

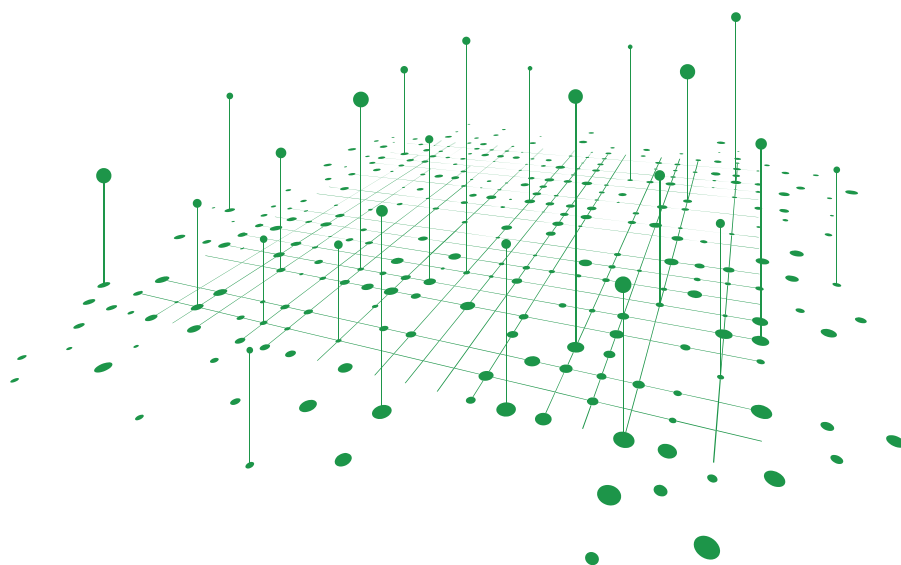


---

# STRATÉGIE NATIONALE DE LA GOUVERNANCE DES DONNÉES SNGD 2030



---





# STRATÉGIE NATIONALE DE LA GOUVERNANCE DES DONNÉES SNGD 2030

© COPYRIGHT MINISTÈRE DE LA TRANSITION NUMÉRIQUE ET DE LA  
DIGITALISATION  
CÔTE D'IVOIRE 2024.

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite ou transmise, sous quelque forme et par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre, ni stockée dans un système de récupération quelconque sans l'autorisation écrite préalable du Ministère de la Transition Numérique et de la Digitalisation, Côte d'Ivoire, pour laquelle une demande doit être adressée.

Ce document a été rédigé par LASSINA KONATÉ, Expert en Télécommunications  
Stratégiste en Transformation Digitale des entreprises  
sous la supervision du Ministère de la Transition Numérique et de la Digitalisation de la  
République de Côte  
d'Ivoire  
Et la participation active et qualitative de l'ensemble de l'écosystème du numérique et  
des données, et particulièrement des experts issus des secteurs publics, privés et des  
partenaires techniques financiers et au développement

Ministère de la Transition Numérique et de la Digitalisation  
Adresse : 17 BP 1404 Abidjan 17  
Tél : +225 2720347372  
Mail : [ministere@telecom.gouv.ci](mailto:ministere@telecom.gouv.ci)  
Site Web : [www.telecom.gouv.ci](http://www.telecom.gouv.ci)

“

**LA SNDG SE VEUT UN  
LEVIER ESSENTIEL POUR  
AMÉLIORER LA  
TRANSPARENCE DANS  
LA GESTION PUBLIQUE ET  
PROMOUVOIR UN  
DÉVELOPPEMENT  
INCLUSIF ET DURABLE  
POUR LE BÉNÉFICE DE  
TOUTES NOS  
COMMUNAUTÉS** ”

" Chers compatriotes, chers partenaires de la Côte d'Ivoire, alors que nous nous avançons résolument vers l'avenir numérique, avec en ligne de mire les grands bouleversements qualitatifs et structurels dans notre quotidien, dans nos communautés et dans nos économies entières, annoncés avec l'Intelligence Artificielle, il est devenu impérieux de reconnaître les données comme une ressource stratégique, essentielle à notre développement.

Le lancement officiel de notre stratégie nationale de la gouvernance des données à l'horizon 2030 marque une étape cruciale dans cet effort.



**Robert MAMBE BEUGRE**

Premier Ministre, Chef du  
Gouvernement, Ministre des  
Sports et du Cadre de Vie

Je salue le caractère participatif et inclusif de ce processus, depuis le début des travaux en avril 2024, qui a vu plus de 200 experts issus du secteur public, du secteur privé, ainsi que de l'ensemble de l'écosystème des données, contribuer à cette initiative, enrichie par le soutien de nos partenaires techniques et financiers.

Cette stratégie incarne notre vision d'un avenir où les données de qualité, utilisées et exploitées conformément à l'éthique et aux règles de sécurité et de respect de la confidentialité et de la vie privée, ne sont pas simplement des chiffres et des faits, mais un véritable catalyseur d'innovation.

Il s'agit à travers la SNGD 2030, de mettre en place le cadre normatif approprié, afin de libérer le potentiel socio-économique des données pour créer de la valeur, tout en renforçant notre capacité de prise de décision étatique. Cette stratégie nationale constitue également un levier essentiel pour améliorer la transparence dans la gestion publique et promouvoir un développement inclusif et durable pour le bénéfice de toutes nos communautés.

Ensemble, engageons-nous à transformer les données en un outil privilégié au service de la croissance inclusive de notre pays, stimulons l'innovation et accélérons notre marche vers un avenir prospère. C'est avec une grande détermination que nous travaillons à consacrer les données comme le socle de notre développement durable.

Continuons d'œuvrer, main dans la main, pour réaliser cette vision ambitieuse pour la Côte d'Ivoire. "



**Ibrahim Khalil KONATE**

Ministre de la Transition  
Numérique et de la Digitalisation

## Mot du **MINISTRE DE LA TRANSITION NUMERIQUE ET DE LA DIGITALISATION**

"Chers partenaires de la transformation numérique en Côte d'Ivoire dans un monde de plus en plus interconnecté, les données se positionnent comme un outil primordial d'innovation et de croissance.

Notre nation a saisi cette opportunité en élaborant une stratégie nationale pour la gouvernance des données à l'horizon 2030. Cette démarche est motivée par notre vision de maximiser la valeur et la capacité des données afin d'en faire l'outil privilégié de prise de décision de l'État, améliorant ainsi les services offerts aux citoyens et usagers, et renforçant le niveau de maturité de la gestion des données au sein de notre administration publique.

Créer de la valeur par des données de qualité, résultat d'un cadre normatif approprié, afin d'alimenter l'innovation et préparer l'introduction inévitable de l'Intelligence Artificielle, dans des secteurs aussi variés que prioritaires pour notre économie. Pour tirer profit de cette dynamique, il est impératif pour notre pays de se doter d'une stratégie robuste qui gouvernera le développement du numérique, et la gouvernance des données, assurant ainsi une transformation digitale réussie.

“

**NOUS SÉCURISONS  
NOTRE TRAJECTOIRE  
VERS UN AVENIR OÙ LES  
DONNÉES SERVIRONT  
NON SEULEMENT L'ÉTAT,  
MAIS AUSSI CHAQUE  
CITOYEN**

”

La stratégie que nous mettons en place définit les lignes directrices et les réformes nécessaires pour atteindre nos objectifs ambitieux.

Par la mise en œuvre de projets audacieux et innovants, nous sécurisons notre trajectoire vers un avenir où les données serviront non seulement l'État, mais aussi chaque citoyen, en favorisant une Côte d'Ivoire plus connectée, plus inclusive, et résolument tournée vers le progrès.

Merci pour votre engagement continu dans cette transition numérique qui porte en elle de meilleures perspectives pour notre nation."

# TABLE DES MATIÈRES

## PREMIERE PARTIE: ANALYSE DIAGNOSTIQUE DE LA GOUVERNANCE DES DONNÉES

<b>I. INTRODUCTION</b> .....	<b>16</b>
a. Contexte	
b. Méthodologie	
c. Etat des lieux	
<b>II. IMPÉRATIF DE DÉFINITION D'UNE TYPOLOGIE DES DONNÉES</b> .....	<b>21</b>
a. Introduction	
b. Nomenclature des données gouvernementales	
c. Terminologie : données publiques, données gouvernementales, données publiques	
d. Objectifs de la nomenclature	
e. Classification des données gouvernementales	
f. Niveau de sensibilité	
g. Catégorie fonctionnelle	
<b>III. CADRE REGLEMENTAIRE ET LEGISLATIF RELATIF À LA GOUVERNANCE DES DONNÉES</b> .....	<b>25</b>
a. Revue des textes existants	
b. Cartographie des textes traitants de divers aspects de la gouvernance des données en cote d'ivoire	
c. Traitement des principes de gouvernance de données dans les lois existantes	
d. Cadre juridique de la protection données à caractère personnel	
i. Normes internationales	
ii. L'Union africaine	
iii. CEDEAO	
iv. Côte d'Ivoire	
v. Principes généraux de traitement des données à caractère personnel	
L'évolution du cadre juridique de l'échange des données entre administrations	
vi. Droit des individus	
vii. Démarches auprès de l'ARTCI	
e. L'évolution du cadre juridique de l'échange des données entre administration	
<b>IV. INFRASTRUCTURES EXISTANTES</b> .....	<b>41</b>
a. Diagnostic sur les infrastructures	
b. Analyse SWOT INFRASTRUCTURES D'ACCÈS AU HAUT DÉBIT	
c. Analyse SWOT INFRASTRUCTURES DE DONNÉES	
d. Cartographie des Data Centers publics	
e. Recommandations	

<b>V. INTEROPÉRABILITÉ POUR LA GESTION ET LE PARTAGE DES DONNÉES</b> .....	<b>51</b>
a. Analyse SWOT INTEROPÉRABILITÉ ET ACCESSIBILITÉ	
b. Principes d'architectures d'une plateforme d'échange des données	
i. Architecture décentralisée	
ii. Communication sécurisée	
iii. Portails de services (Security Servers)	
iv. Gestion d'identités et des droits d'accès	
v. Interopérabilité et standards ouverts	
vi. Résilience et disponibilité	
vii. Open source et extensibilité	
viii. Contrôle et conformité	
ix. Avènement d'un état plateforme	
<b>VI. EVOLUTION DU CADRE DE L'OPEN DATA</b> .....	<b>63</b>
a. Open data : définition et principes	
b. L'open data en côte d'ivoire et dans la région	
c. Portail officiel des données ouvertes	
d. Agence nationale de la statistique (ANSTAT)	
e. Portail de données de la banque centrale des états de l'Afrique de l'ouest (BCEAO)	
f. Portail de données de la banque mondiale	
g. Limites et risques liés à l'Open Data	
<b>VII. CYBERSÉCURITÉ</b> .....	<b>70</b>
<b>VIII. LA GOUVERNANCE DES DONNÉES AU PLAN NATIONAL</b> .....	<b>72</b>
a. Evaluation de la maturité de la gouvernance des données de quelques structures et institutions	
b. La méthodologie	
c. Les interviews en présentiels	
d. Le survey en ligne	
e. Niveaux de maturité mesurés	
f. Résultats et constats	
g. Les interviews	
h. Niveau de maturité évalué/estimé	
i. Résultats	
j. Evaluation des processus en place pour la production	
k. Evaluation des processus en place pour la diffusion, la fiabilisation et la disponibilité des données	
l. Conclusions : tableau récapitulatif des principaux constats et pistes de solutions	

<b>IX. GOUVERNANCE DES DONNÉES AU PLAN RÉGIONAL ET CONTINENTAL</b>	<b>51</b>
<b>X. ENJEUX STRATÉGIQUES</b>	<b>82</b>
<b>XI. DÉFIS</b>	<b>83</b>
<b>XII. RECOMMANDATIONS FINALES</b>	<b>84</b>
<b>DEUXIEME PARTIE : STRATEGIE NATIONALE DE LA GOUVERNANCE DES DONNÉES DE L'ETAT</b>	
<b>I. CONTEXTE</b>	<b>88</b>
<b>II. LA VISION</b>	<b>90</b>
<b>III. LES PILIERS STRATÉGIQUES</b>	<b>90</b>
<b>IV. OBJECTIFS STRATÉGIQUES</b>	<b>94</b>
<b>V. LES INDICATEURS STRATEGIQUES DE PERFORMANCES</b>	<b>96</b>
<b>VI. PRINCIPES DIRECTEURS</b>	<b>99</b>
<b>VII. PLAN D' ACTIONS DÉTAILLÉ</b>	<b>94</b>
<b>VIII. CARACTÉRISTIQUES DU BUDGET</b>	<b>99</b>
a. Déclinaison	
b. Financement	
c. Impact général	
<b>IX. GOUVERNANCE ET MISE EN ŒUVRE DE LA STRATÉGIE</b>	<b>127</b>
a. Organe de gouvernance	
b. Au niveau des structures de l'administration	
<b>X. SUIVI EVALUATION</b>	<b>130</b>
<b>XI. DISPOSITIF INSTITUTIONNEL DE MISE EN ŒUVRE DE LA SNGD – 2030</b>	<b>131</b>
<b>XII. CHRONOGRAMME INDICATIF DES PROCHAINES ETAPES DE LA MISE EN ŒUVRE DE LA SNGD – 2030</b>	<b>135</b>
<b>XIII. ANNEXES</b>	<b>137</b>

# LISTE DES ABRÉVIATIONS

- **ANSI** : L'Agence nationale de la société de l'information
- **ANSSI** : Agence Nationale de la Sécurité des Systèmes d'Information
- **ANSUT** : Agence Nationale du Service Universel des Télécommunications-TIC
- **ANSTAT** : L'Agence Nationale de la Statistique
- **API** : Application Programming Interface (Interface de Programmation Applicative)
- **ARTCI** : Autorité de Régulation des Télécommunications/TIC de la Côte d'Ivoire
- **BAD** : Banque Africaine de Développement
- **BECEAO** : Banque Centrale des États de l'Afrique de l'Ouest
- **CAIDP** : Commission d'accès à l'information d'intérêt public et aux documents publics
- **CAFOP** : Centre d'Animation et de Formation Pédagogique
- **CEPICI** : Centre de Promotion des Investissements en Côte d'Ivoire
- **CICG** : Centre d'Information et de Communication Gouvernementale
- **CIVIX** : Plateforme ivoirienne d'identification numérique
- **CI** : Côte d'Ivoire
- **CNCI** : Conseil National des Chargeurs de Côte d'Ivoire
- **CNPE** : Conseil National de Politique Économique
- **CNPS** : Caisse Nationale de Prévoyance Sociale
- **CNUCED** : Conférence des Nations Unies sur le Commerce et le Développement
- **COM** : Cellule de Mise en Œuvre
- **COS** : Comité d'Orientation Stratégique
- **CPC** : Comité de Planification et de Coordination
- **CP-COM** : Centre de Production pour la Communication
- **CP-CYS** : Centre de Production pour la Cybersécurité
- **CP-SFN** : Centre de Production des Services Financiers Numériques
- **CPSE** : Coordonnateur du Plan de Suivi - Évaluation
- **CPE** : Cadre permanent d'échanges
- **CSV** : Comma-Separated Values
- **DCP** : Données à Caractère Personnel
- **DGI** : La Direction Générale des Impôts
- **DITT** : Direction de l'Informatique et des Traces Technologiques
- **DGTCP** : Direction Générale du Trésor et de la Comptabilité Publique
- **EDGI** : Indice de Gouvernance Électronique
- **EIS** : Executive Information System (ou Système d'Information pour la Direction)
- **ENA** : École Nationale d'Administration
- **ESATIC** : École Supérieure Africaine des TIC
- **ETFPA** : Établissement Technique de Formation Professionnelle et d'Apprentissage
- **FAI** : Fournisseur d'Accès à Internet
- **FTP** : File Transfer Protocol

- **GOTIC** : Groupement des Opérateurs du Secteur des Technologies de l'Information et de la Communication
- **HTTP** : HyperText Transfer Protocol
- **IA** : Intelligence Artificielle
- **ID** : Identité ou Identification
- **IMPHB** : Institut National Polytechnique Félix Houphouët-Boigny
- **INFAS** : Institut National de Formation des Agents de Santé
- **INJS** : Institut National de la Jeunesse et des Sports
- **INS** : L'Institut national de la statistique
- **IoT** : Internet of Things (Internet des Objets)
- **JSON** : JavaScript Object Notation
- **MQTT** : Message Queuing Telemetry Transport
- **MTND** : Ministère de la transition numérique et de la digitalisation
- **NIST** : National Institute of Standards and Technology
- **OGP** : Open Government Partnership
- **ONG** : Organisation Non Gouvernementale
- **ONECI** : Office National de l'État Civil et de l'Identification
- **OUA** : Organisation de l'unité africaine
- **PARAE** : Projet d'Appui au Renforcement de l'Administration Electronique
- **PA-PSGOUV** : Projet d'Appui au Programme Social du Gouvernement
- **PIB** : Produit Intérieur Brut
- **PKI** : Public Key Infrastructure (Infrastructure de Clés Publiques)
- **PLCC** : Plateforme de Lutte Contre la Cybercriminalité
- **PME** : Petite et Moyenne Entreprise
- **PND** : Plan National de Développement
- **PRIDA** : Initiative pour une politique et une réglementation en faveur de l'Afrique numérique
- **PPP** : Partenariats publics et privés
- **PSNDEA** : Projet de Solutions Numériques pour le Désenclavement des Établissements Agricoles
- **REST** : Representational State Transfer
- **RESTful** : Representational State Transfer (adjective form)
- **RGPD** : Règlement Général sur la Protection des Données
- **RNHD** : Réseau National Haut Débit
- **SME** : Small and Medium Enterprise
- **SNDG** : Stratégie Nationale de la Gouvernance des Données en Côte d'Ivoire
- **SNDI** : Société Nationale de Développement Informatique
- **SNNCI** : Stratégie Nationale du Numérique en Côte d'Ivoire
- **SOC** : Système d'Observation Continue
- **SOAP** : Simple Object Access Protocol
- **TIC** : Technologies de l'Information et de la Communication
- **UA** : Union africaine
- **UIT-T** : Union Internationale des Télécommunications - Secteur de la Normalisation des Télécommunications
- **UNITEC** : Universal Technology
- **XML** : Extensible Markup Language

# LISTE DES TABLEAUX

• <b>Tableau II.c. 1.</b> Caractéristiques des données publiques.....	22
• <b>Tableau II.c. 2.</b> Caractéristiques des données gouvernementales.....	22
• <b>Tableau II.c.3.</b> Recapitulatif des caractéristiques des données publiques et des données gouvernementales .....	23
• <b>Tableau II.d.</b> Objectifs de la nomenclature de définition des données.....	23
• <b>Tableau II.f.</b> Définition des données par niveau de sensibilité.....	24
• <b>Tableau II.g.</b> Exemple de nomenclature des données gouvernementales .....	25
• <b>Tableau III.a.</b> Cartographie des textes traitant de la gouvernance des données.....	26
• <b>Tableau III.b.</b> Traitement des principes de gouvernance des données dans les lois existantes.....	30
• <b>Tableau IV.a.</b> Analyse SWOT INFRASTRUCTURES D'ACCÈS AU HAUT DÉBIT.....	42
• <b>Tableau IV.b.</b> Analyse SWOT INFRASTRUCTURES DE DONNÉES .....	45
• <b>Tableau IV.c.</b> Cartographie des DATACENTERS PUBLICS .....	47
• <b>Tableau V.a.</b> Cadre règlementaire de l'interopérabilité .....	51
• <b>Tableau V.b.</b> Sources documentaires Diagnostique interopérabilité.....	55
• <b>Tableau V.c.</b> Analyse SWOT INTEROPÉRABILITÉ ET ACCESSIBILITÉ .....	56
• <b>Tableau VIII.b.i.</b> Les interviews en présentiels .....	73
• <b>Tableau VIII.b.iii.</b> La matrice du modèle de maturité .....	74
• <b>Tableau VIII.f.</b> Conclusions : Tableaux récapitulatifs des principaux constats et pistes de solutions .....	79
• <b>Tableau V.</b> Les indicateurs stratégiques de performances à l'horizon 2030 .....	96
• <b>Tableau VI.</b> Principes directeurs pour la gestion et la gouvernance des données de l'Etat .....	99
• <b>Tableau VII.</b> Plan d'actions détaillé de la stratégie nationale de la gouvernance des données.....	101
• <b>Tableau XI.1.</b> Dispositif institutionnel de mise en oeuvre de la SNGD 2030...	131
• <b>Tableau XI.2.</b> Composition des organes du dispositif institutionnel et désignation des membres.....	132
• <b>Tableau XII.</b> Chronogramme des prochaines étapes de la mise en oeuvre de la SNDG - 2030.....	135

# LISTE DES FIGURES

- **Figure V.a.** Recommandations suite au Diagnostic des infrastructures de haut débit ..... 44
- **Figure V.e.** Avènement d'un état plateforme ..... 62
- **Figure VI.a.i.** Domaines d'intervention et caractéristiques de l'Open data ..... 63

---

**PREMIERE PARTIE :**  
**ANALYSE**  
**DIAGNOSTIQUE DE LA**  
**GOUVERNANCE DES**  
**DONNÉES**

---

# I. INTRODUCTION

## a. Contexte

**Les économies se numérisent de plus en plus rapidement sous l'impulsion des États qui mettent en œuvre des stratégies ambitieuses de transformation digitale.** Ce qui signifie que les citoyens et les consommateurs, des secteurs privé et public, auront accès à la plupart des services sur les plateformes numériques par le biais d'appareils électroniques.

**L'activité gouvernementale génère, recueille et stocke d'énormes volumes de données grâce aux services qu'il fournit au grand public.** Le secteur privé effectue, recueille et génère des volumes extrêmement importants de données par le biais de divers services et transactions commerciales. De même, les établissements universitaires génèrent et collectent des volumes extrêmement importants de données à la suite de la recherche.

