possibilité de mettre en œuvre toutes leurs potentialités en vue de favoriser leur développement et d'améliorer leur qualité de vie »⁶⁰. L'utilisation des systèmes d'intelligence artificielle et technologie émergente s'inscrit parfaitement dans cette définition.

- **La loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel.**

Cette loi a pour objet de mettre en place 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 personnel⁶¹. Son champ d'application porte sur la collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel par une personne physique, par l'Etat, les collectivités locales, les personnes morales de droit public ou de droit privé et tout traitement :

- automatisé ou non de données contenues ou appelées à figurer dans un fichier ;
- mis en œuvre par un responsable sur le territoire sénégalais ou en tout lieu où la loi sénégalaise s'applique ; le traitement mis en œuvre par un responsable, établi ou non sur le territoire sénégalais, qui recourt à des moyens de traitement situés sur le territoire sénégalais, à l'exclusion des moyens qui ne sont utilisés qu'à des fins de transit sur ce territoire,
- des données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, même liées à un intérêt économique ou financier important de l'Etat⁶².

Sont exclues du champ d'application de cette loi , “ *les traitements de données mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition toutefois que les données ne soient pas destinées à une communication systématique à des tiers ou à la diffusion ; et les copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises*”⁶³.

La loi garantit que tout traitement, sous quelque forme que ce soit, respecte les libertés et droits fondamentaux des personnes physiques.

Elle veille à ce que les Technologies de l'Information et de la Communication (TIC) ne portent pas atteinte aux libertés individuelles ou publiques, notamment à la vie privée. C'est pourquoi le traitement des données à caractère personnel est soumis à des régimes de protection caractérisé par l'accomplissement de formalités préalables avant tout traitement. Ces formalités sont les suivantes : la déclaration, l'autorisation et l'avis.

Le traitement de données est soumis au respect des principe de loyauté, de confidentialité et de transparence. Au-delà du respect de ces principes, la loi a mis également à la charge du responsable de traitement de données, des obligations dont les manquements sont sanctionnés. Parallèlement aux obligations imposées au responsable de traitement de données, la loi accorde aux personnes dont les données sont recueillies, des droits permettant de garantir leur vie privée et leurs droits fondamentaux tels que le droit d'accès, de rectification, de suppression....

Accompagnée de **son décret d'application n° 2008-721 du 30 juin 2008**, la loi instaure une autorité indépendante, la Commission de Protection des Données (**CDP**) chargée de l'application et du contrôle de conformité.

Comme on l'a constaté, les systèmes d'intelligence artificielle requièrent l'usage d'une masse importante données parmi lesquelles les données à caractère personnel. Cette loi a besoin d'être révisée pour davantage s'adapter aux enjeux liés aux systèmes d'IA et des technologies émergentes. Toutefois, ils ne sont pas pour autant hors du champ de la loi.

Par ailleurs, il faut relever que le Sénégal est membre de la convention 108 sur la protection des données à caractère personnel et a entamé le processus de révision de la loi.

- **La loi n° 2008-41 du 20 aout 2008 sur la cryptologie**

Elle a pour objet de fixer les règles applicables aux moyens, modalités et systèmes de cryptologie composée

60 Article 3 op cité

61 Par données à caractère personnel on entend “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

62 Article 2 de la loi -12 du 25 janvier 2008 sur la protection des données à caractère personnel

63 Article 3 de la loi du 12 du 25 janvier 2008 sur la protection des données à caractère personnel

des techniques suivantes : la cryptographie et la cryptanalyse. Ainsi, ces techniques tendent à assurer la protection et la sécurité des informations transmises notamment la confidentialité, l'authentification, l'intégrité et la non répudiation des données transmises. A l'instar du traitement des données à caractère personnel, les opérations afférentes sont soumises à l'accomplissement de formalités : le régime de déclaration et le régime d'autorisation.

La loi a institué une autorité chargée de la conformité et de l'application des dispositions de la loi. Il s'agit de la commission nationale de cryptologie dont la composition, le fonctionnement et les attributions ont été précisées dans le **décret d'application n°2010-1209 du 13 septembre 2010**.

- **La loi n° 2008-11 du 25 janvier 2008 sur la Cybercriminalité**

Bien avant la ratification de la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel du 27 juin 2014 et la convention de Budapest sur la cybercriminalité du 23 novembre 2001⁶⁴ le Sénégal a adopté la loi n° 2008-11 du 25 janvier 2008 sur la Cybercriminalité qui a conduit à la modification du Code pénal et du code de la procédure pénale. Les dispositions introduites par la loi précitée ont été remplacées par la **loi n° 2016-29 du 08 novembre 2016 modifiant le code pénal**. Ces infractions instaurées sont relatives :

- À la confidentialité, l'intégrité et à la disponibilité des systèmes informatiques ;
- Aux données informatiques ;
- Aux droits de la personne au regard du traitement des données à caractère personnel.

- **La loi 2008-09 du 25 janvier 2008 sur le droit d'auteur et les droits voisins**

Cette loi a pour but de protéger les œuvres littéraires et artistiques en accordant des droits patrimoniaux et moraux. A ce titre, cette loi permet à l'auteur d'utiliser les techniques de protection informatiques telles que la cryptologie pour protéger son œuvre. La neutralisation de ces mesures de protection fait l'objet de sanctions pénales prévues par la loi.

Il faut relever que la loi est centrée sur le créateur humain, or, on voit émerger depuis quelques temps des œuvres protégeables par le droit d'auteur, réalisées par les systèmes d'IA, presque en toute autonomie à l'image du tableau « The Next Rembrandt »⁶⁵. Se pose alors des questions juridiques sur la titularité des droits. Doit-on accorder des droits à la machine au propriétaire de la matière à l'initiative de l'œuvre ? Toutes ces questions doivent susciter des réflexions en cas de révision de la loi sur le droit d'auteur.

- **La 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**

Concernant les activités statistiques qui constituent l'une des approches utilisées par le système d'intelligence artificielle, elles font l'objet de la 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. Cette loi a pour objet de définir les principes fondamentaux et le cadre institutionnel qui régissent les activités des services et organismes chargés du développement, de la production et de la diffusion des statistiques publiques. Elle traite du fonctionnement général du système statistique national et de la coordination au sein de ce système. La collecte et l'utilisation de données à des fins informatiques se doit dans le respect de la vie privée d'où la nécessité d'assurer la confidentialité des données et de les utiliser qu'à des fins de diffusion et de publication de résultats statistiques.

1.3 Cadre institutionnel

Les acteurs qui interviennent ou susceptibles d'intervenir dans l'univers du numérique et in fine de l'Intelligence artificielle et des technologies émergentes peuvent être divisés en deux principales catégories : les acteurs institutionnels et les acteurs non institutionnels.

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

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

Tableau non exhaustif des acteurs évoluant dans l'écosystème de l'IA

Acteurs publics	Acteurs privés
Ministère de l'économie numérique	Opérateurs de télécommunications (Orange, free, expresso)
Ministère de l'enseignement supérieur et de la recherche scientifique	Fournisseurs d'accès à internet
Société Sénégal numérique SA (Ex ADIE)	Société civile (jonction)
Autorité de régulation des télécommunications et des postes (ARTP)	Organisations patronales
Commission de protection des données personnelles (CDP)	Associations
Universités publiques (UVS, Gaston berger, UCAD, ESP)	ONG
Institut de recherches	Institut de formation privé

2. Côte d'ivoire

2.1 Cadre politique

A l'image du Sénégal et de la majorité des Etats de l'Afrique de l'Ouest, la Côte d'ivoire a élaboré des stratégies pour le développement du numérique. Ces stratégies sont : la Stratégie nationale de développement du numérique 2021-2025 et la Stratégie Nationale de Cybersécurité 2021- 2025.

- **Stratégie nationale de Développement numérique 2021-2025**

A travers cette stratégie, la Côte d'ivoire ambitionne d'accélérer la transformation numérique en vue de faire du pays, un hub et leader en matière d'innovation.

Cette stratégie repose sur sept (07) piliers :

Pilier 1 : les infrastructures numériques ;

Pilier 2 : les services numériques

Pilier 3 : les services financiers numériques ;

Pilier 4 : les compétences numériques

Pilier 5 : l'environnement des affaires dans le secteur de l'économie numérique ;

Pilier 6 : l'Innovation

Pilier 7 : la cybersécurité et la confiance numérique.

Par ailleurs, la Côte d'ivoire souhaite promouvoir une industrie numérique propice à l'innovation et la création de valeur à travers le développement des systèmes d'IA et de technologies émergentes. Ainsi, dans le pilier 6 de la stratégie, il a été demandé d'élaborer et de mettre en œuvre une stratégie nationale pour le développement des technologies de la 4ème révolution industrielle comme les 5G, l'IA, l'internet des objets, la réalité virtuelle et la réalité augmentée. Il faudra s'attendre à une production de document stratégique et politique en ce sens dans les années à venir. Ce qui montre que les enjeux liés à l'IA et autres technologies émergentes sont bien appréhendés par les pouvoirs publics ivoiriens.

- **Stratégie nationale de l'Innovation 2021-2025**

La Côte d'ivoire a également une stratégie de l'innovation dont l'ambition est de faire de l'innovation un moteur de développement économique et social à l'horizon 2025. La vision de cette stratégie est « *Utiliser l'innovation comme levier de croissance et de compétitivité de l'économie ivoirienne pour créer de la richesse et*

des emplois de qualité ⁶⁶». A terme cette stratégie s'est fixée pour objectifs stratégiques d'incuber plus d'une centaine de startups par an dans des incubateurs labellisés, multiplié par 10 le volume des investissements dans les startups installés dans le pays, de multiplier par 10 le nombre de brevets délivrés par l'OMPI aux ressortissants ivoiriens, d'améliorer le classement mondial de la Côte d'Ivoire au niveau de l'Indice mondial de l'innovation (Global Innovation Index-GII) et de faire hisser au premier rang en Afrique subsaharienne.

Cette stratégie s'appuie sur quatre (04) axes stratégiques :

Axe1 : Cadre institutionnel et juridique

- création d'un comité national d'innovation ;
- création d'une cellule de promotion de l'innovation ;
- mise en place d'un cadre légal incitatif pour l'innovation
- facilitation du processus de protection de la propriété intellectuelle ;

Axe2 : Infrastructures

- poursuite du programme de création d'incubateurs ;
- création des infrastructures de valorisation ;
- développement des pôles de compétitivité

Axe 3 : Financement et appui

- opérationnalisation du fonds ivoirien de l'innovation ;
- développement des mécanismes de financement alternatifs
- mobilisation des fonds internationaux de l'innovation ;

Axe 4 : Compétences et talents

- Promotion de l'innovation ;
- Masse critique de compétences et de talents innovateurs
- **Stratégie nationale de la cybersécurité 2021-2025**

Outre cette stratégie, le gouvernement ivoirien a adopté une stratégie dans le domaine de la cybersécurité. Cette stratégie a pour objectifs : (i) le renforcement du cadre légal, (ii) la protection du cyberspace, (iii) le renforcement de la confiance numérique ; (iv) la refonte du cadre institutionnel, (v) le renforcement de la capacité du capital humain et (vi) 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 en 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.

2.2 Cadre juridique

Du point de vue légal et réglementaire, la Côte d'Ivoire a adopté à partir de 2013 un arsenal législatif dans le domaine numérique. Il s'agit notamment de la loi n° 2013-546 du 30 juillet 2013 relative aux transactions électroniques, la loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité et la loi n° 2013 – 450 du 19 juillet 2013 relative à la protection des données à caractère personnel. A cela s'ajoute, des ordonnances prises par le gouvernement en 2012 et 2017 portant respectivement sur les télécommunications et aux technologies de l'information et de communication (ordonnance n°2012-293 du 21 mars 2012) et sur les échanges électroniques entre usagers et les autorités administratives (ordonnance 2017-500 du 02 août 2017) et la loi 2017-803 du 07 décembre 2017 d'orientation de la société de l'information. Bien évidemment ce dispositif légal ne traite pas spécifiquement des systèmes d'IA et de technologies émergentes mais il est susceptible de s'appliquer à ces domaines.

Loi d'orientation sur la société de l'information en 2017

66 <https://docplayer.fr/228030345-Strategie-d-innovation-de-la-cote-d-ivoire.html>

- **La loi n° 2013-546 du 30 juillet 2013 relative aux transactions électroniques**

Cette loi a pour objet de régir les transactions électroniques c'est à dire les échanges et ou transactions, de quelque nature qu'ils soient prenant la forme d'un message ou d'un document électronique, à l'exclusion des jeux d'argent, même sous forme de pari ou de loteries, les activités de représentation et d'assistance en justice et les activités notariales. Les transactions utilisant les systèmes d'IA sont incluses dans le champ d'application de la loi. Il est rappelé que les transactions électroniques faisant l'objet de la loi restent soumises aux dispositions non contraires applicables en matière civile et commerciale.

Au sens de la loi, les transactions électroniques doivent se faire dans le respect des droits fondamentaux tels que le respect de la vie privée⁶⁷ et la non-discrimination. En cas violations des dispositions légales, la loi a prévu des sanctions pénales avec des peines allant d'une amende d'un million à cinq millions et/ou une peine d'emprisonnement d'un (01) an à cinq (05) ans.

- **La loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité**

En matière de cybersécurité, bien n'étant pas signataire, ni de la convention africaine sur la cybersécurité, ni de la convention de Budapest sur la cybersécurité, la Côte d'ivoire adopté une loi sur la cybersécurité, en l'occurrence **la loi n°2013-451 du 19 juin 2013**. Cette loi s'inspire des instruments internationaux précédemment cités. Elle reconnaît la prévalence des définitions de certains termes juridiques données par la CEDEAO et l'Union africaine en l'absence de définitions par la loi. Cette loi dont le champ d'application porte sur les infractions relatives à la cybersécurité ainsi que les infractions pénales dont la contestation requiert la collecte de la preuve électronique, a pour objet de lutter contre la cybercriminalité qui est définie par la loi comme "***l'ensemble des infractions pénales qui se commettent au moyen ou sur un réseau de télécommunication ou système d'information***⁶⁸". Par système d'information, on entend "***tout dispositif isolé ou non ou ensemble de dispositif assurant tout ou partie un traitement automatisé de données en exécution d'un programme***". La loi a prévu une large gamme d'infractions pouvant être considérés comme cybercriminelles parmi lesquelles on peut citer les infractions portant sur la confidentialité des systèmes d'information, sur les données informatiques, sur l'utilisation des données à caractère personnel à des fins de prospection, sur la diffusion de pornographie infantile à travers les systèmes d'information et sur la violation des droits de propriété intellectuelle à travers les systèmes d'information ou réseau.

- **La loi n° 2013 – 450 du 19 juillet 2013 sur la protection des données à personnel**

On ne peut pas parler de système d'IA sans parler de données. Celles-ci constituent même le fondement des systèmes d'IA tant leur fonction sont importantes. Parmi les données, il y a une catégorie de données qui fait l'objet de réglementation très protectrice, c'est les données à caractère personnel. La Côte d'ivoire n'est pas en reste dans la protection de ces catégories de données puisqu'elle a adopté **la loi n° 2013 – 450 du 19 juillet 2013 sur la protection des données à personnel**. Cette loi s'applique à "*toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel par une personne physique, l'Etat, les collectivités locales, les personnes morales de droit public ou de droit privé et tout traitement* :

- *Automatisé ou non de données contenues ou appelées à figurer dans un fichier ;*
- *Données mis en œuvre sur le territoire national ;*
- *Données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sureté de l'Etat"*.

Comme on le remarque, le champ d'application de cette loi est très vaste, seules lui échappent "*les traitements de données mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition toutefois que les données ne soient pas destinées à une communication systématique à des tiers on a la diffusion ; - les copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises* »⁶⁹.

67 Article 14: Est interdite, la prospection directe par envoi de message au moyen d'un automate d'appel ou d'émission de SMS, d'un télécopieur ou d'un courrier électronique ou tout autre moyen de communication électronique utilisant, sous quelle que forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen

68 Article 1 de la loi sur la cybercriminalité

69 Article 1 de la loi sur la protection des données à caractère personnel

Que faut-il entendre par données à caractère personnel ? Il s'agit au sens de la loi de *“toute information de quelque nature qu'elle 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 à un numéro d'identification, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique génétique, psychique, culturelle, sociale ou économique”*.⁷⁰

La loi a mis en place des régimes de protection à travers l'accomplissement de formalité placés sous le contrôle de l'Autorité en charge de la régulation des télécommunications et des technologies d'information et de communication.

Les régimes de protection instaurés par la loi sont les suivants : le régime de déclaration et le régime d'autorisation. La loi a également conféré des droits aux personnes qui font l'objet de traitement de données à caractère personnel et mis à la charge du responsable de traitement des obligations dont les manquements est susceptible de sanctions pénales et pécuniaires. Les modalités pratiques de dépôt de la déclaration et de demande d'autorisation sont fixées par le **décret n°2015-79 du 04 février 2015**. Contrairement au Sénégal, les formalités de déclaration et la demande d'autorisation ne sont pas gratuites, elles sont soumises au paiement de frais de dossiers pouvant aller de deux cent mille (200.000) FCFA pour les personnes physiques à trois cent mille (300000) pour les personnes morales⁷¹.

- **L'ordonnance n° 2012-293 du 21 mars 2012 relative aux télécommunications et technologies de l'information et de la communication**

Cette ordonnance régit toutes les activités de télécommunications/Technologies de l'information et de communication (TIC) exercées à partir ou à destination du territoire de la République de Côte d'Ivoire, à l'exception de : l'établissement et l'exploitation des réseaux ou services de télécommunications/TIC par l'Etat pour les besoins de la défense nationale, de la sécurité publique et de la sécurité aérienne et maritime ; les installations de l'Etat utilisant, pour les besoins propres de l'administration, des bandes de fréquences conformément aux avis et prescriptions de l'Union internationale des Télécommunications (UIT) ; la réglementation en matière de politique et de contenus audiovisuels.

Au sens de cette ordonnance, les activités de télécommunications doivent se faire dans le respect de la vie privée, de manière transparente et non discriminatoire. A ce titre, l'accès aux réseaux de télécommunications ainsi que le partage d'infrastructures doivent se faire dans les conditions d'équité, de non-discrimination et d'égalité d'accès. Le contrôle des activités de télécommunications est placé sous la responsabilité de l'Autorité de régulation des télécommunications de la Côte d'Ivoire (ARTCI) qui est une autorité administrative indépendante mais qui dispose de compétence judiciaire puisqu'elle connaît au premier ressort tout litige pouvant survenir dans le domaine de la télécommunication et les nouvelles technologies⁷². En plus des sanctions administratives et pécuniaires, ARTCI peut également infliger des sanctions pénales en cas de violations des obligations prévues par l'ordonnance.