**La cinématique de la donnée, de sa création à sa transformation a pour objectif final de la valoriser qualitativement comme quantitativement.** Par ailleurs, les données sont de plus en plus considérées comme une ressource stratégique, intégrant l'élaboration des politiques, de l'innovation et de la gestion des performances dans les secteurs privé et public, et offrant de nouvelles opportunités entrepreneuriales pour les entreprises et les particuliers.

**Ainsi le rôle central des données implique une perspective politique stratégique et de haut niveau.**

qui puisse équilibrer des objectifs politiques multiples allant de la libération du potentiel économique et social des données à la prévention des préjudices associés à la collecte et au traitement de masse des données à caractère personnel.

L'utilisation des données est l'un des principaux facteurs permettant d'accélérer la réalisation de l'Agenda 2063 et des Objectifs de développement durable (ODD), l'absence de données de qualité étant identifié comme l'un des principaux obstacles à l'évaluation des progrès accomplis dans la réalisation des objectifs sous-jacents,

La **CNUCED** a constaté en 2020 que 66 % des pays du monde disposent d'une législation quelconque, que 10 % ont un projet de législation, que 19 % n'ont aucune législation et que 5 % n'ont aucune législation sur les données.

**On estime que 32 des 55 pays d'Afrique ont adopté ou repris à leur compte une forme de réglementation dont l'objectif principal consiste à protéger les données à caractère personnel.**

Dans ce contexte, la Commission a élaboré le Cadre stratégique en matière des données de l'UA, qui a été approuvé par le Conseil exécutif de l'UA en février 2022, et encourage les États membres à mettre en place et adopter des politiques, afin de libérer tout le potentiel socio-économique des données au profit des communautés.

Tenant donc compte de l'importance des données dans la future économie mondiale et des économies nationales, la Côte d'Ivoire dans la nouvelle stratégie de développement du numérique adoptée par le gouvernement en 2021, au nombre des réformes importantes, a envisagé la mise en place, à l'instar des pays développés, d'une stratégie nationale de gouvernance des données (*projet N°45 de la SNNCI*).

La mise en place de politique de données et cloud vise à permettre de réaliser la valeur socio-économique des données grâce à l'alignement des politiques, des lois et des réglementations existantes.

L'élaboration de la **Stratégie Nationale des Données en Côte d'Ivoire** contribuera à renforcer la capacité de l'État à fournir des services numériques aux citoyens, à assurer l'élaboration de politiques basées sur l'analyse des données, et à promouvoir et assurer la souveraineté et la sécurité des données, tout en complétant le dispositif législatif et juridique régissant la production, la collecte, la gestion ainsi que la propriété des données.

Elle vise en outre à mettre en place un environnement propice à la prospérité de l'écosystème des données et à créer un environnement propice à la fourniture de données et de services cloud afin d'assurer le développement socio-économique pour l'inclusion.

Le document de la **Stratégie Nationale de la Gouvernance des Données en Côte d'Ivoire** à l'horizon 2030 (SNGD2030) est structuré en trois parties principales :

- **Une étude situationnelle ou diagnostique** faisant l'état général des lieux avec un focus sur le cadre réglementaire et juridique, les infrastructures d'accès au haut débit et infrastructures de données, l'interopérabilité et l'accessibilité pour favoriser et stimuler l'Open Data, et la maturité en termes de gouvernance des données
- **Les orientations et axes stratégiques** comprenant les principes directeurs, et le plan d'action
- **Le dispositif de pilotage et de suivi-évaluation** de la mise en œuvre.

La **Stratégie Nationale de la Gouvernance des Données** en Côte d'Ivoire est en ligne avec la **Stratégie Nationale du Numérique en Côte d'Ivoire** (SNNCI 2025), le **Plan National de Développement 2021-2025**, et dans la **Vision Côte d'Ivoire 2030**.

## b. Méthodologie

Conformément aux attentes des termes de références exprimées en termes d'expertise la mission d'étude a eu l'aimable collaboration de :

- Maître Aissatou SYLLA, avocate aux barreaux de Paris et New York du cabinet DENTONS pour l'étude diagnostique du cadre réglementaire et de partage des données en Côte d'Ivoire
- Dr ETTY Claude Aubert, du cabinet DATA CONSULTING pour l'étude diagnostique de l'interopérabilité et l'accessibilité
- Du cabinet MARABU services pour le survey et les enquêtes lors de l'évaluation de la maturité de la gouvernance des données

## c. Etat des lieux au démarrage de la mission

Estimation sur une échelle de 0 à 10, confirmée par les interviews et survey au cours de la mission:

### c. Etat des lieux au démarrage de la mission

Estimation sur une échelle de 0 à 10, confirmée par les interviews et survey au cours de la mission:

	0	1	2	3	4	5	6	7	8	9	10
Réglementati on sur la classification des données	█	█									
Réglementati on sur la cybersécurité	█	█									
Règlement sur la gestion des données	█										
Réglementati on sur la protection des données	█	█	█	█	█	█					
Infrastructure / connectivité	█	█	█	█							
Numérisation	█	█	█								
Formation	█	█									
Politique Open Data	█	█									
Cadre règlementair e open Data	█										
Innovation	█	█	█	█							
Gouvernance	█	█									

Le diagnostic, et la démarche s'appuient sur diverses études et sources dont :

- **Approfondissement du secteur des télécommunications** – Plan Stratégique CI 2030 (Mc Kinsey), décembre 2018
- **Cadrage stratégique du secteur de l'économie numérique** – Plan Stratégique CI 2030 (Mc Kinsey), février 2019
- **Le rapport DE4A : Étude diagnostique de l'économie numérique de la Côte d'Ivoire**, World Bank Group, décembre 2020
- **Le Plan Stratégique Côte d'Ivoire 2030**, Présidence de la République, Conseil National de Politique Économique (CNPE), décembre 2020
- **Le rapport PARAE (Projet d'Appui au Renforcement de l'Administration Electronique)**, EY, avril 2021
- **Programme National de Développement 2021-2025**, Ministère du Plan et du Développement, janvier 2021
- **Stratégie Nationale du Numérique de la Cote d'Ivoire à l'horizon 2025**
- **Le corpus règlementaire et juridique** existant et traitant en particulier du secteur de l'économie numérique et des secteurs connexes (Protection des Consommateurs, Loi sur la concurrence, Loi sur les droits d'auteur/propriété intellectuelle, etc.)
- **Note de présentation BAD** du Projet d'Appui au Renforcement de l'Administration Electronique (PARAE) – Juin 2023
- **CNUCED – Rapport sur l'économie numérique 2021 - Flux transfrontières de données et développement : a qui profitent ces flux ?**

Autres documents de références :

- *Data conscience: algorithmic s1ege on our humanity* – Brandeis Hill Marshall PhD
- *Stratégie européenne pour les données : règlement sur la gouvernance des données-2023*
- *Data Maturity Assessment for Government: a Data Maturity Assessment Framework adapted from the Data Orchard Data Maturity Framework.*
- *CAIDP (Commission d'Accès a l'Information d'Interet Public) : Textes fondamentaux . Edtion septembre 2024* Protection des données à caractère personnel en Côte d'Ivoire : comprendre les textes de lois – Leon BRANDRE
- *Protection des données à caractère personnel : les bases légales en droit positif ivoirien* – Leon BRANDRE

## II. IMPÉRATIF DE DÉFINITION D'UNE TYPOLOGIE DES DONNÉES

### a. Introduction

La gestion des données étatiques, et plus spécifiquement leur échange et leur partage entre administrations, est devenue un enjeu majeur dans un contexte de transformation numérique accélérée. Les données gouvernementales, en tant que ressource stratégique, jouent un rôle clé dans l'amélioration des services publics, la transparence, et l'efficacité des politiques publiques. Cependant, leur exploitation soulève des questions complexes, notamment en matière de classification, de sécurité, de confidentialité, et d'interopérabilité.

Cette étude se propose d'examiner l'environnement juridique régissant la gestion des données étatiques en Côte d'Ivoire, avec un focus particulier sur l'échange et le partage entre administrations.

À travers une analyse détaillée, elle aborde la nomenclature des données gouvernementales, leur classification, et les objectifs sous-jacents à leur structuration. En parallèle, il explore l'évolution du cadre légal entourant l'open data et la protection des données à caractère personnel, tout en mettant en lumière les défis et les opportunités associés à la modernisation des pratiques de gestion des données.

Enfin, cette démarche s'inscrit dans une perspective proactive, en proposant des recommandations visant à renforcer le cadre juridique existant et à promouvoir une gouvernance efficace des données publiques en Côte d'Ivoire.

### b. Nomenclature des données gouvernementales

Afin de traiter de la question des données de l'Etat il est indispensable de définir les termes clé qui seront employés au cours de la présente étude et également de préciser les nomenclatures.

### c. Terminologie : Données publiques, données gouvernementales

Il convient de distinguer la locution « **données gouvernementales** » de « **données publiques** ».

L'information principale à retenir dans la présente section est que les données gouvernementales constituent l'ensemble le plus vaste qui comprend des données ouvertes, dites « données publiques », des données restreintes, qu'elles soient stratégiques, sensibles ou critiques, et nécessaires à la gouvernance et à l'administration.

## LES DONNÉES PUBLIQUES

Les données publiques regroupent l'ensemble des informations créées ou conservées par des organismes publics, mises à la disposition de tous sans limitation, sauf dans les cas prévus par la loi.

Les caractéristiques principales des données publiques sont les suivantes :

Tableau II.c. 1. Caractéristiques des données publiques

	CARACTÉRISTIQUES PRINCIPALES
<b>ORIGINE</b>	Elles sont produites ou collectées par des institutions publiques (administrations, collectivités locales, agences publiques). Elles peuvent aussi provenir d'organismes financés ou mandatés par l'État, tels que les organes parapublics dans le cadre de leurs activités et missions de service public ou des agences de recherche.
<b>FINALITÉ</b>	Les données publiques ont vocation à être partagées et utilisées pour favoriser la transparence, la responsabilité et l'innovation. Elles sont souvent mises à disposition dans des formats réutilisables pour les citoyens, les chercheurs et les entreprises.
<b>ACCESSIBILITÉ</b>	Les données publiques sont disponibles sans restriction majeure, souvent via des <b>portails d'open data</b> , tels que les budgets des collectivités locales ou des statistiques officielles

## LES DONNÉES GOUVERNEMENTALES

Les données gouvernementales sont toutes les informations produites, collectées ou détenues spécifiquement par des entités gouvernementales. Elles incluent à la fois des données accessibles au public et des données restreintes ou confidentielles.

Les caractéristiques principales des données gouvernementales sont les suivantes :

Tableau II.c. 2. des Caractéristiques des données gouvernementales

	CARACTÉRISTIQUES PRINCIPALES
<b>ORIGINE</b>	Elles sont produites ou collectées par des ministères, administrations centrales ou tout autre organisme relevant directement du gouvernement.
<b>ACCESSIBILITÉ</b>	Les données gouvernementales ont vocation à être utilisées pour la gestion et l'administration des politiques publiques. Elles peuvent également inclure des informations stratégiques ou sensibles liées à la gouvernance.
<b>FINALITÉ</b>	Les données gouvernementales ne sont pas nécessairement accessibles au public. En effet, certaines sont strictement réservées à l'usage interne des administrations (données confidentielles ou classifiées).

Tableau II.c.3. récapitulatif des caractéristiques des données publiques et des données gouvernementales

	CARACTÉRISTIQUES	
	DONNÉES PUBLIQUES	DONNÉES GOUVERNEMENTALES
<b>ORIGINE</b>	Toutes les institutions publiques.	Principalement les entités gouvernementales.
<b>ACCESSIBILITÉ</b>	Généralement accessibles à tous.	Certaines données sont accessibles à tous. <b>D'autres</b> sont limitées, certaines classifiées.
<b>EXEMPLE D'UTILISATION</b>	Transparence et innovation (open data).	Gestion des politiques publiques, sécurité nationale.
<b>EXEMPLES</b>	Statistiques démographiques.	Données militaires, plans stratégiques.

### d. Objectifs de la nomenclature

Tableau II.d. Objectifs de la nomenclature de définition des données

<b>ORGANISER ET STANDARDISER LES DONNÉES</b>	L'organisation permet notamment d'éviter les doublons et incohérences dans les bases de données. Par ailleurs, elle permet la facilitation de la recherche, de l'accès de la réutilisation des données.
<b>PERMETTRE LE PARTAGE ET L'ÉCHANGE DE DONNÉES ENTRE DIFFÉRENTS SERVICES PUBLICS ET AVEC DES PARTENAIRES PRIVÉS</b>	<p>Cela peut être réalisé notamment par :</p> <ul style="list-style-type: none"> <li>La standardisation des catégories de données. En effet une nomenclature claire définit des standards homogènes pour décrire, structurer et classer les données, ce qui facilite leur compréhension et leur utilisation par tous les acteurs concernés.</li> <li>La réduction des ambiguïtés en ce sens qu'en attribuant des libellés et définitions normalisés, les services publics et les partenaires privés peuvent interpréter et utiliser les données de manière cohérente, réduisant les risques d'erreur et de malentendu.</li> <li>La compatibilité technique : La nomenclature peut être associée à des formats d'échange standardisés, simplifiant ainsi l'intégration dans des systèmes diversifiés.</li> <li>Le respect des cadres juridiques et réglementaires : La nomenclature peut inclure des balises ou des classifications spécifiques aux exigences légales (par exemple, protection des données à caractère personnel, sensibilité des données, etc.).</li> </ul>
<b>FAVORISER L'INTÉGRATION DES DONNÉES</b>	<p>Afin que les prises de décisions soient basées sur des informations consolidées, il convient de s'assurer de ce qui suit :</p> <ul style="list-style-type: none"> <li>Regroupement et harmonisation : Une nomenclature standardisée permet de rassembler des données issues de diverses sources en supprimant les doublons et les incohérences, ce qui renforce la qualité et la fiabilité des analyses.</li> <li>Visualisation et analyse globale : Des données bien structurées peuvent être intégrées dans des outils d'analyse avancés (entrepôts de données, plateformes de décision) pour générer des tableaux de bord consolidés, facilitant l'accès à l'information pour les décideurs.</li> <li>Optimisation des politiques publiques : Des décisions éclairées reposent sur des données intégrées, croisées et contextualisées, aidant les autorités à mieux cerner les enjeux et à proposer des réponses adaptées.</li> <li>Innovation et collaborations : Une catégorisation claire des données facilite leur utilisation par des partenaires privés et académiques, favorisant le développement de solutions innovantes, la recherche et la mise en œuvre de projets collaboratifs.</li> </ul>

<b>AMÉLIORER L'INTEROPÉRABILITÉ</b>	Avoir une nomenclature permet de partager et d'échanger des données entre différents services publics et avec des partenaires privés. Cela favorise également l'intégration des données pour une prise de décision basée sur des informations consolidées.
<b>ASSURER LA SÉCURITÉ ET LA CONFIDENTIALITÉ</b>	Cela permet, en effet, d'identifier les niveaux de sensibilité et définir des règles d'accès et de protection adaptées. Cela permet aussi d'assurer la conformité aux cadres juridiques, tels que les lois et décrets sur la protection des données.
<b>ENCOURAGER LA TRANSPARENCE ET L'INNOVATION :</b>	Une nomenclature claire donne aux citoyens et aux entreprises la possibilité d'accéder aux données publiques (open data) dans le respect des règles définies.

## e. Classification des données gouvernementales

Les données gouvernementales (comprenant les données publiques) peuvent être classées notamment par (i) **niveau de sensibilité**, (ii) **par catégorie fonctionnelle** ou (iii) **par normes techniques**.

## f. Niveau de sensibilité

Tableau II.f. Définition des données par niveau de sensibilité

<b>LES DONNÉES CRITIQUES</b>	<p>Les données critiques sont d'une importance essentielle pour assurer la souveraineté nationale, le fonctionnement de l'État, et la protection des infrastructures vitales. Elles comprennent, entre autres, les informations relatives à la défense et à la sécurité nationale, les informations sur les infrastructures critiques telles que l'approvisionnement en énergie, en eau ou les réseaux de transport aérien.</p> <p>Données stratégiques sur les menaces ou les crises nationales (cybersécurité, terrorisme, etc.).</p> <p>Les données critiques requièrent une protection renforcée via des systèmes hautement sécurisés et une limitation stricte d'accès, réservée à des personnels autorisés.</p>
<b>LES DONNÉES SENSIBLES</b>	<p>Les données sensibles font l'objet d'une acception large et étroite.</p> <p><b>Au sens large</b>, l'expression « données sensibles » se réfère à toute information qui, si divulguées, pourraient porter préjudice à des individus, organisations ou institutions (par exemple, des dossiers administratifs confidentiels, des informations quant à l'identité ou les coordonnées bancaires).</p> <p><b>Au sens étroit</b>, l'expression « données sensible » est définie par la loi ivoirienne n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel de la manière suivante : « Toutes données à caractère personnel relatives aux opinions ou activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ». Cette définition correspond aux l'approche internationale du droit de la protection des données à caractère personnel, en ce qu'elle vise toute donnée dont le traitement abusif pourrait constituer une cause de discrimination ou porter une atteinte grave à l'intimité d'un individu</p> <p><i>Pour les besoins de la présente étude et, sauf spécification contraire, nous retiendrons l'acception large de l'expression « données sensibles ».</i></p>
<b>LES DONNÉES NON SENSIBLES</b>	<p>Les données non sensibles sont considérées n'être ni critiques ni sensibles, peuvent être rendues publiques et réutilisées pour des analyses, des recherches ou le développement d'innovations. Des exemples de données non sensibles comprennent les statistiques démographiques (taux de natalité, densité de population), les informations économiques générales (PIB, taux de chômage).</p>

## g. Catégorie fonctionnelle

Les données peuvent être classées par catégories fonctionnelles, telles que :

- **Les secteurs** (santé, éducation, transport, fiscalité, etc.) ;
- **Les types de données** (texte, images, données géospatiales, etc.) ;
- **Les usages** (statistiques, décisions politiques, services aux citoyens).

Tableau II.g. Exemple de nomenclature des données gouvernementales

CATÉGORIE	TYPE DE DONNÉES	SENSIBILITÉ	EXEMPLE
SANTÉ	Dossiers médicaux	Sensible	Informations sur les patients
ÉDUCATION	Résultats scolaires	Sensible	Notes des élèves
FINANCES PUBLIQUES	Budget national	Public	Répartition des dépenses publiques
DÉFENSE	Données militaires	Critique	Localisation et mouvement des forces armées.

## III. CADRE REGLEMENTAIRE ET LEGISLATIF RELATIF À LA GOUVERNANCE DES DONNÉES

La Côte d'Ivoire, à l'instar de bien d'autres pays au niveau régional qu'international, depuis la libéralisation du secteur en 2012, s'est dotée de textes pour régir la nouvelle société du numérique, et l'environnement des communications électroniques.

Comparée à d'autres pays à économie similaire, la Côte d'Ivoire dispose d'un corpus réglementaire et juridique favorisant l'éclosion et le développement du secteur, tout en adressant les problématiques liées à la digitalisation qui s'est accélérée depuis la pandémie de la COVID 19.

Une vingtaine de textes traitent de différents aspects des données définies comme l'information dans sa forme la plus brute.

La table ci-dessous (liste non exhaustive) donne un aperçu de l'ensemble des textes régissant le cadre réglementaire et juridique traitant des aspects relatifs aux droits en rapport avec la production, la collecte, le traitement, le partage, la protection et l'accès à certains types de données et informations devant faire l'objet d'analyse au cours de cette mission.