- **Loi n°2017-803 du 07 décembre 2017 d'orientation de la société de l'information**

Cette loi fixe les principes généraux juridiques, institutionnels pour le développement de la société de l'information de la Côte d'Ivoire. Cette loi pose les principes fondamentaux régissant la société de l'information. Ces principes sont notamment :

- l'exigence d'une société moderne caractérisée par un usage accru et quotidien des infrastructures, des données, des outils de télécommunications dimension humaine, inclusive, solidaire, ouverte, transparente, sécurisé, et propice au développement économique, social, ainsi que culturel ;
- la garantie de l'exercice des droits et libertés reconnues aux personnes par la constitution , les conventions internationales ou traités ratifiés par la Côte d'Ivoire ;
- l'affirmation du droit fondamental de l'Homme d'accès à l'Internet et aux réseaux de communication électronique,
- la garantie de l'accès universel aux services des TIC
- la garantie de la liberté accrue à la circulation des données et du savoir de réseaux ;
- le principe de neutralité de l'internet et des réseaux de communications

⁷⁰ Art 1 op cité

⁷¹ Article 3 du décret n° 2015-79 du 04 février 2015

⁷² Art 104 de l'ordonnance sur les télécommunications et les techniques de l'Information et de communications

- la sécurité des réseaux et des systèmes d'informations ;
- le principe de séparation entre les fonctions de réglementation et de régulation ;
- le principe de la libre et loyale concurrence.

Cette loi prévoit la mise en place d'une commission nationale de développement de la société de l'information chargé de veiller à la bonne coordination des actions et des projets de l'Etat en matière des TIC.

2.3 Cadre institutionnel

Dans l'écosystème de l'intelligence artificielle et de technologies émergentes, une multitude d'acteurs institutionnels et non institutionnels interviennent

Tableau non exhaustif des acteurs intervenant dans l'écosystème de l'IA

Acteurs publics	Acteurs privés
Ministère des technologies numériques	Opérateurs de télécoms (Orange Moov, Mtn)
Ministère de l'enseignement supérieur et de la recherche scientifique	Fournisseurs d'accès
Autorité de régulation des télécommunications (ARTCI)	Incubateurs
Comité national de l'innovation	Fédération de startups
Fonds national de l'innovation	Patronat
Universités publiques	Société civile
Institut de recherches	Association

3. Bénin

3.1 Cadre politique

- **Stratégie nationale d'intelligence artificielle et des mégadonnées 2023-2027**

Le Bénin a publié en février 2023 une stratégie nationale sur l'IA et des mégadonnées (SNIAM) pour la période 2023-2027 faisant de ce pays un pionnier en Afrique de l'ouest. La SNIAM a pour vision de faire rayonner le Bénin, à l'horizon 2027, grâce à l'IA. Cette stratégie, axée autour des technologies de l'IA adaptées aux besoins du pays, se décline en trois orientations stratégiques : (1) l'organisation et consolidation de l'embryon d'écosystème existant et valorisation des résultats ; (2) développement et soutien accru à l'écosystème de l'IA) et (3) Valorisation de l'écosystème, de la connaissance et du savoir-faire béninois. Ces orientations stratégiques sont axées sur les domaines d'intervention suivants : les infrastructures, services et données par le développement et la mise en œuvre de solutions d'IA à fort impact ; la recherche, innovation et partenariat à travers l'appui à la formation, à la recherche, à l'innovation et au secteur privé ; et la gouvernance par la mise en place d'un cadre de gouvernance de l'IA et de la gestion des données de masse. La mise en œuvre des actions prévues pour le développement de l'IA au Bénin nécessite un budget de 4,68 milliards de FCFA.

- **Stratégie Nationale de la Sécurité numérique (2020-2022)**

Face aux enjeux du numérique qui connaît un développement fulgurant en Afrique et vu 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 une **Stratégie Nationale de la Sécurité Numérique (2020-2022)** dont la vision est d'avoir "*un cyberspace sécurisé et attrayant pour une économie*

numérique florissante⁷³. 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** visant la mise en place d'un environnement juridique complet comportant des lois et 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. **Coordination nationale et la coopération internationale.**

Cette stratégie est de portée générale dans le domaine du Numérique et ne vise pas spécifiquement les problématiques de l'Intelligence artificielle et des technologies émergentes. C'est pourquoi le gouvernement béninois a lancé au cours de 2022 les travaux d'élaboration d'une stratégie nationale de l'Intelligence artificielle et d'exploitation des Méga données⁷⁴. Au vu de l'enjeu majeur de l'IA des politiques nationales de développement, la mise en place d'une stratégie dans ce domaine permettra de faire du Benin la plateforme des services numériques en l'Afrique de l'ouest et de participer à l'éclosion de l'épanouissement de l'IA dans le pays.

3.2 Cadre juridique

- **Loi 2017-20 du 13 juin 2017 portant Code du Numérique**

A la faveur de la loi 2017-20 du 13 juin 2017, le Benin a adopté le Code du Numérique. Le Benin a pris l'option de regrouper au sein de ce Code toutes les matières relevant du Numérique abrogeant ainsi toutes les dispositions législatives contraires notamment : 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 et la loi 2009-09 du 24 mai 2009 portant protection des données à caractère personnel.

Ce Code consiste donc en la codification des textes existants ajustés d'une part, et l'adoption de textes complémentaires sur des sujets n'ayant pas été réglementés. Ce Code du Numérique a pour objet de régir les activités qui relèvent des réseaux et services de communications électroniques, les outils électroniques, les services de confiance en l'économie numérique, le commerce électronique, la protection des données à caractère personnel, ainsi que la cybercriminalité et la cybersécurité.

Il est divisé en sept (07) livres regroupant 647 articles disposé comme suit⁷⁵:

- Livre préliminaire dénommé "Définitions et objet" et qui dispose de deux (02) articles (1-2) qui posent les différentes définitions des termes utilisés ;
- Livre premier relatif aux "Réseaux et services de communications électroniques" comportant les articles 03 à 265 qui traite des activités de communications électroniques et le statut juridique des exploitants ;
- Livre deuxième "Outils et écrits électroniques " relatif à la valeur juridique des actes électroniques tels que les écrits, signatures, système de cryptologie, l'archivages électronique et l'authentification des sites internet (Art 266 à 304) ;
- Livre troisième "Prestataires de services de confiance" qui définit le statut, les obligations, le contrôle et les sanctions de ces prestataires (Art 305 à 325) ;
- Livre quatrième "Commerce électronique" s'appliquant à toute commande, contrat ou transaction

73 Stratégie nationale de la sécurité numérique 2020-2022

74 <https://numerique.gouv.bj/actualites/article.php?IDArticle=183>

75 Décryptage de la loi portant code du numérique au Benin, Julien Coomlan Hounkpe, <https://www.village-justice.com/articles/decryptage-loi-portant-code-numerique-benin,27107.html>

conclu en ligne ou par voie électronique dans le cadre de la fourniture de biens ou de services et les activités connexes liées au commerce électronique (Art 326 à 378) ;

- Livre cinquième sur la “Protection des données à caractère personnel “ traite de la collecte, le traitement, la transmission, le stockage et l’usage des données à caractère personnel (Art 379 à 490) ;
- Livre sixième “Cybercriminalité et cybersécurité” pose les règles et les modalités de lutte contre la cybercriminalité et le cadre institutionnel, les règles et modalité d’utilisation de la cryptologie (Art 491 – 639)
- Livre septième “Dispositions transitoires et finales (Art 640- 647).

Il serait fastidieux d’étudier en détail tous les livres de ce Code, ainsi l’option a été prise de s’appesantir davantage sur les livres 4, 5, 6.

Le livre 4 relatif au Commerce électronique porte sur toute commande, contrat ou transaction conclus en ligne ou par voie électronique en vue de la fourniture et toute activité exercée sur le territoire du Bénin ou à destination des utilisateurs résidants sur ce territoire. Sont exclus du champ d’application de ce livre, les activités de jeux d’argent, sous forme de paris, de loterie ou autres ; les activités de représentation et d’assistance en justice ; les activités exercées par les notaires. Conformément à la loi, pèsent sur les personnes exerçant les activités entrant dans le champ d’application de ce livre, une obligation d’information. Elles engagent également leur responsabilité contractuelle.

En matière de publicité électronique, l’identité de l’expéditeur doit être clairement identifiable. De plus, aucune activité de prospection directe par moyens de systèmes automatisés ne peut se faire sans le consentement préalable du destinataire de la prospection sous réserve de quelques exceptions prévues par le Code. Est accordé à toute personne, un droit d’opposition à la prospection. En tout état de cause, toute personne exerçant une activité électronique est soumise aux respects des dispositions relatives à la protection des données à caractère personnel et doivent prendre les dispositions pour garantir la confidentialité des données personnelles. Ceci nous amène à voir les dispositions du livre 5 relatif à la protection des données à caractère personnel.