## a. Cartographie des textes traitants de divers aspects de la gouvernance des données en Côte d'Ivoire

Tableau III.a. Cartographie des textes traitant de la gouvernance des données

TEXTES	DESCRIPTION	CHAMPS
ORDONNANCE 2012 – 293 DU 21 MARS 2012 MODIFIÉE PAR LA LOI 2024-352 SUR LES COMMUNICATIONS ÉLECTRONIQUES	Télécommunications et technologies de l'information et de la communication	<ul style="list-style-type: none"> <li>• Sécurité des informations</li> <li>• Confidentialité</li> </ul>
LOI 2013 -450 DU 19 JUIN 2013	Protection des Données à Caractère Personnel	Collecte et traitement des données
ARTICLE 47 DE LA LOI N°2013-0450 DU 19 JUIN 2013 RELATIVE À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL, L'AUTORITÉ DE PROTECTION	Attribution, organisation et fonctionnement de l'Autorité de Protection des Données à Caractère Personnel	<ul style="list-style-type: none"> <li>• Informations des personnes concernées et les responsables de traitement de leurs droits et obligations ;</li> <li>• Répondre à toute demande d'avis portant sur un traitement de données à caractère personnel</li> </ul>
LOI 2013 -451 DU 19 JUIN 2013	Lutte contre la cybercriminalité	<ul style="list-style-type: none"> <li>• Altération de données</li> <li>• Confidentialité</li> <li>• Intégrité</li> <li>• Sincérité</li> <li>• Propriété intellectuelle</li> </ul>
LOI 2013-546 DU 30 JUILLET 2013	Transactions électroniques	Commerce électronique

LOI 2013 – 867 DU 23 DÉCEMBRE 2013	Accès à l'information d'intérêt public	<ul style="list-style-type: none"> <li>• Règles d'accès a l'information publique et aux documents publics</li> <li>• Conservation et gestion des données par les organismes publics</li> <li>• Catégorisation/classification des informations et documents publics</li> </ul>
LOI N°2013-537 DU 30 JUILLET 2013 PORTANT	Organisation du Système statistique national	Données statistiques
LOI N°2016-412 DU 15 JUIN 2016	Loi relative à la consommation	<ul style="list-style-type: none"> <li>• Droits des consommateurs</li> <li>• Protection des consommateurs</li> </ul>
LOI 2016-555 DU 26 JUILLET 2016	Droits d'auteurs et droits voisins	Propriété intellectuelle (littéraire et artistique)
LOI 2017 – 803 DU 7 DÉCEMBRE 2017	Orientation de la société de l'information en Côte d'Ivoire	<ul style="list-style-type: none"> <li>• Principes généraux, juridiques et institutionnels pour le développement de la société de l'information en Côte d'Ivoire</li> </ul> <p>La reconnaissance par l'État de ce que :</p> <ul style="list-style-type: none"> <li>• La société de l'information assure à chaque personne l'exercice des droits et libertés reconnues par la constitution</li> <li>• Accès à internet et aux réseaux de communications électroniques comme un droit fondamental</li> <li>• Garantie d'accès universel aux services de TIC</li> <li>• Garantie d'une liberté accrue pour la circulation des données et du savoir sur les réseaux de communication électronique</li> <li>• Affirmation de ce que l'environnement des TICs favorise le partage de l'information et du savoir sans restriction ni discrimination dans le respect des lois et règlements en vigueur</li> </ul>

<p><b>LOI N° 2020-950 DU 07 DÉCEMBRE 2020 MODIFIANT ET COMPLÉTANT LA LOI N° 2013-537 DU 30 JUILLET 2013</b></p>	<p>Portant organisation du système statistique national</p>	<p>Données statistiques</p>
<p><b>ORDONNANCE 2013-662 DU 20 SEPTEMBRE 2013</b></p>	<p>Relative à la Concurrence</p>	<p>Conditions de détermination des prix des biens, produits au services échanges en Côte d'ivoire sont librement par le jeu de la concurrence.</p>
<p><b>DÉCRET 2014 - 06 AOÛT 2014</b></p>	<p>Attribution, organisation et fonctionnement de la Commission d'Accès à l'Information et aux Documents Publics (CAIDP)</p>	<p>S'assurer du respect par les organismes publics, du droit des personnes d'accéder, sans discrimination, aux informations et aux documents publics</p>
<p><b>DÉCRET N° 2015 -79 DU 04 FÉVRIER 2015</b></p>	<p>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 personnel.</p>	<p>Traitement des Données à Caractère Personnel</p>
<p><b>DÉCRET N° 2021-916 DU 22 DÉCEMBRE 2021</b></p>	<p>Portant adoption du Référentiel Général de Sécurité des Systèmes d'Information et du Plan de Protection des Infrastructures Technologiques</p>	<p>Sécurité des infrastructures et SI de l'État</p>
<p><b>DÉCRET N° 2021-915 DU 22 DÉCEMBRE 2021</b></p>	<p>Portant adoption de la Politique de Sécurité des Systèmes d'Information de l'Administration Publique</p>	<p>Sécurité des infrastructures et SI de l'État</p>

DÉCRET N° 2021-913 DU 22 DÉCEMBRE 2021	Portant adoption du Référentiel Général d'Interopérabilité des Systèmes d'Information	Cadre d'interopérabilité
DÉCRET N° 2021-912 DU 22 DÉCEMBRE 2021	Portant adoption du Cadre Commun d'Urbanisation des Systèmes d'Information de l'Etat	Cadre d'urbanisation et d'interopérabilité
DÉCRET N° 2021-911 DU 22 DÉCEMBRE 2021	Portant adoption du cadre commun d'architecture de référentiel de données	Architecture de référentiel de données

## b. Traitement des principes de gouvernance de données dans les lois ivoiriennes existantes

Tableau III.b. Traitement des principes de gouvernance des données dans les lois existantes

TEXTES	INTITULÉ	CLASSIFICATION	CATÉGORISATION	LOCALISATION	SOUVERAINETÉ	SÉCURITÉ / CONFIDENTIALITÉ	TRAITEMENT ET PROTECTION DES DONNÉES
Ordonnance 2012 – 293 du 21 mars 2012 modifiée par la loi 2024-352 sur les communications électroniques	Télécommunications et technologies de l'information et de la communication						
Loi 2013 -450 du 19 juin 2013	Protection des Données à Caractère Personnel						
Loi-n-2023-593-du-7-juin-2023-modifiant-les-articles-17-33-58-60-62-et-66-de-la-loi-n-2013-451-du-19-juin-2013	Lutte contre la cybercriminalité						
Loi 2013 -546 du 30 juillet 2013	Transactions électroniques						
Loi 2013 – 867 du 23 décembre 2013	Accès à l'information d'intérêt public						
Loi n° 2020-950 du 07 Décembre 2020 modifiant et complétant la loi n° 2013-537 du 30 Juillet 2013	Organisation du Système statistique national						
Loi n°2016-412 du 15 juin 2016	Loi relative à la consommation						
Loi 2016-555 du 26 juillet 2016	Droits d'auteurs et droits voisins						
Loi 2017 – 803 du 7 décembre 2017	Orientation de la société de l'information						
Ordonnance 2013-662 du 20 septembre 2013	Relative à la Concurrence						
Décret n° 2021-916 du 22 décembre 2021	Référentiel Général de Sécurité des Systèmes d'Information et du Plan de Protection des Infrastructures Technologiques						
Décret n° 2021-915 du 22 décembre 2021	Politique de Sécurité des Systèmes d'Information de l'Administration Publique						
Décret n° 2021-913 du 22 décembre 2021	Référentiel Général d'Interopérabilité des Systèmes d'Information						
Décret n° 2021-912 du 22 décembre 2021	Cadre Commun d'Urbanisation des Systèmes d'Information de l'Etat						
Décret n° 2021-911 du 22 décembre 2021	Cadre commun d'architecture de référentiel de données						

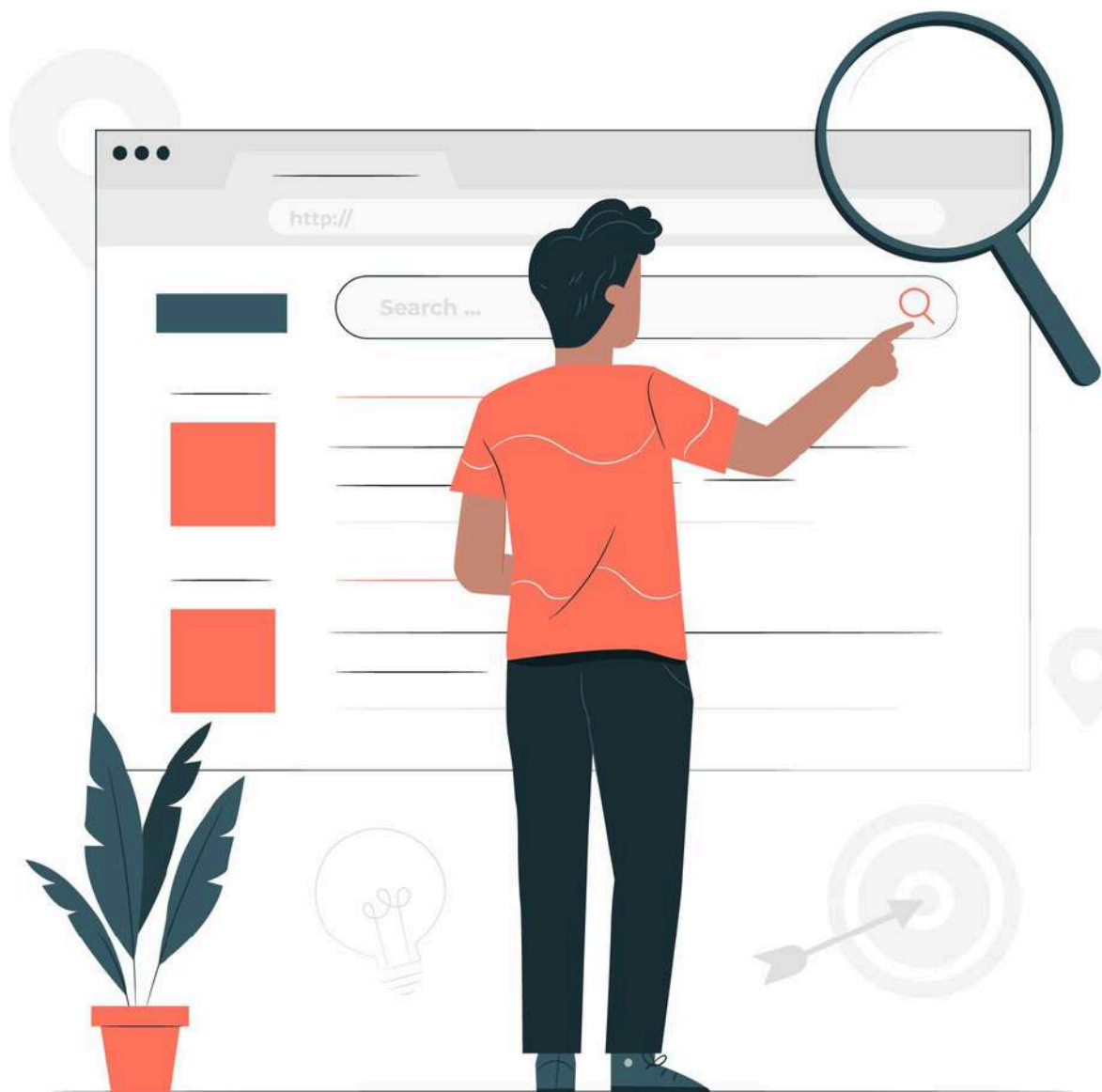
TEXTES	INTITULÉ	ACCÈS AUX DONNÉES	INTEROPÉRABILITÉ	FLUX DE DONNÉES TRANSFRONTALIERS	PROPRIÉTÉ INTELLECTUELLE	CONCURRENCE	PROTECTION DES CONSOMMATEURS
Ordonnance 2012 - 293 du 21 mars 2012	Télécommunications et technologies de l'information et de la communication						
Loi 2013 -450 du 19 juin 2013	Protection des Données à Caractère Personnel						
loi-n-2023-593-du-7-juin-2023-modifiant-les-articles-17-33-58-60-62-et-66-de-la-loi-n-2013-451-du-19-juin-2013	Lutte contre la cybercriminalité						
Loi 2013 -546 du 30 juillet 2013	Transactions électroniques						
Loi 2013 - 867 du 23 décembre 2013	Accès à l'information d'intérêt public						
Loi n° 2020-950 du 07 Décembre 2020 modifiant et complétant la loi n° 2013-537 du	Organisation du Système statistique national						
Loi n°2016-412 du 15 juin 2016	Loi relative à la consommation						
Loi 2016-555 du 26 juillet 2016	Droits d'auteurs et droits voisins						
Loi 2017 - 803 du 7 décembre 2017	Orientation de la société de l'information						
Ordonnance 2013-662 du 20 septembre 2013	Relative à la Concurrence						
Décret n° 2021-916 du 22 décembre 2021	Référentiel Général de Sécurité des Systèmes d'Information et du Plan de Protection des Infrastructures Technologiques						
Décret n° 2021-915 du 22 décembre 2021	Politique de Sécurité des Systèmes d'Information de l'Administration Publique						
Décret n° 2021-913 du 22 décembre 2021	Référentiel Général d'Interopérabilité des Systèmes d'Information						
Décret n° 2021-912 du 22 décembre 2021	Cadre Commun d'Urbanisation des Systèmes d'Information de l'Etat						
Décret n° 2021-911 du 22 décembre 2021	Cadre commun d'architecture de référentiel de données						

## CONSTATS

La Côte d'Ivoire dispose d'un cadre réglementaire et juridique robuste adressant l'ensemble des problématiques du secteur.

De nombreux champs et principes de gouvernance sont abordés y compris des problématiques souvent partiellement, et insuffisamment au regard de la nouvelle orientation.

Au regard de sa future vision qui met au cœur de la problématique de développement la nouvelle économie basée sur les données, ce cadre doit être adapté, complété afin de libérer tout le potentiel des données pour créer de la valeur.



Credits photo : [https://www.freepik.com/free-vector/web-search-concept-illustration\\_12079893.htm#fromView=search&page=1&position=43&uuiid=3160e239-e1b2-46e8-8d9b-7887b02341b9](https://www.freepik.com/free-vector/web-search-concept-illustration_12079893.htm#fromView=search&page=1&position=43&uuiid=3160e239-e1b2-46e8-8d9b-7887b02341b9)

## c. Cadre juridique de la protection données à caractère personnel

### i. Normes internationales

La protection de la vie privée est largement considérée comme un droit fondamental en Afrique et elle est proclamée dans la Constitution de la plupart des pays.

Le droit spécifique à la protection des données en Afrique a une histoire de plus de 20 ans. Le Cap-Vert a été le premier pays à promulguer des lois sur la protection des données en 2001, suivi en 2004 par Maurice et le Burkina Faso.

L'initiative de légiférer sur la protection de la vie privée n'a pas été initialement motivée par des considérations d'harmonisation au niveau régional.

**Les efforts d'harmonisation des organisations régionales africaines ont commencé à se concrétiser en 2010 avec l'adoption par la Communauté économique des États de l'Afrique de l'Ouest (« CEDEAO ») de l'Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel (2010) (« Acte additionnel de la CEDEAO ») d'une loi additionnelle sur la protection des données personnelles, après que 8 pays africains et 4 États membres de la CEDEAO ont adopté des lois.**

L'**Union africaine** a adopté la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles en 2014 (« Convention de Malabo »). À cette date, 15 pays africains avaient adopté des lois sur la protection des données.

Bien que les initiatives législatives en Afrique n'ont pas résulté initialement d'un effort d'harmonisation, les lois des différentes juridictions ont plusieurs principes en commun, dont la plupart se retrouvent dans le droit européen, par exemple la Directive sur la protection des données de 1995, telle que mise en œuvre par la France et le Royaume-Uni, le Règlement général sur la protection des données de 2016 (« **RGPD** ») et la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (« Convention 108 »), telle qu'amendée en 2018 pour incorporer les principes du **RGPD** (« Convention 108+ »). Le Cap-Vert, le Maroc, l'île Maurice, le Sénégal et la Tunisie ont d'ailleurs ratifié la Convention 108.

## ii. L'Union africaine

L'**Union africaine** est l'organisation de tous les États africains, créée en 2002 pour succéder à l'Organisation de l'unité africaine (OUA). Elle vise, entre autres, à encourager le développement économique et la stabilité politique par le biais d'une coopération accrue entre ses membres. Ses activités comprennent la diplomatie, la médiation des conflits, la recherche en économie et la communication. Les actes, traités ou accords adoptés par l'**Union africaine** doivent être ratifiés par un nombre minimum d'États membres pour entrer en vigueur, après quoi ils deviennent contraignants.

L'**Union africaine** a adopté la Convention sur la cybersécurité et la protection des données personnelles du 27 juin 2014.

L'**Union africaine** a également lancé l'Initiative pour une politique et une réglementation en faveur de l'Afrique numérique (PRIDA). L'un des objectifs de cette initiative est de créer un cadre politique et réglementaire harmonisé qui favorise la transformation et l'intégration numérique de l'Afrique. Ce projet implique un renforcement des capacités et une coopération accrue entre les régulateurs, les autorités chargées de la protection des données et la société civile.

## iii. LA CEDEAO

La principale initiative d'harmonisation régionale est l'**Acte additionnel de la CEDEAO sur la protection des données personnelles, 2010**.

Dans sa rédaction, l'Acte additionnel présente des similitudes importantes avec la loi sénégalaise de 2008 sur la protection des données.

Contrairement à l'**Union africaine** et à l'instar de l'**Union européenne**, la **CEDEAO** peut adopter des actes et règlements complémentaires qui s'appliquent directement aux États membres. Ils tendent à imposer des obligations contraignantes aux États membres pour qu'ils adoptent des lois mettant en œuvre un Acte additionnel.

L'**Acte additionnel de la CEDEAO est la seule loi régionale contraignante sur la protection des données en Afrique**. Il est accompagné d'un **Acte additionnel sur les transactions électroniques**, qui comprend des dispositions sur le commerce électronique, la publicité électronique, le marketing direct, les contrats électroniques et les signatures électroniques.

**La nature contraignante des actes additionnels explique pourquoi presque tous les États membres de la CEDEAO disposent désormais d'un cadre juridique pour la protection des données et les transactions électroniques.**

**Il convient de noter que, bien que l'Acte additionnel de la CEDEAO sur la protection des données personnelles soit contraignant, certains États membres ont choisi d'adopter des dispositions divergentes plus conformes aux normes internationales actuelles (par exemple, en basant la portée territoriale sur le lieu où se trouve la personne concernée, indépendamment du lieu où se trouve le responsable du traitement).**

#### **iv. la côte d'ivoire**

Dans le cadre des grandes réformes qui ont eu lieu en 2012 et 2013, notamment la promulgation de la loi sur les transactions électroniques, la loi portant sur le Code des postes et la loi relative à la lutte contre la cybercriminalité, **la Côte d'Ivoire a légiféré en matière de protection des données à caractère personnel en promulguant la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel (« Loi sur la protection des données »).**

Parmi les objectifs prioritaires de la **Côte d'Ivoire** par le biais de ces réformes figurent la promotion du développement, de la bonne gouvernance et de la sécurité.

Cette loi a été adoptée la même année que son équivalent malien et trois ans après l'Acte additionnel de la CEDEAO en matière de protection des données et de cybersécurité.

La Côte d'Ivoire est le quatorzième pays d'Afrique à avoir légiféré en matière de protection des données. La Côte d'Ivoire a cette particularité d'être l'un des seuls pays d'Afrique dont la législation prévoit que l'autorité en charge de la protection des données sera l'autorité en charge des télécommunications et technologies de l'information et de la communication, en l'occurrence l'Autorité de Régulation des Télécommunications/TIC de la Côte d'Ivoire (« ARTCI »).

En effet, en dehors de la loi tchadienne, la loi zimbabwéenne, la loi rwandaise et la loi de Eswatini, les lois africaines prévoient la mise en place d'une autorité ou d'une commission indépendante uniquement dédiée à la protection des données personnelles.

## v. Principes généraux de traitement des données à caractère personnel

Les principes généraux de la Loi sur la protection des données sont les suivants :

- La collecte, l'enregistrement, le traitement, le stockage et la transmission des données à caractère personnel doivent se faire de manière licite, loyale et non frauduleuse.

Les données doivent être:

- **Collectées pour des finalités déterminées**, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités.
- **Adéquates, pertinentes et non excessives** au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement.
- **Conservées pendant une durée** qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées.
- **Le traitement est légitime** si la personne concernée donne son consentement. Toutefois, il peut être dérogé à l'exigence de consentement lorsque le traitement est nécessaire :
  - **Au respect d'une obligation légale** à laquelle le responsable du traitement est soumis ;
  - **À l'exécution d'une mission d'intérêt public** ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;
  - **À l'exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ;
  - **À la sauvegarde de l'intérêt** ou des droits et libertés fondamentaux de la personne concernée.

- **Le traitement des données sensibles**, dans l'acception étroite du terme, est soumis à des règles distinctes. En effet, il est interdit de procéder à la collecte de données et à tout traitement qui révèle l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée. Les exceptions à cette interdiction sont les suivantes:
  - Lorsque le traitement des données à caractère personnel porte sur des données manifestement rendues publiques par la personne concernée.
  - Lorsque le traitement des données génétiques ou relatives à l'état de santé est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.
  - Lorsque le traitement, notamment des données génétiques, est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice de la personne concernée.
  - Lorsqu'une procédure judiciaire ou une enquête pénale est ouverte. Dans ce cas, le traitement des données à caractère personnel n'est poursuivi que pour la manifestation de la vérité.
  - Lorsque le traitement est effectué dans le cadre des activités légitimes d'une fondation, d'une association ou de tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale. Toutefois, le traitement doit se rapporter aux seuls membres de cet organismes ou aux personnes entretenant avec celui-ci des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.
- Les traitements des données à caractère personnel opérés pour le compte de l'Etat, d'une personne morale de droit public ou de droit privé gérant un service public sont autorisés par décret, après avis motivé de l'Autorité de protection. Ces traitements portent sur :
  - **La sûreté de l'Etat**, la défense nationale ou la sécurité publique ;
  - **La prévention**, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté;
  - **Le recensement** de la population ;
  - **Le traitement de salaires**, pensions, impôts, taxes et autres liquidations.

## vi. Droit des individus

La Loi sur la protection des données garantit aux individus les droits suivants :

- Droit à l'information : Le responsable du traitement doit fournir à la personne concernée au plus tard, lors de la collecte des données, les informations suivantes :
  - **L'identité** du responsable du traitement et, le cas échéant, de son représentant ;
  - **Les finalités** déterminées du traitement auquel les données sont destinées ;
  - **Les catégories** de données concernées ;
  - **Les destinataires** ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées ;
  - **Le fait de pouvoir demander à ne plus figurer sur le fichier** ;
  - **L'existence d'un droit d'accès aux données** la concernant et de rectification de ces données ;
  - **La durée de conservation** des données ;
  - **Le cas échéant**, des transferts de données à caractère personnel envisagés à destination de l'étranger.
- Droit d'accès : Toute personne physique dont les données à caractère personnel font l'objet d'un traitement peut demander sous forme de questions et obtenir du responsable de ce traitement :
  - **Les informations** permettant de connaître et de contester le traitement ;
  - **La communication des données** à caractère personnel qui la concernent ainsi que toute information disponible quant à l'origine de celles-ci.
- Droit d'opposition à un traitement : Toute personne physique concernée a le droit :
  - **De s'opposer**, pour des motifs légitimes tenant à sa situation particulière, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement, sauf en cas de dispositions légales prévoyant expressément le traitement. En cas d'opposition légitime, le traitement mis en œuvre par le responsable du traitement ne peut porter sur les données en cause ;
  - **De s'opposer**, sur sa demande et gratuitement, au traitement de données la concernant à des fins de prospection ;
  - **D'être informée** avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et de se voir expressément accorder le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

- **Droit de rectification des données** : Toute personne physique, justifiant de son identité, peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétés, mises à jour, verrouillées ou supprimées les données à caractère personnel, la concernant, qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.
  