Le livre 5 protection des données à caractère personnel abroge et remplace les dispositions de la loi 2009-09 du 22 mai 2009 portant protection des données à caractère personnel. Il a pour objet de mettre en place un cadre légal de protection de la vie privée et professionnelle consécutif à la collecte, au traitement, la transmission, le stockage et à l’usage des données à caractère personnel⁷⁶. Reprenant la loi de 2009 sus citée, le livre 5 porte un principe majeur sur le but de l’informatique qui doit respecter les droits fondamentaux”. L’informatique doit ainsi 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*⁷⁷”. Les dispositions de ce livre ont un champ d’application très large et portent sur ” toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation de données à caractère personnel par une personne physique, par l’État, les collectivités locales, les personnes morales de droit public ou de droit privé ; tout traitement automatisé en tout ou en partie, ainsi que tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier, à l’exception des traitements visés à l’alinéa 2 ; tout traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d’infractions pénales ou la sûreté et les intérêts essentiels de l’État, sous réserve des dérogations définies par des dispositions spécifiques fixées par d’autres textes de loi en vigueur⁷⁸”. Seuls sont exclus, traitements de données utilisées par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques lorsque ces données ne sont pas destinées à une communication à des tiers ou à la diffusion. Ce livre s’applique également lorsque le traitement de données est fait dans le territoire béninois mais également en dehors du territoire mais pour le compte d’un responsable de traitement établi au Bénin. En tout état de cause, le traitement des données doit obéir au principe de licéité et de loyauté dans la collecte et avoir une finalité déterminée, explicites et légitimes. De plus, le traitement de données est soumis à l’accomplissement de formalités que sont : la déclaration, l’autorisation et l’avis auprès de l’autorité en chargé de la protection des données à caractère personnel. La loi prévoit des exemptions par rapport à l’accomplissement de ces formalités notamment la désignation par le responsable de traitement d’un délégué à la protection des données à caractère personnel

⁷⁶ 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, ci-après dénommée personne concernée. Est réputée identifiable, une personne qui peut être identifiée, directement ou indirectement notamment par 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

⁷⁷ Art 379 du Code de numérique

⁷⁸ 381 du Code Numérique

qui garantit que le traitement ne soit pas susceptible de porter atteinte aux droits et libertés des personnes concernées. A ce titre le DPO est chargé d'assurer de manière indépendante l'application des dispositions réglementaires en vigueur et de tenir un registre des traitements effectués par le responsable du traitement⁷⁹. La désignation d'un DPO, prévue par la législation béninoise constitue une innovation importante et s'inspire du Règlement général de protection de données à caractère personnel (RGPD) de l'Union Européenne. Pour comparaison, dans les pays cibles du pays Sénégal, Côte d'Ivoire et Burkina Faso, leur cadre légal sur la protection des données à caractère personnel ne prévoit pas de DPO. Dans la perspective de la prise en compte des évolutions technologiques comme l'IA, les objets connectés et big data, la mise en place de DPO s'inscrit dans le cadre de la responsabilisation du responsable de traitement et du renforcement des droits des personnes. Toutefois, la désignation d'un DPO ne libère pas le responsable de traitement des obligations légales qui pèsent sur lui au titre de ce titre. Parallèlement, le code numérique accorde des droits aux personnes à l'égard de leurs données personnelles comme le droit d'accès, le droit de portabilité des données, le droit d'interrogation, le droit d'opposition, le droit à la rectification et la suppression et le droit à l'oubli. Le contrôle de la conformité et du respect de la vie privée sur le territoire béninois est placé sous la responsabilité de l'Autorité de protection des données à caractère personnel (APDP) qui remplace la Commission nationale de l'informatique et libertés (CNIL). La loi prévoit également des sanctions administratives, pécuniaires et pénales en cas de violation des dispositions contenues dans ce livre.

Livre 6 sur la cybercriminalité et la cybersécurité

Dans le cadre de la lutte contre la cybercriminalité, le Benin est signataire de la Convention de Budapest et de Malabo mais ne les a pas encore ratifiés quoique le processus est en cours⁸⁰. Néanmoins dans le cadre du Code numérique, le Benin a légiféré sur la cybercriminalité et la cybersécurité qui fait l'objet du titre 6 dudit Code. Le livre 6 fixe les règles et les modalités de lutte contre la cybercriminalité et définit également le cadre institutionnel, les règles et les modalités d'utilisation de la cryptologie. Dans les principes généraux de ce livre, le législateur béninois pose le principe de garantie des droits fondamentaux et des libertés. Ainsi, la mise en œuvre des pouvoirs et procédures prévus est soumis au droit béninois qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application du Pacte international relatif aux droits civils et politiques des Nations-Unies et de la Charte africaine des droits de l'homme et des peuples ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité⁸¹. 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 des infractions liées au système informatique⁸², les infractions liées à l'utilisation des données à caractère personnel, les infractions relatives aux atteintes des personnes et biens comme la pédopornographie, les infractions liées à la publicité sur internet, des infractions de presse en ligne, les infractions liées aux droits de propriété intellectuelle et des infractions de droit commun commises en ligne comme le vol de données informatiques⁸³, l'usurpation d'identité. Comme on le constate, ce Code numérique constitue une avancée significative dans le sens, qu'il donne un niveau élevé de sécurité juridique conforme aux standards internationaux et vis-à-vis des partenaires publics, privés, le secteur privé et les investisseurs internationaux. Sous réserve de son application effective, ce code pourrait permettre au Benin d'atteindre son objectif d'être leader le domaine du digital en Afrique de l'ouest et assoir une économie digitale, comme levier de croissance économique inclusive. Il faut noter que la loi de 2017 portant Code du Numérique a fait l'objet de modification par la loi 2020-35 du 10 décembre 2020. Les modifications portent principalement sur la réduction du nombre de conseillers de l'autorité de régulations et des communications, du nombre de membres de l'autorité de protection des données à caractère personnel.

79 Article 408 du Code du numérique

80 <https://cybersecuritymag.africa/Benin-va-bientot-ratifier-conventions-budapest-et-malabo>

81 Art 493 du Code du Numérique

82 Système informatique : dispositif ou groupe de dispositifs interconnectés ou reliés, dont internet, qui, au moyen d'un programme, procède au traitement automatique des données ou à l'exécution d'autres fonctions. Un système informatique est un dispositif composé de matériels et de logiciels, conçus pour le traitement automatisé des données numériques. Il peut comprendre des moyens d'acquisition, de restitution et de stockage des données. Il peut être isolé ou connecté à d'autres dispositifs similaires au sein d'un réseau ;

83 Données informatiques : toute représentation de faits, d'informations, de concepts, de codes ou d'instructions lisibles par une machine, 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

- **La loi n° 99-014 du 12 avril 2000 sur l'organisation et le fonctionnement du Conseil national de la Statistique**

Cette loi porte sur la création, l'organisation et le fonctionnement du Conseil National de la Statistique. Ses organes sont :

- L'Institut National de la Statistique et de l'Analyse Economique (INSAE) en tant qu'établissement public à caractère scientifique et technique ;
- les antennes départementales de la statistique ;
- les services statistiques des départements ministériels ;
- les observatoires et systèmes intégrés de statistiques.

La loi pose le principe de secret statistique et interdit aux agents des services publics et des organismes participant aux enquêtes de divulguer les renseignements individuels figurant dans les enquêtes. Par conséquent, les résultats issus des enquêtes statistiques ne doivent être publiés que sous forme anonyme.

3.3 Cadre institutionnel

L'écosystème du numérique englobant les systèmes de l'IA et les technologies émergentes s'articule autour de nombreux acteurs qui contribuent à son développement. Ces acteurs peuvent être divisés en deux groupes : les acteurs institutionnels et les acteurs non institutionnels.

Tableau non exhaustif des acteurs intervenant dans l'écosystème de l'IA

Acteurs publics	Acteurs privés
Ministère du Numérique et de la Digitalisation	Opérateurs de télécoms (Orange, Moov)
Ministère de la défense nationale	Industriels
Ministère de la justice et de la législation	Fournisseurs d'accès à internet
Ministère de l'Energie	Enseignement privé
Ministère de l'Enseignement supérieur	Intégrateurs et fournisseurs de technologies
Ministère des infrastructures et du transport	Acteurs de la société civile intervenant dans le domaine du numériques
Agence nationale de la sécurité des systèmes d'information (ANSSI)	Starts ups
Agence pour le Développement du numérique (ADN)	ONG
Autorité de protection des données à caractère personnel (APDP)	
Autorité de régulation des communications électroniques (ARCEP)	
Conseil National de la Sécurité numérique (CNSN)	
Agence Béninoise du service universel des communications et de la poste (ABSU-CEP)	
Universités	
Instituts de recherche	

4. Burkina FASO

4.1 Cadre politique

A l'image des trois pays cibles du projet (Sénégal, Côte d'Ivoire et Bénin), le Burkina Faso a également élaboré des stratégies dans le domaine du Numérique et de la cybersécurité. Il s'agit notamment de la stratégie nationale de développement de l'économie numérique (2018-2027) et la stratégie nationale de cybersécurité (SNCS) pour la période 2019-2023.

- **Stratégie nationale de développement de l'économie numérique (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.

Cette 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'utilisateur 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.

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.

- **La Stratégie nationale de la cybersécurité (2019-2023)**

Conscient des enjeux liés à la cybersécurité et la cybercriminalité compte tenu de la montée croissante du risque numérique, le Burkina Faso a également adopté une stratégie nationale de la cybersécurité (2019-2023). Elle 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 cyberspace 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 cyberspace et de la société civile autour des actions prévues dans la SNCS en vue de lutter contre la cybercriminalité.

Tout comme pour le Sénégal, cette stratégie est arrivée à terme depuis 2023.

4.2 Cadre juridique

Le Burkina Faso dispose d'un cadre légal dans le domaine du Numérique. Ce cadre légal est constitué de la loi n°61-2008/AN du 27 novembre 2008 portant réglementation générale des réseaux et des services de communications électroniques, la loi n°045-2009/AN du 10 novembre 2009 relative à la réglementation des services et des transactions électroniques et la loi n°001-2021/AN du 31 mars 2021 portant protection des personnes à l'égard du traitement des données à caractère personnel.

- **La loi n°045-2009/AN du 10 novembre 2009 relative à la réglementation des services et des transactions électroniques**

Concernant les services et transactions électroniques, l'Etat Burkinabé a adopté la loi n°045-2009/AN du 10 novembre 2009. Cette loi s'applique notamment aux services de la société de l'information qui donnent lieu à la conclusion de contrats pour se procurer un bien ou une prestation de services, qui fournissent des informations, des publicités ou encore des outils permettant la recherche, l'accès et la récupération de données, ou qui consistent à transmettre des données par le biais d'un réseau de communication, à fournir un accès à un tel réseau ou à assurer le stockage de données, même lorsque ces services ne sont pas rémunérés par ceux qui les reçoivent ; la dématérialisation des procédures administratives à la mise en ligne des informations publiques par l'Etat, les collectivités territoriales et toute personne de droit public ou de droit privé chargée de la gestion d'un service public.

Ne sont pas soumises à la loi les activités suivantes : les jeux d'argent, impliquant des mises ayant une valeur monétaire dans des jeux de hasard, y compris les loteries et les transactions portant sur des paris ; les activités de représentation et d'assistance en justice ; les activités exercées par les notaires, dans la mesure où elles comportent une participation directe et spécifique à l'exercice de l'autorité publique ; les accords et pratiques régis par le droit sur les ententes.

Les règles applicables en matière de protection des données à caractère personnel s'appliquent également dans les matières couvertes par la loi.

La loi de 2009 sur les transactions régit notamment la signature électronique, le commerce électronique et la mise à disposition par voie électronique d'informations publiques. Dans le cadre de la protection de la vie privée, du consommateur, les autorités publiques peuvent prendre des mesures restreignant la libre prestation des services électroniques.⁸⁴

- **La loi n°001-2021/AN du 31 mars 2021 portant protection des personnes à l'égard du traitement des données à caractère personnel**

Avec la loi n°10-2004/AN du 20 avril 2004, le Burkina Faso fut l'un des pays de la région ouest africain 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 et sa ratification de la convention 108 sur la protection des données à caractère

⁸⁴ Article 5 de la loi de 2009 sur les transactions électroniques

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.

Cette loi a pour objet de protéger les droits et libertés fondamentaux des personnes physiques en matière de traitement de leurs données à caractère personnel, quels qu'en soient la nature, le mode d'exécution ou les responsables. Elle 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. Toutefois sont exclus du champ d'application de la loi : les traitements des données faites une personne physique dans l'exercice exclusif d'activités personnelles, des copies temporaires faites dans le cadre d'activité de transmission et traitements effectués aux seules fins littéraires, artistiques ou journalistiques⁸⁵.

La loi de 2021 pose le principe du respect des droits fondamentaux. 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.

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) ;
- 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.

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. Ces sanctions administratives sont toutefois sans préjudice des sanctions pénales.

Cette loi constitue une avancée significative dans la protection des données personnelles mais pourrait avoir des limites notamment pour garantir cette protection surtout face aux enjeux des systèmes d'IA et des technologies émergentes.

- **La loi n°12-2007 /AN du 31 mai 2007 sur les activités statistiques**

Dans le cadre de la régulation des activités statistiques, le Burkina a adopté **la loi n°12-2007 /AN du 31 mai 2007** qui définit les principes fondamentaux régissant les activités statistiques ainsi que les règles d'organisation du système national de statistique. Au rang de ces principes fondamentaux, figurent les principes d'indépendance scientifique, d'impartialité, d'objectivité et de transparence. Par ailleurs, la loi dispose du secret statistique et de l'obligation des services statistiques de respecter la vie privée et de protéger les données à caractère personnel.

- **La loi n°025-2018/AN du 31 mai 2018 portant Code pénal**

A l'instar des trois autres pays cibles du projet, le Burkina Faso a prévu des dispositions en matière de cybercriminalité. Ces dispositions sont contenues dans la loi n°025-2018/AN du 31 mai 2018 portant Code pénal aux articles 711-1 au 721-1. Le Code pénal a prévu deux grandes catégories : les infractions en matière informatique et les infractions commises au moyen des technologies de l'information et de la communication.

Dans la première catégorie, le code prévoit des infractions liées aux systèmes et données informatiques et les infractions relatives aux manquements aux obligations légales dans la mise en œuvre et l'utilisation d'un système de traitement automatisé des données à caractère personnel⁸⁶.

Au titre de la deuxième catégorie, il est prévu des infractions concernant la violation du secret de correspondance, l'utilisation frauduleuse à des fins personnelles ou non un service de communications électroniques ouvert au public, la diffusion volontaire de signaux radio électroniques, appel de détresse faux ou trompeurs, l'interruption volontaire des communications électroniques, vol et vandalisme sur les infrastructures électroniques.

85 Article 2 de la loi sur la protection des données à caractère personnel

86 Loi n°025-2018/AN du 31 mai 2018 portant code pénal – Bienvenue sur le portail officiel du Conseil Supérieur de la Magistrature du Burkina Faso (csm.bf)

4.3 Cadre institutionnel

De nombreux acteurs interviennent autour de l'univers du numérique. Ces acteurs identifiés sont susceptibles d'intervenir dans le domaine de l'IA et des technologies émergentes. Ces acteurs peuvent être regroupés en deux groupes : les acteurs publics et les acteurs privés.

Tableau non exhaustif des acteurs intervenant dans l'écosystème de l'IA

Acteurs publics	Acteurs privés
Ministère du développement de l'économie numérique et des postes	Opérateurs de téléphoniques (ONATEL, TELECEL et AIRTEL)
Ministère de la communication chargé des relations avec le parlement	Les fournisseurs d'accès internet
Ministère de l'enseignement supérieur et de la recherche scientifique	Les intégrateurs de solutions
Autorité de régulation des communications électroniques et des postes	Les développeurs et/ou fournisseurs de contenus multimédias
La Commission de l'Informatique et des libertés (CNIL)	Les spécialistes en sécurité informatiques
L'agence nationale de la sécurité des systèmes d'information (ANSSI)	Le patronat burkinabé
L'Agence nationale de promotion des technologies de l'information et de la communication (ANPTIC)	Associations, ONG

B. Exploitations et des synthèses des textes politiques, législatifs et éthiques d'autres pays (France, Canada, Maroc, Kenya, Ile Maurice)

Dans une démarche de benchmarking, il a paru intéressant de voir comment d'autres pays appréhendent les systèmes d'IA et des technologies émergentes. Les pays choisis sont la France, le Canada, l'Ile Maurice, le Maroc, et le Kenya. Pour ces pays, il ne s'agit pas d'étudier l'ensemble des textes politiques, juridiques et éthiques, relatifs à l'IA mais sélectionner les plus pertinents pour l'objet de recherche.

1. France

• Stratégie AI for humanity

En 2018, la France a lancé sa stratégie sur l'IA dénommée "**Stratégie AI for humanity**" financée à 1,5 milliards sur une période de cinq (05) ans (2018-2022). L'objectif majeur de cette stratégie est de propulser la France parmi les champions de l'IA à côté des Etats unis, du Japon et du Canada. La stratégie est guidée par trois priorités que sont : la recherche, l'ouverture des données et l'éthique⁸⁷. Sur la base de ces priorités, la stratégie a été déclinée en trois axes :

- **Axe 1** : les talents : disposer de la meilleure expertise en intelligence artificielle ;
- **Axe 2** : L'Etat moteur de la conduite de projets et de l'évolution des données pour la diffusion de l'IA dans l'économie et la société ;
- **Axe 3** : Ethique : Engager un dialogue entre performance et Humanité.

Le premier axe de la stratégie vise le renforcement du capital humain de la France grâce à la formation de nouveaux talents à travers la mise en place de programme de formation et de recherche.

⁸⁷ AI for Humanity, l'intelligence artificielle au service de l'humain, https://cache.media.enseignementsup-recherche.gouv.fr/file/strategie_IA/60/7/mesri_IA_dep_A4_09_1040607.pdf

Le deuxième axe vise l'ouverture des données pour permettre la diffusion de l'IA dans l'économie soit de manière sectorielle ou dans tous l'écosystème de l'innovation.

Le troisième axe porte sur la réflexion à mener sur les enjeux éthiques liées au développement des technologies de l'IA.

En 2021, la deuxième phase de la stratégie nationale pour l'IA (2021-2025) a été lancée dont l'ambition de faire de la France, un pays pionnier en matière d'innovation à l'horizon 2030⁸⁸. Cette nouvelle phase financée à hauteur de 2,2 milliards vise à renforcer les acquis obtenus dans le cadre de la première phase de la stratégie. Les objectifs clés de cette deuxième phase est d'accroître les compétences en IA du pays, positionner la France en leader des domaines de l'IA et accélérer le déploiement de l'IA.

Pour ce faire, la France ambitionne de mettre en place un plan massif de formation à l'IA avec un volet formation d'excellence et un volet massification de l'offre nationale de formation en IA. Au-delà de la formation, un soutien important à l'innovation sera apporté afin de positionner l'économie française sur des domaines d'avenir de l'IA.

Dans le cadre de cette deuxième phase, la France souhaite accélérer la diffusion des systèmes d'IA responsables en vue de la modernisation de l'économie grâce à l'industrialisation de l'IA, l'accès aux données par les services, le développement de l'écosystème de startups en IA et l'appropriation de l'IA par les petites et moyennes entreprises.

- **La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux**

La France a très tôt adopté une réglementation pour encadrer les dangers liés au développement de l'informatique notamment les traitements automatisés des informations nominatives c'est à dire des données personnelles". Il s'agit de la loi la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, appelée loi "Informatique et libertés". Cette loi prévoyait déjà en son article 1 que « *l'informatique 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* ». En 2016, est intervenu le règlement européen général de protection des données à caractère qui s'applique directement au niveau des Etats membres de l'Union européenne depuis son entrée en vigueur en depuis le 25 mai 2018. L'entrée en vigueur du RGDP a conduit à la révision de la loi informatiques et libertés par la loi du 20 juin 2018 n° 2018-493. Coexistent alors les textes, la primauté étant accordée au RGDP. Le RGDP poursuit trois objectifs : le renforcement des droits des personnes grâce notamment le droit à la portabilité des données⁸⁹ et des dispositions relatives aux mineurs, la responsabilisation des responsables de traitement et des sous-traitants avec l'obligation de conformité qui remplace les formalités préalables (déclarations et autorisations) et la crédibilisation de la régulation par un renforcement des autorités de protection des données⁹⁰.