- **Droit à l'effacement des données** : La personne concernée a le droit d'obtenir, sans délai, du responsable du traitement l'effacement de données à caractère personnel la concernant et la cessation de diffusion de ces données, en particulier en ce qui concerne des données à caractère personnel que la personne concernée avait rendues disponibles lorsqu'elle était mineure, ou pour l'un des motifs suivants :
  - Les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées ;
  - La personne concernée a retiré le consentement sur lequel est fondé le traitement ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement des données ;
  - La personne concernée s'oppose au traitement des données à caractère personnel la concernant lorsqu'il n'existe pas de motif légal audit traitement ;
  - Le traitement des données n'est pas conforme aux dispositions de la présente loi ;  
ou
  - Pour tout autre motif légitime.

## **vii. Démarches auprès de l'ARTCI**

**Avant tout transfert des données à caractère personnel vers un pays tiers**, le responsable du traitement doit préalablement obtenir l'autorisation de l'ARTCI. L'autorisation de l'ARTCI est requise même pour les transferts vers des pays apportant un niveau de protection équivalent, y compris les pays de l'Union européenne et les pays faisant l'objet d'une décision d'adéquation rendue par la Commission européenne.

**Le traitement des données à caractère personnel est soumis à une déclaration préalable auprès de l'ARTCI.** Seule la réception du récépissé donne droit à la mise en œuvre d'un traitement.

**Le récépissé doit être remis dans un délai d'un mois à compter de la réception de la déclaration**, l'absence de réponse dans le délai imparti valant rejet. Toutefois, ce délai peut être prorogé d'un mois supplémentaire sur décision motivée de l'ARTCI.

## d. L'évolution du cadre juridique de l'échange des données entre administration

Le cadre juridique ivoirien concernant l'échange de données entre administrations a évolué vers une meilleure structuration et une plus grande protection des données personnelles, tout en favorisant l'efficacité et la transparence des services publics régissant l'échange de données entre les administrations en Côte d'Ivoire.

Cela reflète une volonté accrue de moderniser l'administration publique, de renforcer la transparence et d'améliorer l'efficacité des services publics.

Les principaux instruments juridiques ont été adoptés à partir de l'année 2013. Lesdits instruments comprennent:

- **La Loi sur la protection des données dont les dispositions principales sont décrites dans la partie (IV) ci- dessus.**
- **La Loi n° 2013-546 du 30 juillet 2013** relative aux transactions électroniques. Cette loi encadre les transactions électroniques, y compris les échanges de données entre administrations. Elle vise à promouvoir la confiance dans les échanges numériques et à établir un cadre légal pour les communications électroniques.
- **L'Ordonnance n° 2017-500 du 2 août 2017** relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Cette ordonnance spécifie les modalités des échanges électroniques entre les usagers et les administrations, ainsi qu'entre les différentes autorités administratives. Elle vise à simplifier les procédures administratives et à encourager l'utilisation des technologies de l'information et de la communication dans le secteur public.
- **La mise en place du Cadre permanent d'échanges (CPE) au sein de l'ARTCI.** Le CPE a été lancé en 2022 en vue d'instaurer un dialogue continu entre les différentes parties prenantes afin de renforcer la protection des données et d'améliorer les pratiques d'échange entre les administrations.

La Côte d'Ivoire dispose d'institutions clés dans la gestion, la régulation et l'utilisation des données, telles que :

Régulateur dans la cadre de d'accès à l'information d'intérêt public et aux documents publics (« CAIDP »)	L'Agence nationale de la société de l'information (« ANSI »)	L'Institut national de la statistique (« INS »)	Centre d'Information et de Communication Gouvernementale (« CICG »)
Autorité de protection des données (« ARTCI »)	La Direction Générale des Impôts (« DGI »)	Direction Générale du Trésor et de la Comptabilité Publique (« DGTCP »)	Les universités et instituts de recherche

## IV. INFRASTRUCTURES EXISTANTES

La problématique des infrastructures dans la chaîne des valeurs des données, au regard du niveau de maturité estimé de l'administration publique en termes de gouvernance des données, conduit à aborder le diagnostic sous deux angles stratégiques:

- Les infrastructures d'accès au haut débit comme prérequis à la production et à l'utilisation des données
- Les infrastructures de données directement liées à la gouvernance des données durant leur cycle de vie : collecte, stockage, traitement, analyse, partage, destruction, etc.
- L'analyse a consisté en une revue documentaire de rapports, d'études, et de stratégies existantes (liste non exhaustive de documents en introduction).
- L'outil d'analyse SWOT a permis de déterminer les Forces, les Faiblesses, Opportunités et Menaces de l'environnement actuel des infrastructures vu sous les deux angles précités, et de l'état de préparation à l'avènement d'une économie de données et une société d'information basées sur les données.

### a. Diagnostic sur les infrastructures (Voir matrice SWOT Ci dessous)

## a. Analyse SWOT INFRASTRUCTURES D'ACCÈS AU HAUT DÉBIT

Tableau IV.a. Analyse SWOT INFRASTRUCTURES D'ACCÈS AU HAUT DÉBIT

S

- Cadre législatif et réglementaire conforme aux meilleures pratiques ;
- Existence d'une Loi d'orientation sur la société de l'information (Loi n°2017- 803 du 07 décembre 2017)
- Existence d'une stratégie nationale du numérique adoptée en décembre 2021 par le gouvernement
- Institutions disposant de ressources, de pouvoirs et d'outils réglementaires leur permettant d'exercer leurs missions ;
- Analyses et décisions de marché permettant d'une part, de mettre fin aux pratiques anticoncurrentielles et de respecter le principe d'orientation des tarifs vers les coûts, et d'autre part de disposer d'offres de référence d'accès réglementées
- Près de 30 000 km de backbone fibre optique (privés et publics) disponibles

W

- Absence de décrets d'application de la Loi d'orientation sur la société de l'information ;
- Existence de nombreuses administrations publiques et structures décentralisées non connectées au haut débit
- Absence de politique spécifique d'accélération du taux de pénétration du haut débit fixe (PME, SME, Ménages, etc.)
- Faible taux de pénétration du haut débit fixe au niveau national (moins de 5 pour cent des ménages) freinent la croissance des services numériques et constituent un défi pour les entreprises.
- Taux de pénétration national porté exclusivement par l'internet mobile

O

- Arrivée annoncée des technologies émergentes (5G, intelligence artificielle, blockchain...);
- Disponibilité de financement pour le développement des infrastructures auprès des bailleurs ;
- Existence du projet PARAE dans sa composante 2 portant sur les infrastructures numériques de base et e-services d'un financement BAD/KfW/Etat Cote d'Ivoire (111 M euros)
- Existence d'initiatives au sein de certaines entités du secteur public ayant des rôles et des responsabilités de leadership numérique définis et dotés en personnel, et certaines pratiques de planification et de mise en œuvre pertinentes (Infrastructure, plateformes, interopérabilité, Développement de Compétences, Capacité et puissance de Calcul, etc.)

T

- Insuffisance d'application des dispositions réglementaires ;
- Insuffisance des investissements publics dans les projets structurants d'infrastructures numériques
- Manque de coopération intersectorielle pour le déploiement de projets structurants d'infrastructures ;
- Ralentissement de la croissance dans le secteur des Télécommunications/TIC ;
- Insuffisance dans la gouvernance des infrastructures publiques ;
- Absence de panorama des infrastructures nationales de télécommunications/TIC ;

S

- Projet de reprise de l'initiative d'opérationnalisation des tronçons du backbone national (RNHD) installés (environ 5000 km) pour couvrir le territoire national et améliorer l'accès dans les zones rurales ;
- Taux de couverture (population) élevé de la téléphonie mobile et du haut débit mobile ;
- Taux de pénétration internet mobile élevé (91 % /Population)
- Existence d'un cadre législatif et réglementaire favorisant le développement d'une administration électronique.
- Existence de plusieurs initiatives sectorielles de digitalisation de l'administration publique
- Couverture en énergie satisfaisante, diversifiée et partiellement libéralisée ;

W

- Absence d'obligation de couverture en fonction du territoire ;
- RNHD toujours pas totalement opérationnel dans le sens des missions de service universel des télécommunications ;
- Inefficacité du Service universel des télécommunications/TIC pas encore disponible pour l'ensemble de la population ;
- Fin du PSNDEA de désenclavement des zones rurales (composantes « connectivité au haut débit mobile »)
- Faible déploiement de réseaux publics d'accès WIFI
- Le budget d'investissement de l'état est fragmenté entre les structures avec peu de coordination des investissements
- La perspective de l'analyse de rentabilisation est à peine prise en compte pour les investissements

O

- Accès ouvert, transparent et non discriminatoire aux infrastructures ;
- Acteurs de capacités de transmission nationales et internationales, et de connectivité internationale pouvant fournir la connectivité aux utilisateurs finaux ;
- Initiatives gouvernementales affichées de Couverture des zones blanches ;
- Projets de construction de centrales électriques et de centrales photovoltaïques (solaires) à travers le pays
- Déploiement effectif du CIVIX et raccordement de tous les opérateurs mobiles et FAI ;

T

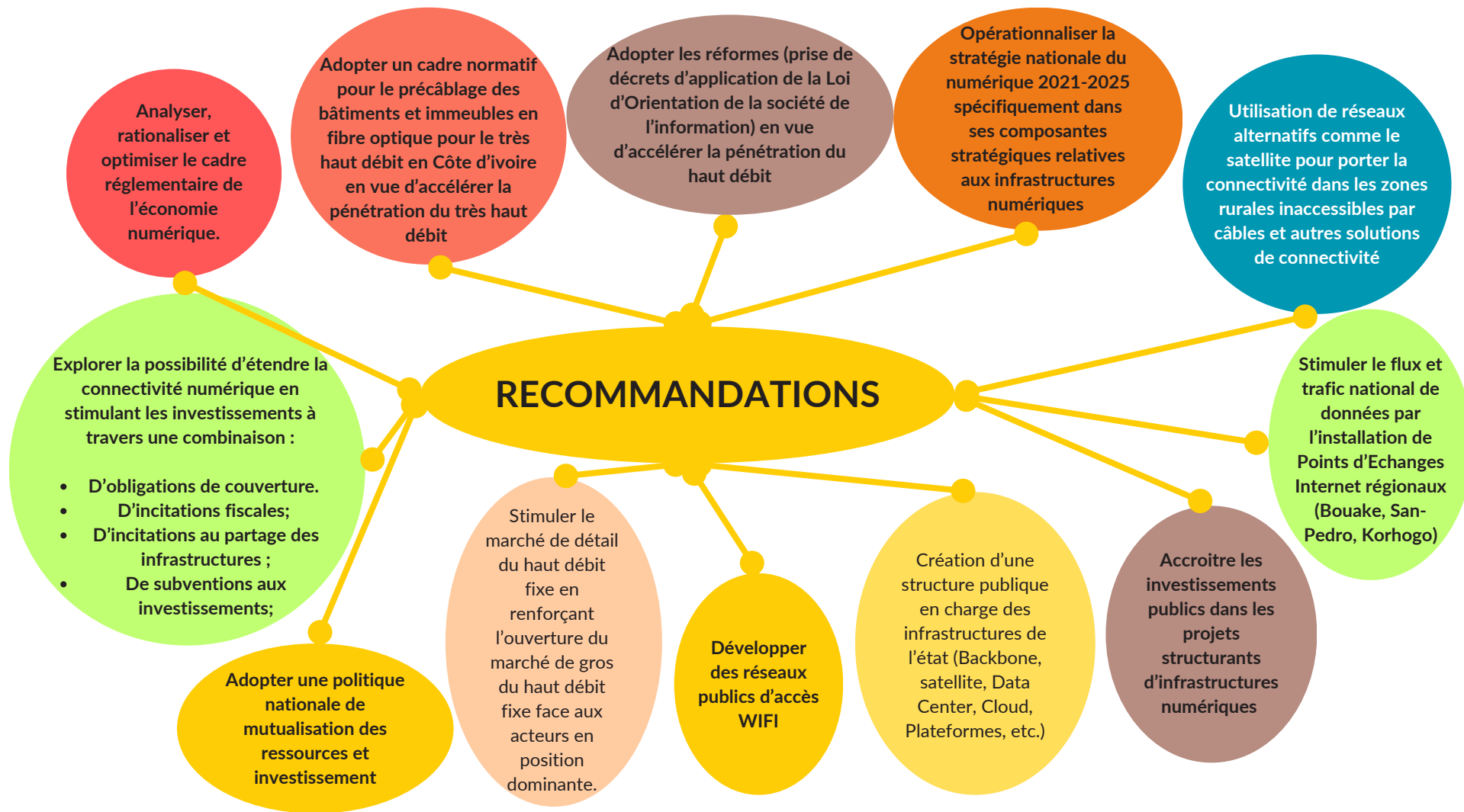
- Présence de plusieurs acteurs en situation de quasi-monopole sur certains segments de marché ;
- Coupures périodiques de câbles sous-marins ;
- Vandalisme des infrastructures de télécommunications/TIC ;
- Non-conformité aux obligations de couverture par les opérateurs
- Etat de dégradation avancée de certains tronçons du RNHD
- Récurrence des incidents physiques et attaques cybercriminelles affectant la confiance numérique
- Fin du financement Banque Mondiale du PSNDEA depuis novembre 2023
- Fracture numérique persistente
- Instabilité sur le réseau électrique ;

Malgré un cadre réglementaire et des conditions favorables pour accélérer la maturité numérique, la connectivité en vue de l'interconnexion des administrations, ainsi que le niveau de digitalisation de l'administration publique demeurent faibles.

Ainsi, l'interconnexion, l'accès des administrations au haut débit, et la poursuite de la digitalisation demeurent un défi majeur, mais surtout l'un des prérequis à une « **donneification** » de l'environnement pour une meilleure accessibilité aux services et données publics pour les citoyens.

De l'analyse situationnelle du cadre des infrastructures d'accès au haut débit, il ressort les recommandations suivantes :

Figure V.a. Recommandations suite au Diagnostic des infrastructures de haut débit



1.source : <http://www.ppp.gouv.ci/projets/portefeuille-de-projets/154>

## b. Analyse SWOT INFRASTRUCTURES DE DONNÉES

Par infrastructures de données, il est entendu l'ensemble des infrastructures permettant, la production, la collecte, le stockage, l'analyse et le partage des données.

Tableau IV.b. Analyse SWOT INFRASTRUCTURES DE DONNÉES

S

- Existence d'une Loi d'orientation sur la société de l'information (Loi n°2017- 803 du 07 décembre 2017)
- Existence d'une stratégie nationale du numérique adoptée en décembre 2021 par le gouvernement
- Des Instruments fondamentaux au niveau régional et continental de gouvernance des données (Cadre stratégique de l'UA pour la gouvernance des données, Convention de Malabo, etc.)
- Existence de lois sur les données et la propriété intellectuelle
- Existence d'autorités administratives nationales de protection des données (APD) et d'accès à l'information d'intérêt public
- Délivrance des licences/autorisations basée sur le principe de la neutralité technologique ;
- Disponibilité des investisseurs et investissements privés ;
- Environnement concurrentiel dynamique avec la présence de plusieurs acteurs internationaux disposant de capacités techniques et financières pour développer les infrastructures de données ;

W

- Absence de décrets d'application de la Loi d'orientation sur la société de l'information ;
- Pas de mutualisation des investissements dans les projets d'investissements dans les infrastructures publiques de données ;
- Multiplicité de Data Centers sectoriels
- Très peu de Datacenter qui répondent aux normes internationales ;
- Solutions cloud peu ou pas utilisées dans les administrations et la politique cloud n'est pas définie.
- Services Cloud quasi inexistant ou à l'état embryonnaire
- Coûts onéreux d'accès aux Datacenters ;
- Existence de centres de données de base, mais fragmentés et fonctionnant en silos.
- Niveau de Plateformisation insuffisante des services publics
- Peu ou pas de tentative stratégique de développement et d'utilisation de solutions en tant que plateforme à l'échelle du gouvernement (résolution de besoins/fonctionnalités communs).
- Absence d'un super calculateur

O

- Initiatives gouvernementales de digitalisation (Education nationale, Sante, ETFPA, etc.)
- Dynamisme des stratégies de digitalisation dans les structures publiques
- Donneification accélérée de l'environnement par l'introduction de plus en plus accélérée des technologies émergentes (5G, intelligence artificielle, blockchain...);
- Existence de base de données et/ou de plateformes dans le cadre de projets sectoriels
- Volonté politique de l'amélioration des services et du cadre de vie aux citoyens

T

- Insuffisance des investissements publics dans les infrastructures de données
- Absence de culture de données
- Manque de coopération intersectorielle;
- Insuffisance dans la gouvernance des infrastructures publiques
- Faible niveau d'équipements d'interconnexion entre datacenters publics /public-privé
- Récurrence des incidents physiques et attaques cybercriminelles affectant la confiance numérique ;
- Actes de sabotage sur le réseau électrique ;
- Suspension régulière de la fourniture de l'électricité.

## S

- Existence d'initiatives et de projet de digitalisation dans l'administration publique
- Existence d'un Centre National de Calcul » dote d'un calculateur de 322 teraflopes, 16 nœuds
- Existence de Data Centres sectoriels
- Existence d'initiatives de création de conditions de collecte, stockage, analyse et partage de données par certaines structures dans le cadre de leurs missions (SNDI, CNCI, ANSUT, ESATIC, INPHB)
- Existence d'une PKI nationale ;
- Couverture en énergie satisfaisante, diversifiée et partiellement libéralisée ;
- Déploiement effectif du CIVIX et raccordement de tous les opérateurs mobiles et FAI ;
- Existence de financement de base en plus du

## W

- Vétusté des infrastructures du site du Centre National de Calcul
- Inexistence d'un décret de création du Centre National de Calcul
- Fonctionnement en silos du Centre National de Calcul (format pilote académique)
- Manque et /ou Sous équipement des services publics en infrastructures de données pour la prise en charge des données durant leur cycle de vie (production, collecte, stockage, traitement, analyse, partage)
- Inexistence d'une base règlementaire et pratique pour soutenir l'initiative Open Gouvernement/Public Data Initiative)
- L'administration de l'Etat de Côte d'Ivoire ne dispose pas à date de centre de supervision sécurité (SOC) national ;
- Insuffisance de financement de base en plus du financement par projet/donateurs
- Mauvaise qualité de l'énergie électrique.
- Insuffisance de compétences dédiées à l'exploitation et la maintenance des infrastructures
- Inexistence de compétences dédiées aux nouveaux métiers des donnée

## O

- Existence d'initiatives au sein de certaines entités du secteur public ayant des rôles et des responsabilités de leadership numérique définis et dotés en personnel, et certaines pratiques de planification et de mise en œuvre pertinentes (Infrastructure, plateformes, interopérabilité, Développement de Compétences, Capacité et puissance de Calcul, etc.)
- Disponibilité de financement pour le développement des infrastructures auprès des bailleurs ;
- Accès ouvert, transparent et non discriminatoire aux infrastructures ;
- Entrée sur le marché d'opérateurs de transit IP ;
- Projets de construction de centrales électriques et de centrales photovoltaïques (solaires) à travers le pays et signatures de partenariats publics et privés (PPP) dans le secteur de l'énergie ;
- Utilisation des énergies renouvelables.

## T

- Actes de sabotage sur le réseau électrique ;
- Suspension régulière de la fourniture de l'électricité.

## c. Cartographie des datacenters publics

Tableau IV.c. Cartographie des DATACENTERS PUBLICS

#	STRUCTURES PUBLIQUES	AVÉRÉE	INITIATIVES EN PROJET
01	Data Center National		X
02	Data center public (SNDI)	✓	
03	Data centre Egouv (Bloc Conseillers)	✓	
04	Data center Présidence	✓	
05	Data Center Trésor public	✓	
06	Data center Direction du Budget	✓	
07	Data center Direction des Impôts	✓	
08	Data Center Finances	✓	
09	Data Center Douanes	✓	
10	Data Center Défense	✓	
11	Data Center Ministère de l'Éducation nationale et Alphabétisation		X
12	Data Center Enseignement Supérieur		X
13	Data Center Santé	✓	
14	Data Center DITT/PLCC	✓	
15	Data Center Cepici	✓	
16	Data center Agriculture /Conseil Café Cacao	✓	
17	Data Center ministère de l'Intérieur	✓	
18	Data center Agriculture /Conseil Café Cacao	✓	
19	Data Center GIPC Construction		X

2. <http://www.ppp.gouv.ci/projets/portefeuille-de-projets/154>

3. <http://www.ppp.gouv.ci/projets/projets-signes/154>

la cartographie des data centers publics indique une multitude de data centers pas toujours aux normes et ne disposant pas de toutes les ressources techniques et humaines pour une exploitation optimale. Les Datacenters existants sont hébergés dans des espaces restreints, avec des difficultés d'extension. Les systèmes de refroidissement ne sont pas optimaux (climatisation de confort).

Les sites de reprise des activités après incidents ne sont pas définis. Les sites de ces Datacenters existants sont vétustes (Moisissures observées dans les murs des Datacenters de la Présidence et du VITIB).

Les équipements des Datacenters sont obsolètes. Ils ne disposent pas de site secours à l'exception de celui de l'administration hébergé à la SNDI.

Dans ces conditions d'exploitation, les équipements/infrastructures deviennent très inefficaces en matière de consommation d'énergie et par conséquent très intensive en matière d'émissions de carbone.

#### **d. Le cloud computing en Côte d'Ivoire**

Selon une étude de PwC publiée en mars 2024, le marché africain du cloud connaît une croissance rapide, avec 50% des entreprises en Afrique qui ont intégré le cloud dans la majorité de leurs opérations. Cependant, il existe de réelles disparités entre pays à travers le continent, et entre entreprises privées et l'administration publique.

En Côte d'Ivoire, si des opérateurs privés comme Orange CI, MTN CI, Yango, etc. disposent d'infrastructures de pointes pour délivrer des services cloud à leurs clients, l'administration publique dans sa volonté de transformation digitale a été très tôt une pionnière en Afrique de l'Ouest, en se dotant de diverses plateformes numériques, notamment de Population à Gouvernement (P2G), de Gouvernement à Gouvernement (G2G) et de Gouvernement à Population (G2P) permettant aux individus et aux administrations publiques de se connecter et d'échanger des informations ;

Du fait des politiques de digitalisation voulues et encouragées par les états, de la création de communauté orientés vers l'innovation (Startups, Chercheurs), et dans le but surtout d'élargir l'accès et l'adoption de services et d'infrastructures publics numériques innovants et centrés sur le citoyen (« client de l'État »), ainsi que de la volonté de création d'un cyberspace de plus en plus sécurisé, **il convient de repenser l'environnement technologique des services, et évoluer vers des architectures CLOUD de plus en plus décentralisées, et dématérialisées, comme bases de l'économie des données.**

Un environnement qui permettra aux gouvernements et aux entreprises de créer le cadre approprié pour des technologies tels que l'intelligence artificielle (IA), et de tirer le meilleur parti de ces technologies pour monétiser les données et jeter les bases de la future économie souveraine des données.

Il s'agira pour l'état de se doter d'un **CLOUD NATIONAL** en raison de l'augmentation significative de l'adoption par les usagers et citoyens, du fait des politiques de transformation digitales, et des besoins de stockage de mégadonnées qui en découlent.

En outre du fait de la flexibilité et son évolutivité, l'environnement CLOUD permet de réaliser des économies d'échelles, un gain en compétitivité et un environnement sécurisé. **La politique nationale du CLOUD qui devra offrir le cadre, les ressources et les caractéristiques pour l'avènement d'une plateforme régionale et panafricaine de service dans le cadre du marché numérique unique de la ZLECAF.**

## e. Recommandations

- **Opérer et adopter** les réformes nécessaires et favorisant le développement d'une économie de données basée sur le partage et l'accessibilité sécurisées des données de l'État :
  - Définir le cadre réglementaire et pratique pour soutenir l'initiative Open Gouvernement/Public Data Initiative)
- **Opérationnaliser** les lois et décrets portant cadre normatif de l'interopérabilité et l'accessibilité :
  - Cadre commun d'urbanisation du système d'information de l'État
  - Cadre Commun d'Architecture des Référentiels de Données
  - Référentiel Général d'Interopérabilité
  - Accès à l'information d'intérêt public (Loi 2013-867 du 23 décembre 2013)
- **Adopter** une stratégie Cloud en addition de la SNGD 2030
- **Optimiser** les ressources d'investissement de l'État par la mise en place :
  - D'un Cloud national
  - Data Centre national
  - Un Centre national de Calcul aux normes
- **Equiper** les services publics en infrastructures de données pour la prise en charge des données durant leur cycle de vie (production, collecte, stockage, traitement, analyse, partage)
- **Création** d'une structure publique en charge des infrastructures de l'État (Backbone, satellite, Data Center, Cloud, Plateformes, etc.)
- **Mettre en place** un centre de données national.
- **Adopter** une politique nationale de mutualisation des ressources et investissement public dans les infrastructures de données
- **Renforcer** la plateformes des services de l'État aux citoyens et usagers
- **Élaborer** un plan directeur pour les plateformes existantes (inventorier et auditer les plateformes existantes)
- **Développer** une couche d'interopérabilité entre les plateformes existantes et la plateforme d'identification (ID).
- **Doter la Côte d'Ivoire** d'une puissance de calcul pouvant soutenir le nouvel environnement des données par :
  - La formalisation du statut et la création du Centre National de Calcul
  - La réhabilitation du Centre National de Calcul
  - Doter la Côte d'Ivoire d'un super calculateur par l'équipement du Centre National de Calcul de capacité et ressources de calcul appropriées
- **Mettre en place** une politique de formation aux métiers des données
- **Mettre en place** un SOC

## V. INTEROPÉRABILITÉ POUR LA GESTION ET LE PARTAGE DES DONNÉES

### a. Cadre réglementaire de l'interopérabilité

En plus des dispositions faisant obligation aux administrations sous les conditions déterminées par **La Loi n° 2013-546 du 30 juillet 2013**, **l'Ordonnance n° 2017-500 du 2 août 2017**, et **la Loi n° 2013-867 du 23 décembre 2013** relative à l'accès à l'information d'intérêt public, la **Côte d'Ivoire** a adopté en décembre 2021 en vue normaliser et favoriser l'interopérabilité technique entre administrations, et pour faciliter l'accessibilité cinq (5) textes importants :

Tableau V.a. Cadre réglementaire de l'interopérabilité

1	Décret n° 2021-916 du 22 décembre 2021	Portant adoption du Référentiel Général de Sécurité des Systèmes d'Information et du Plan de Protection des Infrastructures Technologiques
2	Décret n° 2021-915 du 22 décembre 2021	Portant adoption de la Politique de Sécurité des Systèmes d'Information de l'Administration Publique
3	Décret n° 2021-913 du 22 décembre 2021	Portant adoption du Référentiel Général d'Interopérabilité des Systèmes d'Information
4	Décret n° 2021-912 du 22 décembre 2021	Portant adoption du Cadre Commun d'Urbanisation des Systèmes d'Information de l'Etat
5	Décret n° 2021-911 du 22 décembre 2021	Portant adoption du cadre commun d'architecture de référentiel de données

Un dispositif qui vise à garantir la sécurité des infrastructures et systèmes d'information de l'État, à définir **un cadre d'urbanisation et d'interopérabilité de même qu'une architecture de référentiel de données**.

Il conviendra cependant, comme la plupart des textes existants abordant la question des principes de gouvernance des données, **d'affiner l'étude pour déterminer les gaps pour la mise en place d'un cadre idéal d'interopérabilité, en vue de rendre accessibles les données publiques de l'État**.

## RECOMMANDATIONS

De nombreux champs et principes de gouvernance des données sont abordés, mais très souvent partiellement, mais surtout insuffisamment au regard de la nouvelle orientation.

Au regard de sa future vision qui met au cœur de la problématique de développement la nouvelle économie basée sur les données, ce cadre doit être adapté, complété.

Pour la **Côte d'Ivoire**, l'interopérabilité des données est essentielle pour assurer une communication fluide entre les systèmes d'information des différentes administrations et entités publiques. Il est néanmoins à noter qu'il convient d'avoir un corpus juridique s'adressant frontalement à cette question.

Pour cela il est nécessaire, a minima de :

- **Définir** une nomenclature des données à l'échelle nationale qui reflète la réalité ivoirienne et qui est compatibles avec les nomenclatures internationales ;
- **Créer** des liens clairs avec tous les types de données traitées ainsi qu'une cohérence dans leur terminologie.
- **Adopter** un cadre régissant l'acquisition des données publiques par des tiers
  - **Les modalités d'accès** (gratuit ou payant, en ligne ou en physique)
  - **Respect** des directives relatives à l'Open Data.
- **Se conformer** aux règles régionales contraignantes ;
- **Harmoniser** les différentes branches du droit, les régimes réglementaires et les organismes de contrôle qui traitent des données ;
- **D'adopter** des standards communs pour assurer l'interopérabilité des systèmes d'information de l'administration publique ;
- **Renforcer le cadre législatif** en mettant à jour les lois existantes, notamment la Loi sur les données personnelles et (i) d'y inclure un volet plus conséquent relatif au traitement des données par les ou pour le compte des personnes morales de droit public ou dans le cadre de la fourniture d'un service public, (ii) de prévoir la création d'une autorité indépendante, conformément à l'obligation découlant de l'Acte additionnel de la CEDEAO et aux normes internationalement reconnues.
- **De définir** des règles de cybersécurité par une loi dédiée à la cybersécurité et des décrets d'application et autres règlements et normes impératives imposant des mesures de sécurité de l'information en fonction des catégories de données, telles que définies dans la nomenclature.
- **De renforcer** les capacités en formant les agents publics à la gestion des données numériques.

## En matière d'open data, pour éviter le risque de désinformation, il est recommandé de :

- **S'assurer** que les données publiées soient **complètes, fiables, et régulièrement mises à jour pour éviter des analyses obsolètes.**
- **Accompagner** les données ouvertes avec des guides, des tutoriels ou des exemples d'utilisation correcte.
- **Mettre en place** des équipes ou des partenariats pour surveiller l'utilisation publique des données ouvertes et réagir rapidement en cas de diffusion de fausses informations.
- **Collaborer** avec des experts et des scientifiques pour produire des interprétations rigoureuses des données.
- **Identifier** clairement les incertitudes ou limites des données (par exemple, erreurs de mesure, biais potentiels).
- **Promouvoir** une utilisation éthique des données ouvertes par des lignes directrices ou des chartes d'utilisation.

Sur le plan des technologies et infrastructures, il est recommandé de réaliser les investissements nécessaires à la modernisation des infrastructures numériques pour les rendre compatibles avec les exigences d'échange de données, notamment la mise en place d'une plateforme centralisée ou un hub d'échange sécurisé pour faciliter les transferts de données entre entités.

## b. Diagnostic sur l'interopérabilité pour la gestion et le partage des données

Sur la base d'une revue documentaire couvrant différents aspects de l'interopérabilité des données tels que les cadres réglementaires, les défis techniques et les approches innovantes, nous proposons dans le tableau ci-après une vue d'ensemble des développements récents et des approches actuelles en matière d'interopérabilité des données.

D'une manière générale, de l'analyse documentaire, il ressort qu'un cadre d'interopérabilité doit couvrir au moins les ensembles de contraintes suivants :

### Les dimensions politiques et techniques du cadre

qui devront couvrir à la fois les politiques et les règlements internes et externes (c'est-à-dire définis par l'Etat). Des accords visant à supprimer toute divergence pouvant mettre en danger la mise en œuvre de l'interopérabilité des échanges et accès aux données devront être établis à chaque fois que cela s'avérera nécessaire ;

### La dimension sémantique

qui devra reposer sur les métadonnées, lesquelles établissent un modèle des principaux concepts métier liés aux opérations de l'interopérabilité (par exemple, le partage ou les échanges de données ou l'invocation de services), ainsi que des relations entre les administrations de s'accorder sur une définition unique de ces concepts pour toutes les administrations et faciliter le traitement automatisé des données. Si l'interopérabilité concerne toutes les entités étatiques, il conviendra de préciser les métadonnées interétatiques correspondantes ;

### La dimension organisationnelle

qui devra indiquer les processus et les transactions interopérables au sein des administrations, en précisant les interfaces (API) et les niveaux de services correspondants ;

### La dimension technique

devra définir les technologies utilisées pour mettre en œuvre l'interopérabilité de manière à garantir une intégration technique adaptée de l'information et des systèmes ; cette spécification technique constituera une norme interne applicable à toute évolution institutionnelle.

### La dimension juridique

concerne l'établissement d'un cadre juridique, réglementaire et institutionnel qui encadre, facilite et protège l'échange de données entre différentes entités. Elle garantit que les échanges de données sont réalisés dans le respect des droits des parties, tout en maintenant la transparence, la responsabilité et la sécurité.

Tableau V.b. Sources documentaires Diagnostique interopérabilité

SOURCES DOCUMENTAIRES	
TITRE ET ORIGINE DU DOCUMENT	RÉSUMÉ
<b>DATA ACT (COMMISSION EUROPÉENNE, 2023)</b>	Ce document explicatif décrit le <i>Data Act</i> , une législation de l'Union Européenne qui vise à améliorer l'interopérabilité en harmonisant les normes de traitement des données. Le cadre soutient une meilleure intégration des services et la libre circulation des données entre les États membres, tout en assurant la sécurité des données.
<b>L'INTEROPÉRABILITÉ DES DONNÉES POUR LES ENTREPRISES DATA-CENTRIC</b>	Cet article explore comment l'interopérabilité permet aux entreprises orientées données de créer des flux d'information optimisés et d'améliorer la prise de décision. Il insiste sur l'importance de normaliser les données pour surmonter les défis organisationnels et sémantiques.
<b>INTÉGRATION DES API WEB ET DES TRIPLE STORES (ARXIV, 2022)</b>	Une étude sur une architecture d'intégration de données fédérée qui permet de traiter des sources de données variées, rendant l'interopérabilité possible dans des contextes industriels. Cette approche améliore la qualité et la cohérence des données échangées.
<b>MÉTHODES POUR RENDRE LES DONNÉES INTEROPÉRABLES (OPEN SCIENCE PASTEUR, 2022)</b>	Ce guide pratique détaille les méthodes permettant d'assurer l'interopérabilité des données, en abordant les normes à adopter, les technologies et les défis de gouvernance. Il encourage les institutions à collaborer autour de référentiels communs.
<b>INTEROPÉRABILITÉ INFORMATIQUE ET ÉCHANGE DE DONNÉES INTER-SYSTÈMES (ENREACH, 2022)</b>	L'article présente les concepts fondamentaux de l'interopérabilité et ses niveaux - technique, sémantique, et organisationnelle. Il met en lumière les protocoles de communication nécessaires pour un échange fluide d'informations entre systèmes variés.
<b>INTEROPÉRABILITÉ POUR LA COLLABORATION TECHNOLOGIQUE (ENREACH, 2022)</b>	Cet article souligne que l'interopérabilité est essentielle pour améliorer la collaboration technologique. En permettant aux systèmes de communiquer sans obstacles, elle réduit les redondances et optimise l'utilisation des données à travers des réseaux distribués.
<b>LANGAGE DE REQUÊTE INTER-CHAÎNES POUR LES BLOCKCHAINS (ARXIV, 2023)</b>	Une recherche innovante sur un langage de requête spécifique permettant l'interopérabilité au niveau applicatif entre blockchains. Cette solution répond aux besoins de coordination dans les réseaux décentralisés, particulièrement utiles dans le domaine de la finance.
<b>CRÉATION DE VALEUR GRÂCE À L'INTEROPÉRABILITÉ (ACCENTURE, 2023)</b>	Accenture décrit comment l'interopérabilité peut accélérer la transformation numérique des entreprises. En optimisant l'échange de données, les entreprises peuvent tirer parti de nouvelles opportunités et faciliter une croissance durable.

## c. Analyse SWOT INTEROPÉRABILITÉ ET ACCESSIBILITÉ

Tableau V.c. Analyse SWOT INTEROPÉRABILITÉ ET ACCESSIBILITÉ

S

- La Côte d'Ivoire a adopté une législation pour promouvoir l'interopérabilité.
- Cadre législatif et réglementaire conforme aux meilleures pratiques ;
- Existence d'une Loi d'orientation sur la société de l'information
- Existence d'un Cadre commun d'urbanisation du système d'information de l'état
- Existence d'un Cadre Commun d'Architecture des Référentiels de Données
- Existence d'un Référentiel Général d'Interopérabilité
- Existence d'une Loi relative à l'accès à l'information d'intérêt public (Loi 2013-867 du 23 décembre 2013)
- Existence d'une Autorité administrative autonome pour l'accès, attributions et organisation du CAIDP relative à l'accès à l'information d'intérêt public

W

- Absences de textes de mise en œuvre des lois régissant le cadre de l'interopérabilité et d'accessibilité aux données
- Absence d'une plateforme d'interopérabilité au niveau national
- Démarches administratives peu ou pas entièrement dématérialisées affectant l'accessibilité
- Fonctionnement en silos des diverses plateformes numériques (publiques et privées)
- Manque d'interopérabilité entre les plateformes numériques existantes et les services partagés entre administrations ;
- Très peu de Datacenter existants répondent aux normes internationales ;
- La majorité des services des portails proposés par les administrations est accessible depuis un périphérique mobile mais pas depuis une application dédiée.

O

- Existence d'un cadre d'interopérabilité pour les systèmes d'information du secteur public
- La publication de données ouvertes est encouragée, avec des lignes directrices et un portail national de données ouvertes opérationnels
- Existence de Programmes nationaux soutenus de digitalisation
- Volonté politique d'amélioration des e-services avec diverses initiatives pour numériser les procédures et services de l'administration publique
- Diverses initiatives visant à numériser les services de budgétisation, de passation de marché, de fiscalité et de trésorerie
- Renforcement de la confiance numérique
- Améliorations de la transparence et de l'efficacité

T

- Niveau d'Implémentation faible des stratégies nationales du numérique (SNNCI 2025), de la cybersécurité
- Insuffisance des investissements publics dans les projets structurants du secteur du numérique
- Risques de fragmentation :
- Vulnérabilité des systèmes d'information
- Cybercriminalité
- Insuffisance des investissements publics dans les problématiques de données
- Manque de coopération intersectorielle ;
- Insuffisance dans la gouvernance des infrastructures publiques ;

## S

- Existence de data centers fonctionnels bien que sectoriels
- Taux de pénétration de l'internet élevé porté par l'internet mobile (91%/population)
- Existence de diverses plateformes numériques (publiques et privées),
- Existence d'une initiative Open Government Data
- Existence de plateformes OPEN DATA :
  - Portail Open Data public (data.gouv.ci)
  - Portail de l'Agence Nationale de la Statistique (ANStat)
  - Portail de la BCEAO

## W

- Des initiatives gouvernementales sont mises en ligne mais pas accessibles via un portail unique
- Inexistence d'un site portail unique qui regroupant tous les services informationnels et transactionnels offerts par l'administration aux usagers et aux entreprises
- Insuffisance des niveaux et fonctionnalités de sécurité sur les portails existants (absence d'authentification numérique des citoyens)

Cette analyse combinée aux ensembles de contraintes nécessaires pour l'avènement d'un cadre idéal, indique un aperçu global des atouts, des limites, des perspectives et des défis de l'interopérabilité des données dans le contexte de la Côte d'Ivoire.

Les recommandations ci-dessous contribueront à améliorer l'environnement et le cadre normatif pour favoriser l'interopérabilité et l'accessibilité.

## RECOMMANDATIONS :

- **Actualiser et Opérationnaliser** les 3 décrets pris en décembre 2021 sur le Cadre d'urbanisation des SI, le cadre d'interopérabilité, et la politique des SSI
- **Dans le cadre des dimensions organisationnelles**, sémantiques et techniques de l'interopérabilité, il faudra respectivement :
  - **Au niveau organisationnel:**
    - Coordination interministérielle (structure de gouvernance et cadre de collaboration)
    - Harmonisation des processus
    - Politiques de partage des données et conformité réglementaire
    - Ressources humaines et capacité (formation continue et culture organisationnelle)
    - Gestion du changement
    - Suivi et évaluation
  - **Au niveau sémantique:**
    - Créer un catalogue des données (Dictionnaire des données, glossaire, cas d'usage)
    - Formaliser les modèles de données et standardiser les formats d'échange des données (XML, JSON, CSV)
    - Développer des ontologies spécifiques (Santé, éducation, fiscalité, ...)
    - Développer des Taxonomies pour le classement des données en catégories hiérarchiques pour organiser l'information.
    - Harmonisation des métadonnées (descriptions des données) pour que les systèmes comprennent leur contenu et leur contexte.
    - Utilisation d'interfaces (service Web et API) qui traduisent les données pour que des systèmes différents puissent les interpréter de manière cohérente.
    - Adopter des règles de cohérence et de qualité de données
    - Adopter des outils d'intégration sémantique
  - **Au niveau Technique:**
    - Avoir dans les administrations des datacenters (tiers 3), modernes interreliés
    - Concevoir à terme un cloud propre à la Côte d'Ivoire
    - Avoir le même protocole de communication (REST ou SOAP)
    - Adopter un standard d'échange des données (HTTP, MQTT , FTP)
    - API standardisée
    - Utilisation de services web comme SOAP ou RESTful
    - Adopter des standards de sécurité pour les échanges de données (chiffrement des données, infrastructure à clé publique, Blockchain, ...)
- **Définir** des règles de cybersécurité par une loi dédiée à la cybersécurité et des décrets d'application et autres règlements et normes impératives imposant des mesures de sécurité de l'information en fonction des catégories de données, telles que définies dans la nomenclature

- **S'assurer** que les données publiées soient complètes, fiables, et régulièrement mises à jour pour éviter des analyses obsolètes.
- **Accompagner** les données ouvertes avec des guides, des tutoriels ou des exemples d'utilisation correcte.
- **Mettre en place** des équipes ou des partenariats pour surveiller l'utilisation publique des données ouvertes et réagir rapidement en cas de diffusion de fausses informations.
- **Former** les agents publics aux métiers de l'interopérabilité et de la gouvernance des données
- **Promouvoir** une utilisation éthique des données ouvertes par des lignes directrices ou des chartes d'utilisation.
- **Instaurer** un « état plateforme »

Au regard de ce constat, pour renforcer l'interopérabilité des données en Côte d'Ivoire, la plateforme **X-Road**, développée par l'Estonie qui a démontré son efficacité en facilitant l'échange sécurisé et standardisé de données entre diverses institutions publiques et privées, constituerait un modèle probant basé sur les bonnes pratiques.

ÉTAPES RECOMMANDÉES POUR L'ADOPTION DE X-ROAD EN CÔTE D'IVOIRE	
<b>ÉVALUATION INITIALE</b>	Analyser les infrastructures existantes et identifier les besoins spécifiques en matière d'interopérabilité des données.
<b>FORMATION ET SENSIBILISATION</b>	Organiser des ateliers pour former les responsables techniques et administratifs à l'utilisation et à la gestion de X-Road.
<b>PHASE PILOTE</b>	Lancer un projet pilote avec quelques institutions clés pour tester l'intégration et ajuster les configurations selon les retours d'expérience.
<b>DÉPLOIEMENT PROGRESSIF</b>	Étendre l'utilisation de la plateforme à d'autres institutions et services, en assurant un support technique continu.
<b>MAINTENANCE ET AMÉLIORATION CONTINUE</b>	Mettre en place une équipe dédiée pour superviser le fonctionnement de la plateforme, assurer les mises à jour et intégrer de nouvelles fonctionnalités en fonction des besoins émergents.

## d. Principes d'architecture d'une plateforme d'échanges des données

Les principes d'architecture d'une plateforme pour les échanges de données entre plusieurs structures étatiques, telles que des ministères et des collectivités locales, visent à garantir l'interopérabilité, la sécurité, la performance, et la scalabilité.