- **La loi n° 2016-1321 du 07 octobre 2016 pour une République numérique**

Toujours dans le domaine du numérique particulièrement de l'ouverture des données, la France a adopté la loi n° 2016-1321 du 07 octobre 2016 pour une République numérique. Cette loi apporte comme innovation majeure l'ouverture par défaut des données publiques qui oblige les organismes publics de communiquer gratuitement en ligne leurs bases de données sous réserve d'anonymisation et de protection du secret industriel et commercial. La finalité étant que ces bases de données puissent être exploitées et réutilisées par un particulier. Plus spécifiquement, cette loi renforce l'obligation d'information qui pèse sur les personnes qui déploient des algorithmes et prévoit la communication des code sources des algorithmes utilisées par l'administration. Cette loi qui favorise s'articule autour de la circulation des données et du savoir, de la protection des droits dans la société du numérique et l'accès au numérique⁹¹.

88 Stratégie nationale pour l'Intelligence artificielle, phase 2, https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2021/11/08112021_dp_strategie_nationale_pour_ia_2eme_phase.pdf

89 Ce droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et le cas, échéant de les transférer à un tiers

90 <https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels>

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

2. Canada

• Stratégie pancanadienne en matière d'IA (2017-2022)

Le Canada est le chef de file en matière d'élaboration d'instruments stratégiques dans le domaine de l'Intelligence artificielle. En effet, dès 2017, le Canada a adopté la première stratégie au monde en IA intitulée "Stratégie pancanadienne en matière d'IA" dont la première phase (2017-2022) était financée à hauteur de 125 millions de Dollars canadiens⁹². Cette stratégie a pour objectif général de rehausser le profil international du Canada en matière de recherche et de formation en matière de l'IA. La première phase de la stratégie était axée dans le domaine de la formation et de la recherche. En ce sens, on note la création de trois instituts nationaux en IA et le recrutement et le maintien de talents dans ce domaine par la mise en place de chaires en IA. L'éthique pour un AI responsable occupait une place importante dans cette stratégie. Les efforts consentis lors de la première phase ont permis au Canada d'être classé 4ème au rang mondial du Global index AI.⁹³ En 2022, le gouvernement Canadien a annoncé la deuxième phase de la stratégie pancanadienne financée à 443 millions pour qu'à l'horizon 2030, le Canada puisse "disposer de l'un des écosystèmes nationaux d'IA les plus robustes au monde fondé sur l'excellence scientifique, la qualité de la formation et la recherche des bassins de talents, la collaboration entre le secteur public et le secteur privé ainsi que de solides valeurs visant à faire progresser les technologies d'IA pour procurer les bienfaits sociaux, économiques et environnementaux aux êtres humains et la planète".⁹⁴ A ce titre, le Canada compte renforcer les efforts consentis lors de la première phase dans la formation et la recherche avec comme mesures phares: le recrutement et la rétention des titulaires de chaires en IA accompagnés d'un soutien financier et des mécanismes permettant d'accélérer les découvertes, l'accroissement de l'IA dans le domaine de la santé et de l'industrie et la recherche et le partage des connaissances pour faire avancer les données stratégiques clés sur les répercussions sociétales⁹⁵.

Du point de vue réglementaire, la protection des données à caractère personnel est régie par la loi sur la protection des renseignements personnels⁹⁶, la loi sur la statistique⁹⁷.

La loi sur la protection des renseignements personnels donne une définition très large de la notion de renseignements personnels⁹⁸ faisant entrer dans le champ d'application de la loi une large emprise de renseignements. La loi sur la statistique protège également les données personnelles en ce sens qu'elle pose l'interdiction aux services de statistique de divulguer des renseignements personnels d'un particulier à quiconque notamment la police, l'administration fiscale, la justice. Elle renferme également des dispositions très strictes sur la confidentialité des renseignements recueillis contre tout accès non autorisé.

En 2022, le Canada a entrepris une réforme législative de taille. En effet un projet de loi C-27⁹⁹ qui regroupe trois lois : la loi sur la protection de la vie privée et des consommateurs, la loi sur le Tribunal de la protection des renseignements personnels et des données et la loi sur l'intelligence artificielle et les données.

• La loi sur la protection de la vie privée et des consommateurs

92 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>

93 <https://aiindex.stanford.edu/report/>

94 <https://cifar.ca/fr/ia/>

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

96 <https://laws-lois.justice.gc.ca/fra/lois/P-21/page-1.html#h-387684>

97 <https://laws-lois.justice.gc.ca/fra/lois/S-19/TexteComplet.html>

98 Les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, notamment :

- a) les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge ou à sa situation de famille;
- b) les renseignements relatifs à son éducation, à son dossier médical, à son casier judiciaire, à ses antécédents professionnels ou à des opérations financières auxquelles il a participé;
- c) tout numéro ou symbole, ou toute autre indication identificatrice, qui lui est propre;
- d) son adresse, ses empreintes digitales ou son groupe sanguin;
- e) ses opinions ou ses idées personnelles, à l'exclusion de celles qui portent sur un autre individu ou sur une proposition de subvention, de récompense ou de prix à octroyer à un autre individu par une institution fédérale, ou subdivision de celle-ci visée par règlement;
- f) toute correspondance de nature, implicitement ou explicitement, privée ou confidentielle envoyée par lui à une institution fédérale, ainsi que les réponses de l'institution dans la mesure où elles révèlent le contenu de la correspondance de l'expéditeur;
- g) les idées ou opinions d'autrui sur lui;
- h) les idées ou opinions d'un autre individu qui portent sur une proposition de subvention, de récompense ou de prix à lui octroyer par une institution, ou subdivision de celle-ci, visée à l'alinéa e), à l'exclusion du nom de cet autre individu si ce nom est mentionné avec les idées ou opinions;
- i) son nom lorsque celui-ci est mentionné avec d'autres renseignements personnels le concernant ou lorsque la seule divulgation du nom révélerait des renseignements à son sujet

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

Cette loi a pour objet de régir la protection des renseignements personnels des individus tout en tenant compte du besoin des organisations de recueillir, d'utiliser ou de communiquer de tels renseignements dans le cadre des activités commerciales. Cette loi abroge certaines dispositions de la loi sur la protection des renseignements personnels et remplace le titre de ladite loi par " loi sur les documents électroniques".

- **La loi sur le Tribunal de la protection des renseignements personnels et des données**

Cette loi met en place un tribunal administratif pour recevoir les recours faits à l'encontre de certaines décisions rendues par le Commissaire à la protection de la vie privée et d'infliger les pénalités relatives à la contravention de certaines infractions afférentes à la vie privée.

La loi qui nous intéresse plus dans cette révision est sans aucun doute **le projet de loi sur l'intelligence artificielle et les données** qui vise à réglementer le développement et l'utilisation de l'IA dans le secteur privé.

Tout comme le Règlement européen sur l'IA, cette loi est basée sur une approche fondée sur le risque.

Au sens de cette loi, le système de l'IA s'entend "*système technologique qui, de manière autonome ou partiellement autonome, traite des données liées à des activités humaines en utilisant un algorithme génétique, un réseau neuronal, l'apprentissage automatique ou une autre technique afin de générer du contenu ou prendre des décisions, faire des recommandations ou des prévisions*"

Cette définition confère à la loi un champ d'application très large permettant d'appréhender les risques résultant des systèmes de l'IA sur les droits individuels et de s'appliquer à tous les acteurs du maillon allant de la conception, au développement jusqu'au déploiement.

Les exigences générales¹⁰⁰ posées par la loi sont notamment :

- la mise en place de mesures d'évaluations et d'atténuation des risques par les personnes en charge des systèmes d'IA qui doivent évaluer et atténuer les risques sur les droits fondamentaux résultant de l'utilisation des systèmes de l'IA;
- la mise en place de mécanismes de surveillance par les personnes chargées des systèmes de l'IA notamment ceux à fort impact
- l'obligation d'information et de transparence sur les systèmes d'IA utilisés mise à la charge de toute personne mettant à disposition pour utilisation les système d'IA.
- l'obligation de tenue de registre ;
- l'établissement de mesures sur la manière dont les données sont anonymisées et l'utilisation et la gestion des données anonymées par toute personne traitant ou mettant à disposition pour utilisation les données anonymisées.

En vue d'instaurer un climat de confiance dans l'univers du numérique, le Canada a rédigé une charte du numérique basée sur dix principes, qui vise à garantir le respect de la vie privée et l'utilisation non frauduleuse des données des utilisateurs du numérique¹⁰¹. A ce titre, les entreprises se doivent d'être soumises à une obligation de transparence vis-à-vis des utilisateurs, sur l'utilisation qui est faite de leurs données.

Le Canada est en avance dans l'appréhension des systèmes d'IA. Il est en bonne voie de disposer d'un cadre réglementaire capable d'encadrer l'usage des systèmes d'IA et d'en atténuer les risques

3. Ile Maurice

- **Mauritius Artificial Intelligence Stratégie (2018-2030)**

L'Ile Maurice fait figure de proue dans le continent africain en matière d'encadrement des systèmes d'IA. En effet, il est le premier pays africain à avoir élaborer une stratégie sur les stratégies de l'IA ce qui lui permet en 2021 de se classer 1^{ère} en Afrique et 58^{ème} au plan mondial dans le 2021 AI Readiness Index¹⁰². Fixée sur la période 2018-2030, La stratégie mauricienne pour l'IA intitulée " Mauritius Artificial Intelligence Stratégie " axe son intervention sur les domaines suivants¹⁰³:

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

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

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

103 <https://ncb.govmu.org/ncb/strategicplans/MauritiusAIStrategy2018.pdf>

- la priorisation de secteurs et l'identification des projets nationaux ;
- l'attraction des compétences et le renforcement des capacités ;
- les incitations pour catalyser la mise en œuvre des systèmes de l'IA
- la prise en compte des considérations de l'IA ;
- le développement d'alliance stratégiques dans les technologies émergentes ;
- les campagnes de sensibilisation ;
- l'adoption de nouvelles technologies pour améliorer la prestation de services publics

L'Ile Maurice compte ainsi déployer les systèmes d'IA dans tous les segments de l'économie allant de l'industrie, la santé, l'agriculture, les pouvoirs publics la recherche, la formation à travers la collaboration entre le monde universitaire et le secteur privé, les transports etc. pour transformer durablement son économie.

La stratégie soutient la politique d'exonération fiscale de 8 ans aux entreprises impliquées dans des activités axées sur l'innovation pour les actifs de propriété intellectuelle développés à Maurice

La stratégie mauricienne promeut également une IA responsable et éthique qui doit conduire à la révision du cadre réglementaire actuellement en vigueur. Pour la prise en compte de l'éthique, la mise en place d'un comité permanent éthique est préconisée. La stratégie propose les modifications de la loi sur la protection des données à caractère personnel et l'élaboration d'une orientation politique pour l'ouverture des données.¹⁰⁴

Pour la mise en œuvre effective de la politique de développement d'IA en ile Maurice, un conseil a été mis en place pour guider le gouvernement sur le soutien de l'écosystème d'IA. Il faut souligner que contrairement aux stratégies Canadienne et française sur l'IA, la stratégie mauricienne ne fait pas l'objet de financement explicite et dédié, des indications sont données sur comment mettre en œuvre efficacement les systèmes de l'IA.

- **Stratégie digital Mauritius 2030**

En vue du développement du secteur du numérique, l'Ile Maurice a également élaboré une stratégie sur le numérique dénommée Digital Mauritius 2030 qui vise à renforcer la position du pays en tant que leader africain en matière de TIC. Cette stratégie est axée sur le gouvernement numérique, la cybersécurité et la protection des données, l'infrastructure TIC, l'innovation et la gestion des talents.¹⁰⁵

Concernant le cadre réglementaire, l'Ile Maurice dispose d'un dispositif légal assez complet composé entre autres des lois suivantes :

- La loi sur les technologies de l'information et de communication adoptée en 2001¹⁰⁶;
- La loi sur les transactions électroniques (2000)¹⁰⁷;
- Loi sur la cybersécurité et la cybercriminalité (2021)¹⁰⁸
- La loi sur la protection des données à caractère personnel (2017)¹⁰⁹.

- **Loi sur la protection des données à caractère personnel**

La loi mauricienne de protection des données à caractère personnel s'aligne sur les standards internationaux comme RGPD. A ce titre, elle pose une définition très large d'une donnée à caractère personnel¹¹⁰. Cette définition englobe toutes sortes de données telles que les données génétiques, les données biométriques. La loi s'applique aux responsables de traitement établis à l'intérieur du territoire mauricien mais également les responsables établis en dehors du territoire mais utilisant les installations qui sont à l'intérieur. Elle couvre

104 <https://ncb.govmu.org/ncb/strategicplans/MauritiusAIStrategy2018.pdf>

105 <https://ncb.govmu.org/ncb/strategicplans/DigitalMauritius2030.pdf>

106 <https://mitci.govmu.org/Documents/Legislations/ICT%20Act%202001%20Amended.pdf>

107 https://mitci.govmu.org/Documents/Legislations/ELECTRONIC_TRANSACTION.pdf

108 <https://mitci.govmu.org/Documents/Legislations/CyberSecurity%20and%20Cyber%20Crime%20act1621.pdf>

109 <https://mitci.govmu.org/Documents/Legislations/The%20Data%20Protection%20Act%202017.pdf>

110 Toute information relative à une personne physique identifiée ou identifiable, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs des éléments suivants

Un identifiant en ligne ou à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne, article 2 de la loi de 2017 sur la protection des données à caractère personnel.

les activités du secteur public et le secteur privé.

Pour assurer le rôle de régulation et de conformité, la loi a mis en place l'Office de Protection des données (DPO) auprès de qui doivent s'enregistrer les responsables de traitement avant toute procédure de traitement des données.

A la place des formalités préalables (déclarations et autorisations), la loi prévoit un principe d'autorégulation et de conformité de la part des responsables de traitement de données qui doivent s'assurer que le traitement de données est conforme aux dispositions de la loi.

Pèsent également sur les responsables de traitement une obligation d'évaluation d'impact lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes concernées par le traitement.

La loi leur accorde aux personnes concernées par le traitement des droits comme l'accès, la rectification, la suppression des données en cause. Pour conclure, on peut dire cette loi cherche autant que possible à équilibrer les intérêts et droits fondamentaux d'une manière qui n'entrave pas le développement technologique.

La loi prévoit des sanctions administratives pécuniaires et des sanctions pénales en cas de violation des dispositions de la loi.

- **Loi sur la cybersécurité et la cybercriminalité (2021)**

En matière de cybersécurité et cybercriminalité, l'Ile Maurice ayant signé la convention de Budapest en 2013, a adopté en 2021 une loi sur la cybersécurité et la cybercriminalité en remplacement de la loi de 2003 sur la question, devenue obsolète face aux enjeux du numériques. Cette nouvelle loi qui se veut plus répressive prévoit des peines allant de 25 ans d'emprisonnement et d'une amende de 25000 dollars US. En plus des infractions sur l'accès non autorisé à des données informatiques, la modification non autorisée de données informatique, l'interception non autorisée de service informatique, l'interférence non autorisée, les atteintes aux droits d'auteurs et droits voisins, la loi prévoit aussi de nouvelles infractions telles que :

- Les actes de cyberharcèlement ;
- Les actes terroristes ;
- La cyber-extorsion ;
- Le revenge porn.

4. Maroc

Bien que n'ayant pas encore élaboré de stratégie en matière d'IA, le Maroc est conscient de l'importance des systèmes de l'IA dans le développement économique du pays. Dans le paysage numérique marocain, on note des initiatives dans ce domaine comme la création d'un centre international d'intelligence artificielle¹¹¹, le lancement par d'un programme d'appui à la recherche en intelligence artificielle et ses applications, l'élaboration d'un projet de feuille de route nationale de l'IA¹¹². En Afrique du Nord, le Maroc n'est pas le seul à n'avoir pas élaborer de stratégie, c'est le cas de la Tunisie dont la stratégie en cours d'élaboration et l'Egypte.

- **Stratégie pour le développement du Digital (2020-2025)**

Toutefois, dans le domaine global du digital, le Maroc a rédigé une stratégie pour le développement du Digital (2020-2025) dans laquelle elle donne des orientations stratégiques pour accélérer la transformation digitale en vue de répondre aux enjeux sociaux -économiques du pays. Ces orientations sont les suivantes :

- une administration digitale au service des citoyens et des entreprises amenées par le digital au développement technologique ;
- une économie compétitive grâce aux gains de performance ;
- une société inclusive digitale.

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

112 <https://aujourd'hui.ma/economie/lintelligence-artificielle-priorite-du-chantier-de-la-transformation-digitale>

Ces orientations stratégiques se basent sur trois axes que sont :

Axe 1 : Administration digitale

L'administration digitale passe par la mise en place d'un cadre global d'interopérabilité effectif des administrations, la création de laboratoire d'innovation et la digitalisation de bout à bout des parcours des services publics des citoyens et des entreprises.

Axe 2 : Ecosystème digitale et innovation

La mise en œuvre de cet axe se fera à travers le développement de Starts up sur les technologies émergentes telles que l'IA, le big data et block Chain

Axe 3 : Inclusion sociale et développement humain

Le renforcement de l'accès aux citoyens aux aides sociales, la santé et éducation dans le sens de la réduction des inégalités sociales.

La mise en œuvre de cette stratégie nécessite notamment de légiférer sur l'administration électronique par le renforcement des textes relatifs à la gouvernance des données et en particulier des données ouvertes. Dans ce sens, le gouvernement marocain a engagé depuis 2018 un processus d'ouverture des données publiques.¹¹³

Du point de vue réglementaire, on s'attachera à étudier la loi relative à la protection des données personnelles.

- **La loi n°09-08 du 18 février 2009 sur la protection des données à caractère personnel**

Au Maroc, la protection des données personnelles est régie par la loi n°09-08 du 18 février 2009. Au sens de l'article 1 de la loi, les données personnelles s'entendent de « *toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne physique identifiée ou identifiable* » et le traitement des données est définie comme étant « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.* »

Les opérations de traitement de données sont soumises au principe de loyauté, de transparence et de proportionnalité. Par ailleurs, la loi met à la charge du responsable de traitement des obligations telles que l'accomplissement de formalités (déclaration et autorisation) devant l'autorité en charge de l'application de la loi, la Commission Nationale de Contrôle de la protection des données personnelles (CNDP), l'obligation de recueillir le consentement de la personne concernée, l'obligation de confidentialité et de sécurité des traitements et le secret professionnel.

Parallèlement la loi accorde aux personnes concernées des droits comme le droit à l'information lors de la collecte des données, le droit d'accès, le droit de rectification et le droit d'opposition à la prospection directe.

La loi prévoit également des infractions qui font l'objet de sanctions pénales et pécuniaires.