Ci-dessous des principes clés :

### i. Architecture décentralisée

- La plateforme doit reposer sur une architecture décentralisée où chaque organisme conserve et gère ses propres données. Les données ne sont donc pas centralisées mais partagées via des connexions sécurisées entre les différents systèmes.
- Chaque organisation connectée doit disposer de ses propres services et peut décider quelles informations partager, avec qui, et sous quelles conditions, en gardant le contrôle total.

### ii. Communication sécurisée

- **Chiffrement** : Toutes les communications sur la plateforme sont chiffrées avec des protocoles SSL/TLS, garantissant que les données échangées restent confidentielles et intégrales.
- **Signature numérique** : Les données transmises sont signées numériquement à l'aide de certificats électroniques, ce qui permet de vérifier l'origine et l'authenticité des données échangées.
- **Logs immuables** : Chaque transaction effectuée via la plateforme doit être enregistrée dans des logs immuables. Ces logs permettent de retracer chaque échange pour garantir la transparence et la conformité.

### iii. Portails de services (Security Servers)

- La plateforme doit reposer sur des serveurs de sécurité (Security Servers) installés chez chaque organisation. Ces serveurs doivent assurer l'interface entre le système interne de l'organisation et le réseau de la plateforme.
- Les Security Servers doivent gérer la sécurité de la connexion et assurent le cryptage, la signature et la vérification des données, ainsi que l'authentification des échanges.

#### **iv. Gestion d'identités et des droits d'accès**

- La plateforme doit intégrer des mécanismes d'authentification forte pour s'assurer que seules les entités autorisées puissent accéder aux informations.
- Des droits d'accès granulaires permettent de définir quel système ou organisation peut accéder à quelles données, et à quel moment. Cela offre une flexibilité accrue tout en renforçant la sécurité des données.

#### **v. Interopérabilité et standards ouverts**

- La plateforme est construite sur des standards ouverts, garantissant une interopérabilité maximale entre les différents systèmes informatiques. Les protocoles et interfaces sont documentés et accessibles, ce qui facilite l'intégration de nouveaux services.
- Les services connectés à la plateforme doivent communiquer en utilisant des standards d'échange de données, comme SOAP et REST, pour garantir une compatibilité maximale avec les applications existantes.

#### **vi. Résilience et disponibilité**

- La décentralisation de la plateforme la rend très résiliente aux interruptions de service, car chaque partie conserve ses propres systèmes et peut continuer à fonctionner même si une autre partie du réseau est hors service.
- En cas de défaillance d'un serveur, les autres systèmes connectés ne sont pas affectés, ce qui garantit une haute disponibilité des services.

#### **vii. Open source et extensibilité**

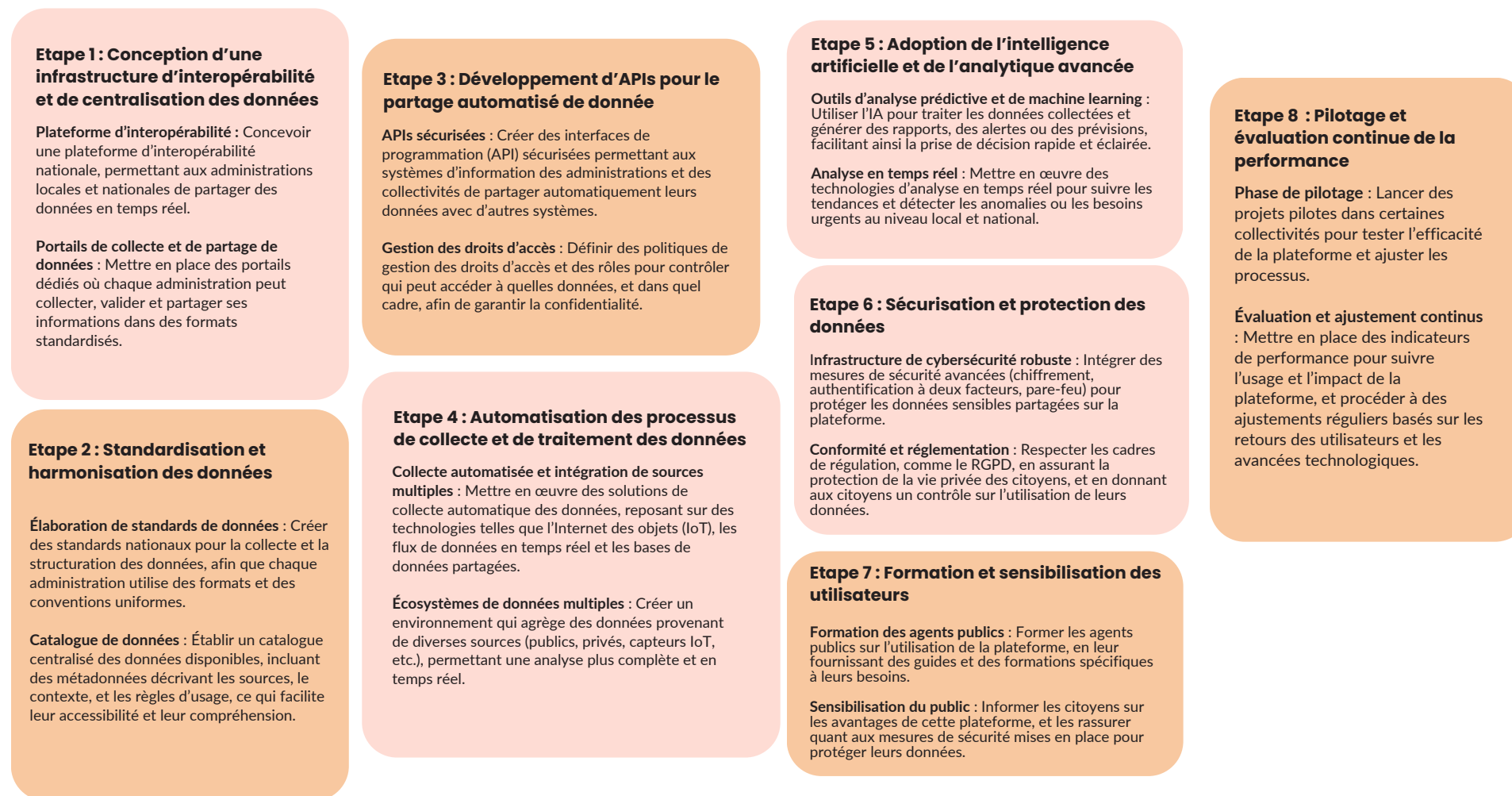
- La plateforme doit être un projet open source, ce qui permet à n'importe quelle organisation ou pays de l'adopter et de l'adapter à ses besoins spécifiques.
- Le code source ouvert permet aussi des audits réguliers pour identifier et corriger les vulnérabilités de sécurité, contribuant à la fiabilité et à la robustesse du système.

#### **viii. Contrôle et conformité**

- La plateforme doit assurer un contrôle complet des échanges de données, ce qui facilite la conformité avec les réglementations locales et internationales (comme la loi sur les données à caractère personnel).
- Les logs immuables et les transactions signées permettent de répondre aux exigences d'audit, et de garantir un suivi détaillé des échanges.

## e. AVENEMENT D'UN ETAT PLATEFORME

Figure V.e. Avènement d'un état plateforme



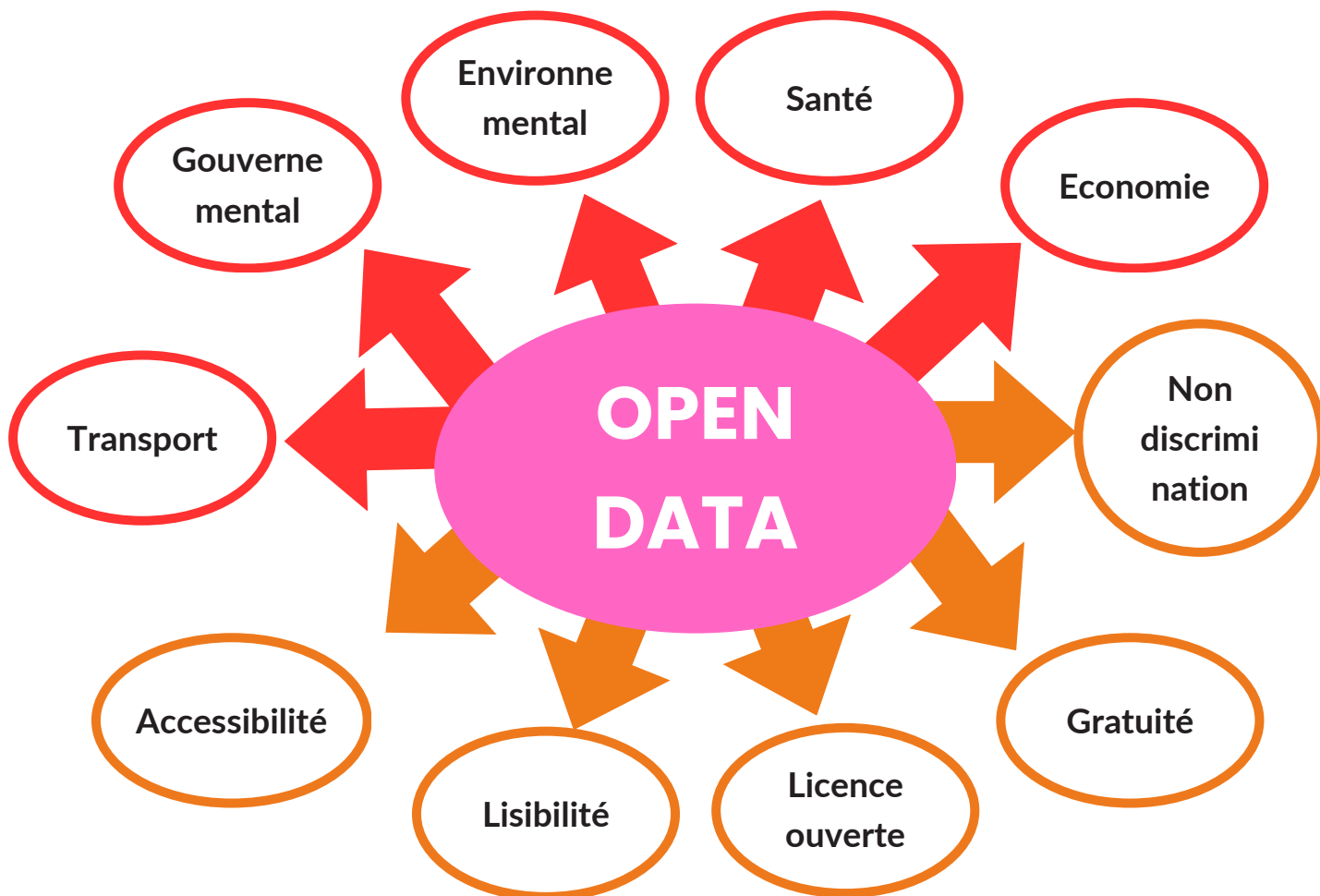
En adoptant une approche structurée et en s'appuyant sur une solution éprouvée, la Côte d'Ivoire pourra améliorer significativement l'efficacité et la transparence de ses services publics, tout en favorisant une meilleure collaboration entre les différentes entités gouvernementales et privées.

## VI. EVOLUTION DU CADRE DE L'OPEN DATA

### a. Evolution du cadre de gestion des données et de l'open data

#### i. Open data : Définition et principes

#### Domaines d'intervention de l'Open data



#### Caractéristiques principales

L'open data peut concerner une grande variété de domaines, notamment :



**Gouvernemental** : budgets publics, données démographiques, résultats électoraux.



**Environnemental** : qualité de l'air, prévisions météorologiques, données sur la biodiversité.



**Transport** : horaires de trains et bus, données sur la mobilité urbaine.



**Santé** : données épidémiologiques, statistiques hospitalières (tout en respectant la confidentialité).



**Économie** : statistiques commerciales, données sur l'emploi.

Les caractéristiques principales de l'open data comprennent :



**L'accessibilité** : Les données doivent être disponibles en ligne et accessibles sans restriction majeure (par exemple, sans avoir à remplir un formulaire complexe).



**La lisibilité et réutilisation** : Les données doivent être publiées dans des formats ouverts et standards (CSV, JSON, XML) permettant leur traitement par des machines et leur réutilisation facile.



**La licence ouverte** : Les données sont accompagnées d'une licence explicite qui définit les conditions d'utilisation (par exemple, Creative Commons, Open Data Commons).



**La gratuité** : Idéalement, les données ouvertes sont accessibles sans frais. Si un coût est associé, il doit être marginal et non dissuasif.



**La non-discrimination** : Tout utilisateur doit avoir les mêmes droits d'accès et d'utilisation.

L'open data présente de nombreux avantages qui contribuent à transformer les sociétés. Tout d'abord, **il renforce la transparence et la responsabilité des institutions publiques** en permettant aux citoyens de surveiller et de mieux comprendre les actions des gouvernements.

**Il constitue également un puissant levier d'innovation et de croissance économique**, stimulant la création de nouveaux services, applications et entreprises grâce à la réutilisation des données.

**Par ailleurs, l'accès aux données ouvertes aide les administrations à identifier les besoins de la population et à ajuster leurs politiques publiques**, améliorant ainsi la qualité des services offerts. En favorisant la participation citoyenne, l'open data incite les individus et les ONG à s'impliquer dans la résolution des problèmes sociétaux en proposant des solutions concrètes.

**Enfin, il facilite la collaboration intersectorielle en permettant un partage efficace des données entre différentes organisations**, essentiel pour aborder des problématiques complexes de manière coordonnée et innovante.

## ii. L'open data en Côte d'Ivoire et dans la région

La Côte d'Ivoire a entrepris des initiatives significatives pour promouvoir l'open data, visant à renforcer la transparence, l'innovation et la participation citoyenne. Parmi les principales plateformes et initiatives figurent les suivantes.

### iii. Portail Officiel des Données Ouvertes

En 2014, le gouvernement ivoirien a mis en place le Portail Officiel des Données Ouvertes, une plateforme centralisée où sont publiés divers jeux de données couvrant des domaines tels que l'économie, l'éducation, la santé et l'énergie.

Ce portail offre des visualisations interactives et des outils de recherche pour faciliter l'accès et la compréhension des données par les citoyens et les entreprises.

Le projet de plateforme nationale « **data.gouv.ci** » incarne concrètement les engagements pris par l'État dans le cadre du Plan d'action de la Côte d'Ivoire au sein de l'initiative internationale « **Open Government Partnership** » (OGP).

En outre, la plateforme vise à promouvoir et garantir un accès équitable aux données publiques pour tous les acteurs, qu'il s'agisse des partenaires techniques et financiers, du secteur privé, de la société civile ou des citoyens.

Parmi les données disponibles figurent les données publiques relatives :

Au suivi des réalisations dans le cadre du Projet d'Appui au Programme Social du Gouvernement (PA-PSGOUV)

À la production de la fève de cacao en Côte d'Ivoire de 1960 à 2024

Au recensement de la population ivoirienne par région

À l'attribution de certificats fonciers de 2017 à 2020.

#### iv. ANSTAT

L'Agence Nationale de la Statistique joue un rôle clé dans la collecte et la diffusion des données statistiques en Côte d'Ivoire. Elle propose une plateforme open data où sont disponibles des ensembles de données relatifs à la démographie, l'économie, l'éducation et d'autres secteurs essentiels.

#### v. BCEAO

La BCEAO offre un accès à des données économiques et financières pertinentes pour la Côte d'Ivoire, incluant des informations sur les institutions de dépôt, les réserves de la banque centrale, les taux de change et les taux d'intérêt.

#### vi. Banque Mondiale

La Banque Mondiale met à disposition des données ouvertes sur la Côte d'Ivoire, couvrant divers indicateurs de développement tels que la croissance économique, la santé, l'éducation et l'environnement.

#### vii. Limites et risques liés à l'open data

##### FIABILITÉ, EXHAUSTIVITÉ ET MAUVAISE INTERPRÉTATION

La qualité et la mise à jour des données constituent un défi majeur dans les initiatives d'open data. Les données publiées peuvent parfois être incomplètes, mal structurées ou obsolètes, ce qui limite leur utilité et leur fiabilité. Par ailleurs, la question de la confidentialité et de la sécurité des données reste cruciale. Il existe un risque de divulgation d'informations sensibles ou d'exploitation abusive des données ouvertes, ce qui peut compromettre la confiance dans ces initiatives.

**Un autre défi est le manque de standards uniformes.** L'absence de formats harmonisés pour les données rend leur intégration et leur utilisation complexe, en particulier pour les utilisateurs techniques et les développeurs. De plus, l'adoption de l'open data reste parfois limitée. **Certaines administrations ou entreprises hésitent à ouvrir leurs données par crainte de perdre un avantage concurrentiel ou de voir leurs pratiques exposées.**

Par ailleurs, l'ouverture de l'accès à une grande quantité de données peut conduire à leur mauvaise interprétation, à une manipulation intentionnelle ou à leur diffusion hors de leur contexte, ce qui pourrait générer des malentendus ou des conclusions erronées.

**La mise en œuvre de plateformes d'open data nécessite également des investissements initiaux significatifs.** L'établissement d'infrastructures pour collecter, nettoyer et publier les données peut représenter un coût élevé, qui peut décourager certains acteurs.

## DÉSINFORMATION

**Les sources de désinformation liées à l'open data proviennent souvent de divers facteurs.**

Tout d'abord, une **mauvaise interprétation des données** peut survenir lorsque des utilisateurs, peu familiarisés avec les analyses techniques ou statistiques, tirent des conclusions erronées. Cela se manifeste, par exemple, par des graphiques ou corrélations qui, bien que basés sur des données fiables, conduisent à des interprétations trompeuses.

Par ailleurs, **certaines personnes peuvent manipuler intentionnellement les données ouvertes à des fins malveillantes**, en sélectionnant uniquement les éléments qui soutiennent un point de vue biaisé ou fallacieux.

**De plus, le manque de contexte ou l'absence de métadonnées explicatives entourant les données peut compliquer leur interprétation et engendrer des erreurs**, comme dans le cas de statistiques de criminalité publiées sans explications sur les variations locales ou temporelles.

**Les outils de visualisation de données, bien que puissants, peuvent également être utilisés pour produire des graphiques trompeurs**, notamment par des choix d'échelle ou de proportions qui exagèrent ou minimisent certaines tendances.

**Enfin, des groupes ayant des intérêts politiques, commerciaux ou idéologiques spécifiques exploitent parfois les données ouvertes pour appuyer des récits orientés**, même si leurs conclusions manquent de fondements scientifiques.

**Les conséquences de cette désinformation sont nombreuses et préoccupantes.** Elle peut entraîner une **perte de confiance dans les données publiques**, compromettant ainsi la crédibilité des institutions qui les publient. En outre, une interprétation erronée des données peut **alimenter des croyances infondées et aggraver les tensions sociales**. Cela conduit également à des décisions mal informées, prises par des citoyens, entreprises ou décideurs, avec des impacts potentiellement graves. Par ailleurs, l'utilisation abusive des données dans des campagnes politiques ou idéologiques peut **intensifier la polarisation de l'opinion publique et faciliter la manipulation**.

**Quelques exemples concrets illustrent ces dérives à travers le monde :** Certaines **analyses trompeuses des données climatiques** ont servi à minimiser l'ampleur du réchauffement climatique. Dans le domaine économique, des **indicateurs comme le chômage ont été partiellement publiés ou présentés hors contexte**, créant des perceptions biaisées de la situation économique d'un pays. Ces exemples montrent comment l'open data, mal utilisé, peut devenir un vecteur de désinformation.

## viii. Cadre juridique de l'open data en Côte d'Ivoire

La Côte d'Ivoire a mis en place un cadre juridique et institutionnel pour promouvoir l'open data et assurer l'accès aux informations publiques.

La Loi n° 2013-867 du 23 décembre 2013 relative à l'accès à l'information d'intérêt public Cette loi (ci-après « **Loi d'accès à l'information** ») établit le droit des citoyens d'accéder aux informations détenues par les organismes publics. Elle définit les conditions et les limites de cet accès, tout en précisant les obligations des institutions publiques en matière de diffusion de l'information.

En vertu de la Loi d'accès à l'information :

- **Toute personne physique ou morale a le droit d'accéder, sans discrimination, à des informations d'intérêt public et documents publics détenus par les organismes publics.**
- **Les organismes publics sont tenus de diffuser au public les informations et les documents publics qu'ils détiennent.**
- **Les organismes publics doivent conserver et gérer leurs données.**
- **Les documents publics sont communicables, notamment les dossiers, rapports, études, documents d'orientation ou de politiques publiques, comptes rendus, procès-verbaux, statistiques, directives, instructions, circulaires, notes de service, avis, prévisions, décisions et réponses ministérielles qui comportent une interprétation du droit ou une description des procédures administratives.**
- **Sont communiqués uniquement à la personne concernée, les informations ou documents :**
  - **portant une appréciation ou un jugement de valeur sur sa personne ;**
  - **révélant le comportement d'une personne, dès lors que la divulgation de cette information pourrait lui porter préjudice ;**
  - **dont la communication porterait atteinte à la protection de sa vie privée, au secret médical et au secret en matière commerciale et industrielle.**

**Les données gouvernementales exclues du champ de la Loi d'accès à l'information sont les informations ou documents publics dont la divulgation porterait atteinte :**

- au secret des délibérations du Gouvernement et des autorités relevant du pouvoir exécutif ;
- au secret de la défense nationale ;
- à la conduite de la politique extérieure de l'Etat ;
- à la sûreté de l'Etat, à la sécurité publique ou à la sécurité des personnes ;
- à la politique monétaire et de change de l'Etat ;
- au déroulement des procédures engagées devant les juridictions ou enquêtes préliminaires à de telles procédures, sauf autorisation donnée par l'autorité compétente ;
- à la vie privée ou à des intérêts privés, notamment le secret en matière industrielle et commerciale, les documents mis en vente au public.