5. Kenya

Le Kenya ne dispose pas de stratégie en matière d'IA, en dépit de nombreuses initiatives sur l'IA mises en œuvre dans le pays. Toutefois, un groupe de travail de onze (11) personnes a été mis en place par le gouvernement kenyan pour l'élaboration d'une stratégie afin d'encourager les technologies émergentes telles que l'IA et la block Chain¹¹⁴. Il a été chargé au groupe de travail d'aider le gouvernement à évaluer les propositions sur la façon d'exploiter les possibilités offertes par la technologie block Chain pour accroître l'efficacité des processus et des services du secteur public, de suggérer l'utilisation à grande échelle de la block Chain dans le gouvernement et d'encourager la recherche et développement d'applications et la promotion de startups.

¹¹³[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\(Open%20Data\),-RETOUR&text=Dans%20le%20cadre%20de%20la,compter%20du%2013%20d%C3%A9cembre%202021.](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),-RETOUR&text=Dans%20le%20cadre%20de%20la,compter%20du%2013%20d%C3%A9cembre%202021.)

¹¹⁴ 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>

- **Loi n° 24-19 de 2019 sur la protection des données à caractère personnel**

Dans le domaine réglementaire, le Kenya dispose d'une loi sur la protection des données à caractère personnel (loi n° 24-19 de 2019)¹¹⁵. Cette loi est similaire à la loi mauricienne sur la protection des données à caractère personnel. A cet effet, elle pose une définition identique de donnée à caractère et du traitement desdites données. Cette loi a pour but de réglementer le traitement des données personnelles, de protéger la vie privée, de mettre en place un dispositif juridique et institutionnel de protection des données personnelles et de fournir aux personnes concernées des droits et recours pour protéger leurs données personnelles contre un traitement non conforme. Elle s'applique au traitement de données consignées dans un enregistrement, par ou pour un responsable du traitement ou un sous-traitant, en utilisant des moyens automatisés ou non, ou lorsque le responsable est établi ou réside habituellement au Kenya et traite des données personnelles pendant son séjour au Kenya ou alors lorsque le responsable n'est établi au Kenya mais traite les données personnelles de personnes situées au Kenya.

Cette loi prévoit l'obligation d'enregistrement auprès de l'Autorité en charge de la conformité, en l'occurrence le Commissaire de tout responsable de traitement ou sous-traitants. Par ailleurs, tout traitement doit être soumis au principe de transparence, de confidentialité et licéité.

En vertu de la loi, le responsable de traitement procède à une autorégulation et une mise en conformité. A ce titre, la loi lui permet de désigner un délégué à la protection des données (DPO) dans des cas spécifiques pour assurer sa conformité vis à vis la réglementation. Le responsable de traitement doit en outre procéder à une évaluation d'impact préalable ou une consultation du CPD sur la protection avant toute opération de traitement susceptible d'entraîner un risque élevé sur les droits et libertés d'une personne concernée.

La loi accorde des droits aux personnes concernées par le traitement tels que le droit d'information, d'accès, d'opposition, de rectification, de suppression et de portabilité des données.

¹¹⁵ <http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019>

Force de constater que les systèmes d'IA occupent actuellement notre quotidien et contribuent au développement grâce à ses nombreux usages dans les secteurs clés tels que l'industrie, la santé, le transport, l'éducation, l'agriculture etc. Depuis quelques années, le continent africain commence à s'approprier de l'IA pour impulser le développement du continent. Comme illustration, on note plusieurs initiatives en cours comme l'élaboration de document stratégique pour encadrer les systèmes d'IA, la mise en place de module de formation en IA, la construction de centre d'excellence sur l'IA, la mise en place de système d'information dans le domaine agricole.

Mais, si utiles qu'ils soient, ces systèmes peuvent avoir des impacts négatifs sociaux économiques notamment dans le cadre des droits fondamentaux.

Ainsi, la présente revue vise à générer une masse critique d'information sur le cadre politique, juridique relatif aux systèmes d'IA, des technologies émergentes et les données.

L'élaboration de cette revue n'a pas été sans difficultés, l'équipe s'est confrontée à l'indisponibilité et l'inaccessibilité de certains documents publics plus spécifiquement au niveau africain.

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

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

Julien Coomlan Hounkpe, Décryptage de la loi portant code du numérique au Bénin, <https://www.village-justice.com/articles/decryptage-loi-portant-code-numerique-benin,27107.html>

Quelle réglementation européenne sur l'intelligence artificielle, Antoine PETEL, Quelle réglementation européenne sur l'intelligence artificielle ? | Cairn.info

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

RECOMMANDATIONS, RÉOLUTIONS, LIGNES DIRECTRICES, LIVRE BLANC

Résolution de l'ONU en date du 21 mars 2024 « Saisir les possibilités offertes par des systèmes d'intelligence artificielle sûrs, sécurisés et dignes de confiance pour le développement durable » <https://documents.un.org/doc/undoc/ltid/n24/065/93/pdf/n2406593.pdf?token=JNBY1r3lfAfYROYaIk&fe=tru>

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

Consensus de Beijing sur l'intelligence artificielle, Beijing Consensus on Artificial Intelligence and Education - UNESCO Bibliothèque Numérique

Les Orientations de l'OMS, Éthique et gouvernance de l'intelligence artificielle pour la santé, <https://www.who.int/fr/news/item/28-06-2021-who-issues-first-global-report-on-ai-in-health-and-six-guiding-principles-for-its-design-and-use>

Recommandation de l'OCDE sur l'IA, OECD Legal Instruments

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

Lignes directrices en matière d'éthique pour une IA digne de confiance, <https://op.europa.eu/fr/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>

Recommandations en matière de politique et d'investissement pour une IA digne de confiance, <https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trust-worthy-artificial-intelligence>

TEXTES LÉGISLATIFS ET RÉGLEMENTAIRES

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 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 (TIC) | CDP

Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO CEDEAO - Acte additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO (www.droit-afrique.com) (afapdp.org)

Règlement (UE) 2016/679 du Parlement Européen Et Du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) <http://data.europa.eu/eli/reg/2016/679/oj>

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) Législation sur l'intelligence artificielle (IA): le Conseil donne son feu vert définitif aux premières règles mondiales en matière d'IA - Consilium (europa.eu)

SÉNÉGAL

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

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

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

Loi n° 2008-41 du 20 août 2008 sur la cryptologie ;

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

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

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

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

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

Décret 2008-720 du 30 juin 2008 relatif à la certification électronique

Décret d'application n°2010-1209 du 13 septembre 2010, relatif à la loi n° 2008-41 du 20 août 2008 sur la Cryptologie au Sénégal

CÔTE D'IVOIRE

La loi n° 2013-546 du 30 juillet 2013 relative aux transactions électroniques

La loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité

La loi n° 2013 – 450 du 19 juillet 2013 sur la protection des données à personnel

Loi n°2017-803 du 07 décembre 2017 d'orientation de la société de l'information

L'ordonnance n° 2012-293 du 21 mars 2012 relative aux télécommunications et technologies de l'information et de la communication

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

BENIN

Loi 2017-20 du 13 juin 2017 portant Code du Numérique

La loi n° 99-014 du 12 avril 2000 portant Organisation et Fonctionnement Conseil Nationale de Statistiques

Décret n°2016-465 du 03 aout 2016 portant obligation d'identification des abonnés aux réseaux et services de communications électroniques

BURKINA FASO

Loi n° 61-2008/AN du 27 novembre 2008 portant réglementation générale des réseaux et des services de communications électroniques ;

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

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

Loi n°12-2007 /AN du 31 mai 2007 sur les activités statistiques

La loi n°025-2018/AN du 31 mai 20218 portant Code pénal

FRANCE

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Loi n° 2016-1321 du 07 octobre 2016 pour une République numérique

CANADA

Loi sur la protection des renseignements personnels, <https://laws-lois.justice.gc.ca/fra/lois/P-21/page-1.html#h-387684>

Projet de loi C-27 du 16 juin 2022, <https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-27/premiere-lecture>

ILE MAURICE

Loi sur la protection des données à caractère personnel (2017), <https://mitci.govmu.org/Documents/Legislations/The%20Data%20Protection%20Act%202017.pdf>

Loi sur la cybersécurité et la cybercriminalité (2021), <https://mitci.govmu.org/Documents/Legislations/CyberSecurity%20and%20Cyber%20Crime%20act1621.pdf>

MAROC

Loi n°09-08 du 18 février 2009 sur la protection des données à caractère personnel, https://www.dgssi.gov.ma/sites/default/files/attached_files/loi_09-08protection_donnees_personnelles.pdf

KENYA

Loi n° 24-19 de 2019 sur la protection des données à caractère personnel, <http://kenyalaw.org:8181/exist/>

DOCUMENTS POLITIQUES ET STRATÉGIQUES

Le Cadre stratégique de l'Union Africaine de la donnée, 42078-doc-AU-DATA-POLICY-FRAMEWORK-FR.pdf

Stratégie de transformation numérique de l'Afrique 2020-2030, 38507-doc-DTS_for_Africa_2020-2030_French.pdf (au.int)

Stratégie de développement de l'Intelligence artificielle, Enabel_Strategie IA Senegal_V1.indd (ai4d.ai)

Stratégie nationale des Données (SND, Résumé de Strategie Nationale des Données du Se_230724_172910.pdf (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%20C2%AB%20Strat%C3%A9gie%20nationale%20de,aux%20objectifs%20de%20la%20SN2025>

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

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

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

Stratégie nationale d'intelligence artificielle et des mégadonnées 2023-2027, <strategie-nationale-d-intelligence-artificielle-et-des-megadonnees-2023-2027.pdf> (gouv.bj)

Stratégie Nationale de la Sécurité numérique (2020-2022), Benin, 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%A9veloppement_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>

Digital Mauritius 2030, Ile Maurice, <https://ncb.govmu.org/ncb/strategicplans/DigitalMauritius2030.pdf>

Stratégie pour le développement du Digital (2020-2025), Maroc,

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

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://aujourd'hui.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://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/>

<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019>