La Commission d'accès à l'information d'intérêt public et aux documents publics (CAIDP) Créée pour veiller à l'application de la Loi d'accès à l'information, la CAIDP est une autorité administrative indépendante (AAI) chargée de garantir le droit d'accès à l'information publique. Elle joue un rôle central dans la promotion de la transparence et de la bonne gouvernance en Côte d'Ivoire.

La CAIDP a été mise en place à la suite de l'adoption des décrets d'application de la Loi d'accès à l'information suivants :

- Décret n° 2014-462 du 6 août 2014 portant attribution, organisation et fonctionnement de la CAIDP.
- Décret n° 2014-784 du 11 décembre 2014 portant nomination des membres du conseil de la Commission d'accès à l'information d'intérêt public et aux documents publics.
- Décret du 9 novembre 2019 portant renouvellement partiel du conseil de la CAIDP.

La CAIDP dispose d'un pouvoir d'injonction et de sanction.

## VII. CYBERSÉCURITÉ

La Côte d'Ivoire dispose depuis 2013 d'un arsenal juridique couvrant la majorité des problématiques en matière de cybersécurité.

Ainsi dénombre-t-on :

- **l'Ordonnance 2012 - 293 du 21 mars 2012** modifiée par la loi 2024-352 sur les communications électroniques relative aux télécommunications et aux TIC (titre IX, chapitre 3), obligeant les opérateurs et fournisseurs de services à garantir le secret des communications (article 162) et à prendre les mesures propres à assurer la protection, l'intégrité et la confidentialité des données à caractère personnel (article 164), ainsi que la sécurité des communications (article 167) ;
- **la Loi n° 2013-450 du 19 juin 2013** relative à la protection des données à caractère personnel ;
- **la Loi n° 2013-451 du 19 Juin 2013** relative à la lutte contre la cybercriminalité ;
- **la Loi n° 2013-546 du 30 Juillet 2013** relative aux transactions électroniques ;
- **la loi n° 2017-803 du 7 décembre 2017** d'orientation de la Société de l'information en Côte d'Ivoire stipule que :
  - *La législation et la réglementation en matière de télécommunication/TIC doivent garantir la sécurité et la redondance des réseaux de communication électronique (article 7), et assurer dans les meilleures conditions possibles la sécurité des réseaux et systèmes d'information (article 8),*
  - *Les responsables de réseaux et systèmes d'information doivent prendre toutes les mesures utiles pour en assurer la sécurité (article 8),*
  - *L'État met en place une politique nationale de sécurité des infrastructures et services TIC (article 18) ;*
- **L'Ordonnance n° 2017-500 du 02 août 2017** relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, qui prévoit la mise en place, par décret, d'un ensemble de référentiels portant notamment sur la sécurité des données échangées par voie électronique ;
- **le décret n° 2014-105 du 12 Mars 2014** portant définition des conditions de fourniture des prestations de cryptologie ;
- **le Décret n° 2014-106 du 12 Mars 2014** fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique ;
- **le décret n° 2016-851 du 19 octobre 2016** fixant les modalités de mise en œuvre de l'archivage électronique ;
- **le décret n° 2020-128 du 29 Janvier 2020** portant création, organisation et fonctionnement du centre de veille et de réponse aux incidents de sécurité informatique (CI-CERT).

**Dans le cadre de l'effort international de coordination de la lutte, la Côte d'Ivoire** est par ailleurs partie prenante dans différentes initiatives régionales et internationales de cybersécurité et de lutte contre la cybercriminalité.

Elle a adopté une **Stratégie Nationale de Cybersécurité en décembre 2021**, et par le décret 2024-958 du 30 octobre 2024, a mis en place l'Agence Nationale de la Sécurité des Systèmes d'Information.

L'ANSSI assure la mise en œuvre des plans d'action, la coordination- et la gestion des crises de Cybersécurité, la coordination des actions de protection des infrastructures critiques et des systèmes d'information publics et privés ainsi que de pilotage des processus de prévention : de protection, de surveillance, de détection et de réponses aux incidents

4

Cependant la problématique de la cybersécurité reste multiforme et changeante, plus particulièrement à l'ère de la digitalisation tous azimuts sous l'impulsion des gouvernements, et les exigences de services de plus en plus digitaux des usagers et citoyens.

La cybersécurité demeure un défi majeur dans la mise en œuvre de toutes stratégies dans une économie basée sur les données.

Et l'administration ivoirienne ne dispose pas à date d'un Centre d'Opérations de Sécurité (COS) qui, en synergie avec un CERT, joue un rôle central dans la prévention et le traitement des cyberattaques quelle qu'en soit sa forme.

**En conséquence toutes politiques nationales en matière de gouvernance de données** devra intégrer la sécurisation du cyberspace et la confiance numérique dans toutes ses composantes.

## VIII. LA GOUVERNANCE DES DONNÉES AU PLAN NATIONAL

### a. Evaluation de la maturité de la gouvernance des données de quelques structures et instructions

En complément de l'analyse situationnelle et étude diagnostique, la mission a initié une série d'interviews et de rencontres en présentiel et en ligne (Survey) dans le but d'avoir une idée de la maturité en termes de gouvernance des données dans certaines structures aussi bien publiques que privées.

Cinquante-neuf (59) structures publiques et privées ont été contactées, selon la nature des données qu'elles produisent ou utilisent, avec des points de discussions (en présentiel) balayant des aspects aussi divers que le cadre réglementaire, l'accès au haut débit, les infrastructures de données (outils de collecte, production, stockage, analyse, partage), l'interopérabilité et accessibilité, et politique interne de gouvernance des données.

Les résultats attendus ont pour but de calibrer l'analyse situationnelle basée exclusivement sur la revue documentaire et le benchmarking.

### b. La méthodologie

En l'absence d'indicateurs et d'évaluation de références, en termes de maturité de données, et en tenant compte des contraintes de délai, nous avons sur la base d'un modèle de maturité adapté à notre environnement, utilisé une approche mixte, comprenant un **Survey en ligne et des interviews**.

L'objectif étant d'apprécier même ne serait-ce que de façon empirique le niveau de maturité des cibles, et d'estimer le niveau général de maturité dans l'espace public, afin de mieux déterminer les orientations stratégiques.

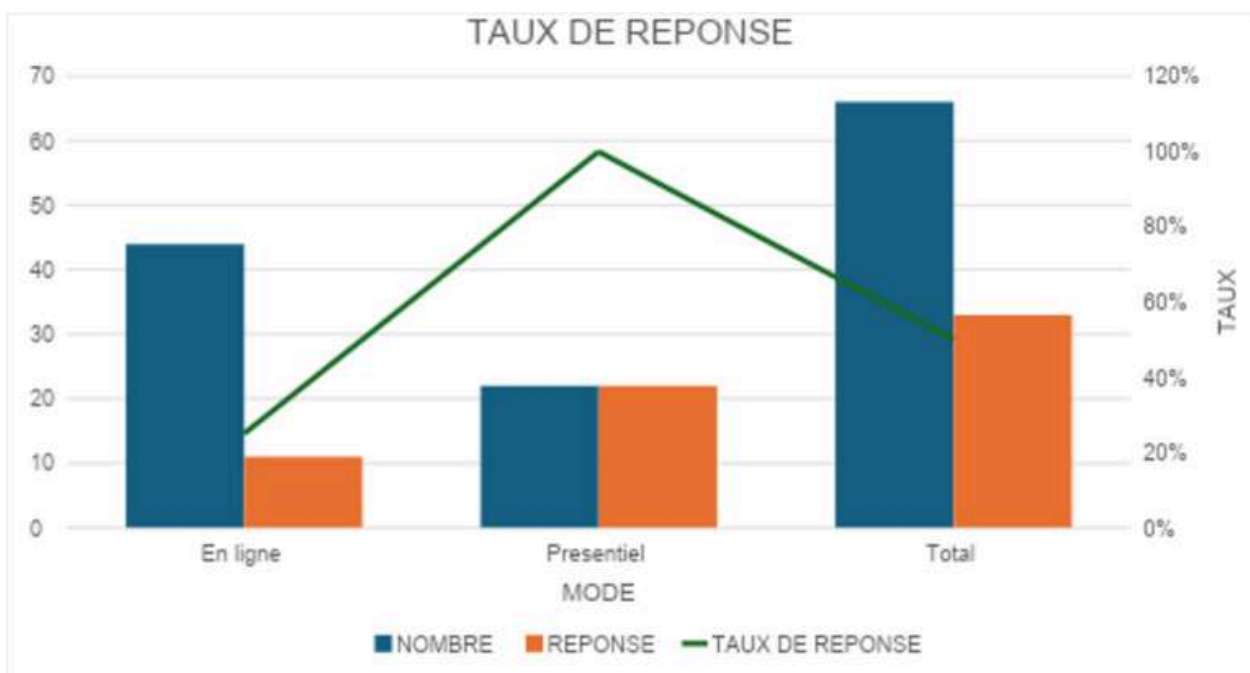
- **Le Survey en ligne** : 33 Cibles choisies sur la base de leur maturité supposée
- **Visites et interviews** : 21 sur 26 structures rencontrées et interviewées.

Le Survey en ligne ainsi que les visites et interviews se sont déroulées entre le 23 octobre et le 11 novembre 2024.

### i. Les interviews en présentiel

Tableau VIII.b.i. LES INTERVIEWS EN PRÉSENTIELS

MODE	NOMBRE	RÉPONSE	TAUX DE RÉPONSE
EN LIGNE	44	11	25%
PRÉSENTIEL	22	22	100%
TOTAL	66	33	50%



- Des interviews post-survey, il ressort que les raisons essentielles expliquant le taux de réponse ou de non-réponse sont entre autres :
- Inaccessibilités récipiendaires (majoritairement dans le public) du fait de connectivité et accès à haut débit
- Problèmes d'adresses email
- Manque de ressource appropriée pour adresser les questions relatives à la maturité des données, Etc.

Le taux de réponse est un indicateur significatif dans l'approche visant à estimer le niveau de maturité

## ii. Le survey en ligne

- **Le Modèle de maturité:**

- Basé sur un questionnaire de 83 questions issues de la combinaison de 10 axes stratégiques abordés sous 6 angles, le questionnaire visait à estimer le niveau de maturité relativement à l'usage, les aspects techniques des données, l'engagement de la haute direction, l'attitude et la responsabilité face aux données, les systèmes et outils ainsi que les compétences.

Tableau VIII.b.iii. La matrice du modèle de maturité

	USAGE	DONNÉES	LEADERSHIP	CULTURE	OUTILS	COMPÉTENCES
	<ul style="list-style-type: none"> <li>• Comment tirer parti des données.</li> <li>• Prendre des décisions, démontrer l'impact, améliorer les services.</li> </ul>	<ul style="list-style-type: none"> <li>• Aspects techniques de la gestion des données.</li> <li>• Actifs, collection, qualité, interopérabilité.</li> </ul>	<ul style="list-style-type: none"> <li>• Engagement avec les données de la haute direction, de la direction stratégique et de la direction commerciale.</li> <li>• Stratégie, responsabilité, surveillance, investissement.</li> </ul>	<ul style="list-style-type: none"> <li>• Attitudes à l'égard des données dans l'ensemble de l'organisation.</li> <li>• Sensibilisation, ouverture, sécurité, responsabilité.</li> </ul>	<ul style="list-style-type: none"> <li>• Systèmes et outils de stockage, de partage et d'utilisation des données.</li> </ul>	<ul style="list-style-type: none"> <li>• La littératie des données et de l'analyse dans l'ensemble de l'organisation.</li> <li>• Offrir des opportunités de développement.</li> </ul>
Axe 1 : Interaction avec les autres						
Axe 2 : Disposer de bonnes compétences et connaissances en matière de données						
Axe 3 : Disposer des bons systèmes et outils						
Axe 4 : Prise de décisions à l'aide de données						
Axe 5 : Connaissance des données à disposition						
Axe 6 : Gestion et utilisation des données de manière éthique						
Axe 7 : Gestion de vos données						
Axe 8 : Définition de l'orientation de vos données (principes, politique, stratégie, etc.)						
Axe 9 : Protection de vos données						
Axe 10 : Responsabilités dans la gestion des données						

### iii. NIVEAUX DE MATURITÉ MESURE : Le niveau de maturité est mesuré sur une échelle de 1 à 5.

#### NIVEAU 1: DÉBUTANT

- Respect des exigences légales minimales. Approche insulaire et travail en silo.
- L'organisation ne considère pas les données comme précieuses pour leurs résultats.
- Absence de responsabilité définie et de surveillance des données.
- Connaissance très limitée des données détenues par l'organisation.
- Littératie des données très limitée.
- Limitations et restrictions par défaut plutôt que par conception.

#### NIVEAU 5: MAÎTRISE

- Vu comme un exemple. Constamment proactif.
- Mise en œuvre à l'échelle de l'organisation.
- Un fort engagement interne et externe.
- Une compréhension claire des besoins et des réponses proportionnées.
- Pérennité et prévision des besoins futurs.
- Capacité large et profonde.

#### NIVEAU 2: ÉMERGENT

- Les données sont utilisées mais ne sont pas prioritaires.
- Les données sont considérées comme une responsabilité informatique ou administrative
- L'utilisation ou l'accès aux données est limité au personnel spécialisé. Manque de sensibilisation à la valeur des données détenues dans l'organisation.
- La propriété et la responsabilité des données ne sont pas bien communiquées.
- Déconnexion entre la direction de l'entreprise et la direction des données.
- L'accent est mis uniquement sur les processus et les résultats les plus importants.

#### NIVEAU 3: APPRENTISSAGE

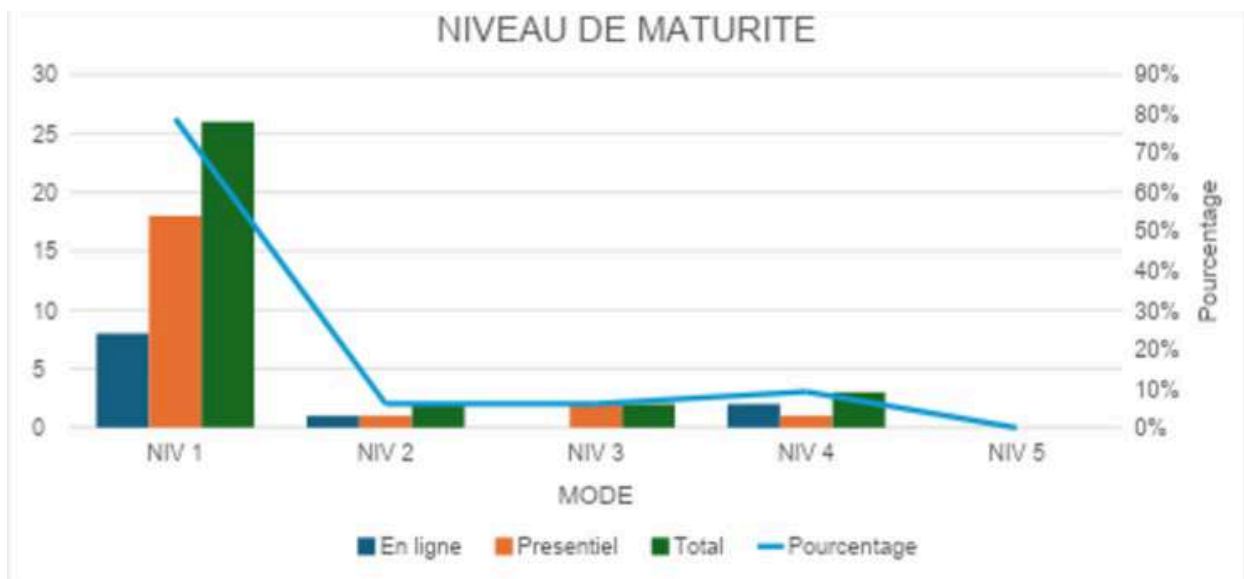
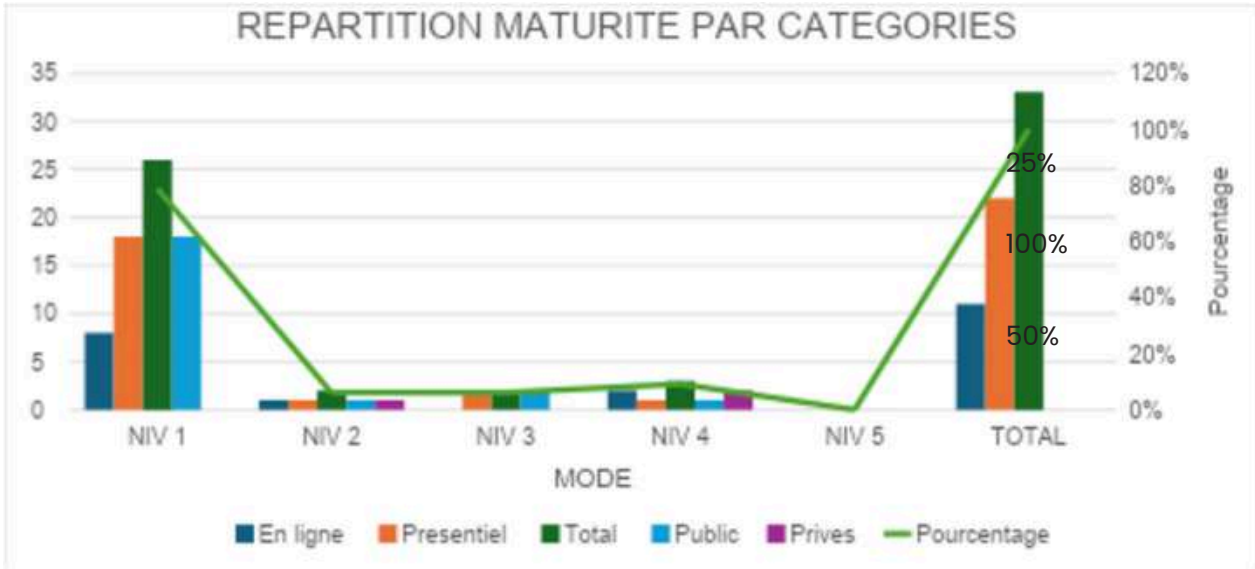
- La littératie des données et de l'analyse est valorisée dans les rôles de leadership. Les exigences juridiques et politiques sont fermement ancrées et largement comprises.
- Les hauts responsables stratégiques sont conscients de l'importance des données. L'engagement du personnel avec les données va au-delà des rôles informatiques ou administratifs.
- Le personnel non expert a besoin de l'aide d'utilisateurs spécialisés pour travailler avec les données.
- Volonté générale et désir d'améliorer la capacité des données.
- Élimination intentionnelle des silos.

#### NIVEAU 4: DÉVELOPPEMENT

- Commencer à intégrer les politiques et les pratiques dans l'ensemble de l'organisation.
- Les utilisateurs de données non experts dépendent peu ou pas du tout de l'assistance d'un spécialiste.
- Des activités de sensibilisation et d'engagement externes.
- Examen régulier des politiques et des pratiques.
- Les données sont toujours considérées comme une priorité.
- Niveaux élevés d'engagement avec les données de tout le personnel.
- Capacités profondes.
- La mise en œuvre des pratiques dans l'ensemble de l'organisation peut être incohérente.

## c. Résultats et constats

### i. Les interviews



## ii. Niveau de maturité évaluée / estimée

Le but de l'évaluation, combinée aux interviews en présentiel, est entre autres d'estimer le niveau de maturité en matière de gouvernance de données sur une échelle de 1 à 5.

## iii. Résultats

Il ressort aussi bien des entretiens physiques que du survey réalisé en ligne, un niveau de maturité estimée proche du niveau 1 pour la majorité des structures de l'État, à l'exception de quelques-unes (Douanes, SNDI, ONECI, données statistiques du CEPICI, etc.) dont les missions découlant de leur objet social, les engagent à un minimum de procédures et d'organisation autour des données dont elles sont en charge.

Ces initiatives sectorielles ne s'inscrivent pas dans une logique ou stratégie de valorisation des données de l'administration.

### NIVEAU 1: DÉBUTANT

- a) Respect des exigences légales minimales.
- b) Approche insulaire et travail en silo.
- c) L'organisation ne considère pas les données comme précieuses pour leurs résultats.
- d) Absence de responsabilité définie et de surveillance des données.
- e) Connaissance très limitée des données détenues par l'organisation.
- f) Littératie des données très limitée.
- g) Limitations et restrictions par défaut plutôt que par conception.

## d. Evaluation des processus en place pour la production

- De l'analyse des sources de production, il ressort que l'essentiel des données actuelles sont produites selon divers processus :
- Résultats d'enquêtes, recensements, études
- Traitement des micro données, de la collecte automatisée de données, des observations, expériences, questionnaires, entretiens personnels (établissements publics, PME, SME, etc.)
- Délibérations et publications gouvernementales
- Sites Web, livres, articles de revues, dossiers internes, articles de recherche, recherches sur Internet ou en bibliothèque
- Transactions numériques électroniques et commerciales.
- La diversité de ces sources et des processus démontre de la nécessité de mettre en place un cadre normatif structuré en vue de valoriser ces mégadonnées.

## **e.Evaluation des processus en place pour la diffusion , la fiabilisation et la disponibilité des données**

La Loi n° 2013-867 du 23 décembre 2013 relative à l'accès à l'information d'intérêt public établit le droit des citoyens d'accéder aux informations détenues par les organismes publics. Elle définit les conditions et les limites de cet accès, tout en précisant les obligations des institutions publiques en matière de diffusion de l'information. En vertu de la Loi d'accès à l'information toute personne physique ou morale a le droit d'accéder, sans discrimination, à des informations d'intérêt public et documents publics détenus par les organismes publics. Les organismes publics sont tenus de diffuser au public les informations et les documents publics qu'ils détiennent. Ils doivent conserver et gérer leurs données. Les documents publics sont communicables, notamment les dossiers, rapports, études, documents d'orientation ou de politiques publiques, comptes rendus, procès-verbaux, statistiques, directives, instructions, circulaires, notes de service, avis, prévisions, décisions et réponses ministérielles qui comportent une interprétation du droit ou une description des procédures administratives.

Nonobstant cette disposition, le constat montre que très peu d'établissements publics sont sensibilisés à l'application de cette loi. De même que les citoyens. De sorte que la CAIDP n'a rendu que très peu de décisions depuis sa création. Il convient également de s'interroger sur les moyens dont disposent les administrations visées par la loi au regard de leurs obligations.

Une adaptation de cette loi au nouveau contexte de la gouvernance des données, accompagnée d'une vulgarisation auprès de l'écosystème devrait contribuer à améliorer l'accessibilité aux informations d'intérêt public.

## f. Tableaux récapitulatifs des principaux constats et pistes de solutions

Tableau VIII.f. CONCLUSIONS : TABLEAU RÉCAPITULATIFS DES PRINCIPAUX CONSTATS ET PISTES DE SOLUTIONS

	PROBLEMES IDENTIFIES	SOLUTIONS	PROJET D'AXES STRATEGIQUES
<b>CONSTATS PRELIMINAIRES</b>			
<b>ACCES AU HAUT DÉBIT</b>	Encore de nombreuses administrations sans connectivité internet haut débit	Infrastructure d'accès	Infrastructure
<b>PRODUCTION DE DONNÉES (DIGITALISATION)</b>	Niveau de digitalisation encore faible	Infrastructure de données	Infrastructure
<b>DISPONIBILITÉ ET PARTAGE</b>	Multitude de datacenter fonctionnant en silos	Interopérabilité	Interopérabilité et accessibilité
<b>CADRE RÉGLEMENTAIRE</b>	Inadaptation et nécessité de création du cadre d'implémentation de la stratégie	Cadre réglementaire	Réformes
<b>ISSU DU SURVEY/ETUDE MATURETE DONNEES</b>			
<b>USAGE</b>	Faible taux d'utilisation des données comme outils d'analyse, de prédiction ou de prise de décision	Sensibilisation	Développement de compétences
	Peu de ressources formées à l'usage	Formation	Développement de compétences
	Fonctionnement en silos/inaccessibilité	Accessibilité	Interopérabilité et accessibilité
<b>DONNÉES</b>	Peu ou pas d'importance accordée	Sensibilisation	Développement de compétences
	Difficultés de Collecte, Stockage, analyse, partage, etc.	Gouvernance des Données	Gouvernance des Données
	Manque de Compétences adéquates	Formation	Développement de compétences
	Absence de cadre Analytique, réutilisation, etc.	Innovation	Innovation

<b>LEADERSHIP</b>	Absence d'engagement au haut niveau de la hiérarchie	Culture	Developpement de competences
	Pas de responsabilité claire	Responsabilisation	Culture
<b>CULTURE</b>	Absence de Compétences adéquates au niveau managérial	Formation	Developpement de competences
	Absence d'engagement au haut niveau de la hiérarchie	Sensibilisation	Culture
	Pas de responsabilité claire	Responsabilisation	Developpement de competences
	Peu d'importance accordée à l'ouverture et au partage de données	Sensibilisation	Culture
	Absence de Compétences adéquates au niveau managérial	Formation	Developpement de competences
<b>OUTILS</b>	Difficultés de Collecte, Stockage, analyse, partage, etc.	Infrastructure	Infrastructure
	Absence de cadre et d'outil de partage et d'interopérabilité	Infrastructures et formation	Développement de competences
<b>COMPÉTENCES</b>	Insuffisance de ressources expertes sur tous les processus de la chaine des valeurs et du cycle de vie des données	Formation	Développement de competences

A ces constats il convient d'ajouter une absence d'harmonisation et de lecture commune des principes directeurs pour la gouvernance des tels que : définitions, classification, catégorisations, etc.

De cette analyse, il ressort les enjeux stratégiques ainsi que les défis importants a relever pour bâtir les fondements solides pour que la Côte d'Ivoire entame sa marche vers une économie basée sur les données, résultante d'un cadre normatif qui stimule la création de valeur autour des données.

## IX. GOUVERNANCE DES DONNÉES AU PLAN RÉGIONAL ET CONTINENTAL

A l'instar des biens et services, la circulation transfrontalière des flux de données conformément aux règles et dispositions sécuritaires, constitue un catalyseur pour le développement du libre commerce, l'innovation et l'inclusion au niveau régional et continental.

Dans le cadre de l'avènement de la ZLECAF, la SNGD 2030 est en parfaite ligne avec les recommandations de l'Union Africaine, entre autres en faisant le choix des principes directeurs ainsi que des cadres réglementaires en vue de stimuler :

- **La coopération pour permettre aux données** de circuler dans le continent tout en préservant les droits de l'homme, la protection des données, la sécurité et le partage équitable des bénéfices ;
- **La coopération pour créer les capacités** nécessaires en matière de données afin de tirer parti des avantages des technologies et des services qui dépendent des données, notamment la capacité de gouverner les données de manière qu'elles profitent aux pays et aux citoyens africains et favorisent le développement ;
- **La promotion de politique transversale** des données et une réglementation souple pour appréhender l'émergence de nouveaux modèles commerciaux dynamiques basés sur les données, qui puissent favoriser le commerce numérique intra-africain et l'entrepreneuriat basé sur les données ;

<sup>5</sup> Cadre stratégique de l'UA en matière de données

<sup>6</sup> Cadre stratégique de l'UA en matière de données

<sup>7</sup> Cadre stratégique de l'UA en matière de données

## X. ENJEUX STRATÉGIQUES

### 1 Contribution au PIB par la consécration des données

actif souverain national à monétiser et qui contribue à la réalisation d'analyses et d'informations qui doivent éclairer les processus de prise de décision, et à la stimulation de l'innovation.

### 2 Accroître la transparence dans la gestion des ressources

et revenus publics du pays, gestion des affaires gouvernementales.

### 3 Stimuler la disponibilité d'informations sur les données

fondées sur l'analyse afin de développer des services adaptés et accessibles en ligne. Soutenir l'innovation dans le développement d'applications et de systèmes, en particulier par les startups.

### 4 Garantir l'ouverture des données et des informations

dérivées stockées au sein des institutions, afin de les rendre accessibles facilement aux communautés de recherche, aux universitaires et à d'autres groupes d'innovation.

### 5 Utiliser de façon innovante le pouvoir des données

dans la prise de décision, la planification, le suivi et l'évaluation du secteur public, afin de créer de la valeur publique en impactant positivement la vie des communautés et les rapports aux citoyens.

### 6 Faciliter les moyens innovants de promouvoir

les avantages publics en utilisant les données de manière nouvelle, ce qui permettrait aux données en Afrique de réaliser la valeur des données.

### 7 Favoriser et faciliter les flux de données transfrontaliers

en augmentant les opportunités commerciales tout en garantissant un niveau adéquat de données personnelles et de vie privée ;

### 8 Consacrer un cyber-espace sécurisé et dynamique

## XI. LES DÉFIS

Au regard des enjeux découlant de l'étude diagnostique, et en tenant compte du niveau de maturité estimé ou présumé dans l'administration publique, de nombreux défis ont été identifiés :

**L'absence d'une vision nationale en matière de données, et pour les données de l'État.**

**La culture et l'éthique** : inculquer une culture des données afin d'engagement l'ensemble des agents publics durablement et de façon responsable dans la construction d'une véritable économie de donnée.

- **Les infrastructures** :

- Finaliser l'interconnexion des administrations, et étendre la connectivité afin d'élargir la base des usagers et accélérer la digitalisation de l'administration publique en vue de la production de données suffisantes pour répondre à la demande.
- Doter les administrations et l'État des infrastructures données aux normes et standards (Serveurs, outils, cloud, plateformes, data center, etc.) en vue d'assurer une bonne gouvernance des données tout le long de leur cycle de vie (production, collecte, stockage, analyse, traitement, partage, etc.), et garantir des données de qualité pour la communauté des entrepreneurs, startups, innovateurs, chercheurs, etc.

**Création de systèmes de données nationaux intégrés et interopérables**

**Gouvernance des données** : adopter les principes et le cadre normatif approprié, en vue de libérer le potentiel des données, et faciliter l'interopérabilité et l'accessibilité

**Innovation** : stimuler un cadre de gouvernance de données qui stimule l'innovation.

**Cybersécurité et la confiance numérique**

**Développement des compétences** : renforcer les capacités des acteurs et des agents publics en vue de soutenir durablement la stratégie

**Partage sécurisé des données et l'amélioration de l'interopérabilité au niveau sous-régional et entre les États**

## XII. RECOMMANDATIONS FINALES

### a. Une vision nationale en matière de gouvernance des données

De l'analyse situationnelle, et des enjeux, mais surtout de son ambition pour une société de connaissance basée sur les données, la Côte d'Ivoire s'est dotée d'une vision nationale pour les données. A savoir :



**« CONSACRER LES DONNÉES COMME UNE RESSOURCE STRATÉGIQUE, ET CRÉER LES CONDITIONS POUR EN LIBÉRER LE POTENTIEL SOCIO-ÉCONOMIQUE, ET EN FAIRE UN CATALYSEUR DE L'INNOVATION EN VUE D'AMÉLIORER LA GOUVERNANCE PUBLIQUE ET D'ACCÉLÉRER LA CROISSANCE INCLUSIVE ET LE DÉVELOPPEMENT DURABLE DE LA CÔTE D'IVOIRE ».**

## **b. Orientations stratégiques**

De l'analyse des défis et en ligne avec la vision nationale, la présente stratégie est bâtie sur six (6) axes stratégiques :

- **La culture et l'éthique**
- **Les infrastructures**
- **L'interopérabilité et l'accessibilité**
- **La Gouvernance des données**
- **L'Innovation**
- **Le Développement des compétences**

---

**DEUXIEME PARTIE :**  
**STRATEGIE NATIONALE DE LA**  
**GOUVERNANCE DES**  
**DONNÉES DE L'ETAT**  
**A L'HORIZON 2030**  
**SNGD – 2030**  
**CÔTE D'IVOIRE**

---



MINISTÈRE DE LA TRANSITION  
NUMÉRIQUE ET DE LA DIGITALISATION

# STRATÉGIE NATIONALE

DE LA GOUVERNANCE DES  
DONNÉES DE L'ÉTAT  
À L'HORIZON 2030

SNGD - 2030 - CÔTE D'IVOIRE

## I. CONTEXTE

Les données sont de plus en plus reconnues comme un atout stratégique, faisant partie intégrante de l'élaboration des politiques, de l'innovation et de la gestion des performances dans les secteurs privé et public, et créant de nouvelles opportunités entrepreneuriales pour les entreprises et les particuliers. Lorsqu'on les applique aux services publics, les technologies peuvent générer des quantités massives de données numériques et contribuer de manière significative au progrès social et à la croissance économique, par la valeur qu'elles peuvent générer du fait d'une gouvernance aux normes et standards qui tiennent compte des spécificités de l'environnement et des priorités des États.

Consciente du rôle central des données et des perspectives politiques stratégiques, et socio-économiques qui en découle, la Côte d'Ivoire s'est engagée à mettre en place la Stratégie Nationale de Gouvernance des Données à l'horizon 2030 (SNGD - 2030), afin de libérer le potentiel socio-économique des données, tout en protégeant efficacement la vie privée, la propriété intellectuelle.

En ligne avec cette volonté politique de consacrer l'importance des données dans la future économie nationale, régionale et mondiale, la Côte d'Ivoire dans la nouvelle stratégie de développement du numérique adoptée par le gouvernement en 2021, a envisagé au nombre des réformes importantes, la mise en place d'une stratégie nationale de gouvernance des données et du Cloud (projet N°45 de la SNNCI).

La présente SNGD - 2030 en matière de données est formulée et mise en place dans le contexte du cadre de gouvernance des données de l'UA, et du renforcement de l'interopérabilité internationale afin de concrétiser la vision partagée et l'approche commune d'un écosystème de données africain intégré au sein de l'UA.

Elle est en parfaite ligne avec le PND 2021-2025, ainsi que la Vision Perspective pour la Côte d'Ivoire qui consacrera le rôle transversal du numérique et de l'innovation comme catalyseur pour accélérer la transformation structurelle et profonde de l'économie nationale dans le PND 2026-2030, et l'atteinte des ODD (Objectifs de Développement Durable " SDGs "

**Afin d'afficher son ambition, les stratégies nationales de la gouvernance des données et du développement de l'IA à l'horizon 2030 doivent prendre une place prépondérante, transversale et visible dans le PND 2026 - 2030.**

---

**UNE VISION  
STRATÉGIQUE EN  
MATIÈRE DE  
GOUVERNANCE  
DES DONNÉES DE  
L'ÉTAT**

---

## II. LA VISION EN MATIÈRE DE GOUVERNANCE DES DONNÉES DE L'ETAT



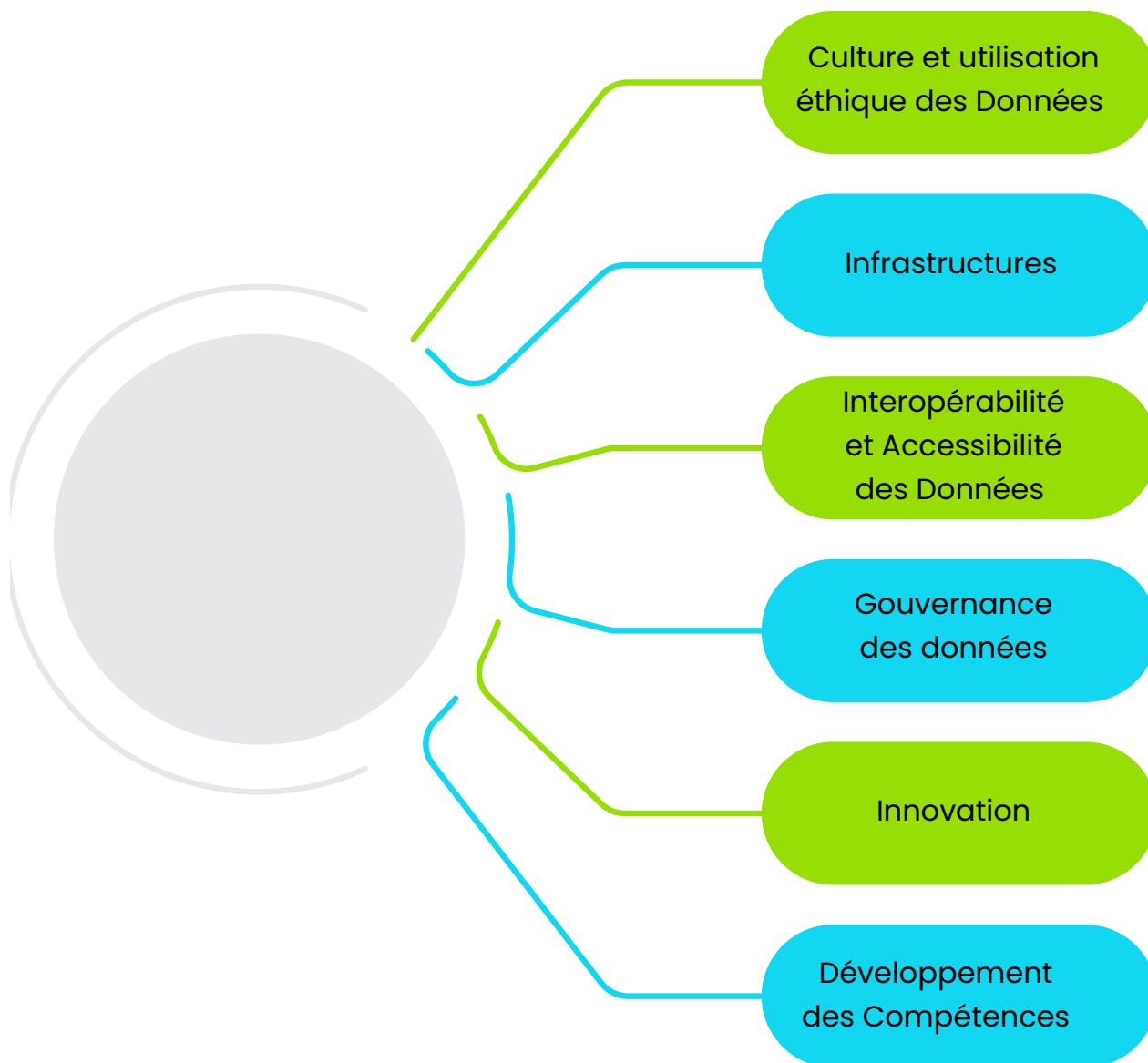
**« EXPLOITER LA VALEUR ET LA CAPACITÉ DES DONNÉES POUR EN FAIRE L'OUTIL PRIVILÉGIÉ DE PRISE DE DÉCISION DE L'ÉTAT, EN VUE EN D'AMÉLIORER LES SERVICES AUX CITOYENS ET USAGERS, ET LE NIVEAU DE MATURITÉ DE GESTION DES DONNÉES DE L'ADMINISTRATION PUBLIQUE À L'HORIZON 2030, EN DÉMEURANT OUVERTE AUX INITIATIVES RÉGIONALES ET INTERNATIONALES SUR LA CIRCULATION DES DONNÉES ».**

Cette vision pour les données de l'État découle de l'état des lieux et des enjeux stratégiques identifiés au niveau national, et est parfaitement en ligne avec la vision nationale sur les données.

La Stratégie nationale de la Gouvernance des Données en Côte d'Ivoire (SNGD -2030), et au regard de ce qui précède, se déclinera autour de six (6) piliers stratégiques.

# LES PILIERS STRATÉGIQUES

### III. LES PILIERS STRATÉGIQUES



---

**OBJECTIFS  
STRATÉGIQUES**

---

## IV. OBJECTIFS STRATÉGIQUES

Les objectifs stratégiques assignés à la SNGD – 2030 sont à la dimension de l'ambition affichée de la Côte d'Ivoire d'être un Hub d'innovation en Afrique, mais aussi d'accélérer son cheminement vers la société de connaissance basée sur les données et au service d'une croissance inclusive et durable pour le bien-être des communautés.

### La Stratégie Nationale de la Gouvernance des Données (SNGD 2030) visera à :

- Établir un cadre institutionnel de gouvernance des données
- Établir des normes et des principes pour la gestion des données en Côte d'Ivoire ;
- Adopter une nomenclature des données à l'échelle nationale qui reflète la réalité ivoirienne et qui est compatibles avec les nomenclatures internationales ;
- Se conformer aux règles régionales ;
- Définir des actions en vue d'opérationnaliser le Référentiel Général d'Interopérabilité définissant une liste de standards et de normes permettant cette interopérabilité ;
- Partage sécurisé des données et l'amélioration de l'interopérabilité au niveau sous-régional et entre les États
- Définir des principes de gouvernance des données et d'un ensemble de bonnes pratiques en termes de contextualisation, journalisation, modélisation ou encore d'auditabilité
- Définir des actions en vue d'opérationnaliser le Cadre Commun d'Architecture des Référentiels de Données permettant de définir l'architecture des solutions de gestion de données de référence, les référentiels de données, qui seront adaptés au contexte de l'administration
- Établir un cadre pour la création, la publication et le cycle d'analyse et de réutilisation des données
- Mettre en place un cadre réglementaire et politique favorable qui facilite l'obtention de données utiles
- Standardiser et simplifier les échanges internes ou externes aux administrations par le cadrage et la formalisation des échanges afin d'assurer leur effectivité, et l'interopérabilité des différentes administrations
- Encourager le partage des données et l'interopérabilité, en vue d'accroître la légitimité et la confiance du public en l'État, pour gérer les données des citoyens de manière responsable
- Instaurer une culture de données à travers toute l'administration publique
- Renforcer et rationaliser le cycle de vie du développement des données
- Stimuler le développement d'innovations basées sur les données pour la création d'emplois dans les domaines public et privé
- Créer des liens clairs avec tous les types de données traitées ainsi qu'une cohérence dans leur terminologie
- Établir un cadre pour développer la capacité des ressources humaines pour le développement de l'industrie des données
- Renforcer les capacités humaines et techniques pour créer de la valeur à partir des données.

---

**LES  
INDICATEURS  
STRATEGIQUES  
DE  
PERFORMANCES  
A L'HORIZON  
2030**

---

## V. LES INDICATEURS STRATEGIQUES DE PERFORMANCES A L'HORIZON 2030

Tableau V. Les indicateurs stratégiques de performances à l'horizon 2030

	INDICATEURS OPÉRATIONNELS	VALEUR DE RÉFÉRENCE	OBJECTIFS POUR 2030
I	<b>CULTURE ET ETHIQUE</b>		
1.	Être n°1 en Afrique au Global Cybersecurity Index	11ème <sup>8</sup>	1er <sup>9</sup>
2.	Être parmi les 20 premiers au niveau mondial au Global Cybersecurity Index	75ème <sup>10</sup>	1 ≤ Rang CI ≤ 20 <sup>11</sup>
II	<b>INFRASTRUCTURES</b>		
	<b>INFRASTRUCTURES D'ACCÈS AU HAUT DÉBIT (CONNECTIVITÉ)</b>		
3	Taux de pénétration du haut débit fixe	4,8% <sup>12</sup>	30% <sup>13</sup>
4	Débit moyen du haut débit fixe	Abidjan et chef-lieu de district	200 Mbps
		Villes	100 Mbps
		Villages	30 Mbps
5	Pourcentage de la population couverte par le mobile 3G	94,62% <sup>15</sup>	100% <sup>16</sup>
6	Pourcentage de la population couverte par le mobile 4G	60% <sup>17</sup>	90%
7	Pourcentage de la population couverte par le mobile 5G	0%	30%
8	Proportion de la population ayant accès à Internet fixe à 5 Mbps ou plus	1,2% <sup>18</sup>	25%
9	Proportion des locaux de service public ayant accès à Internet à 10 Mbps ou plus		100%
10	Ménage disposant d'un accès internet	17% <sup>19</sup>	100%
11	Investissement public dans la digitalisation de l'Etat	3\$/habitant (Afrique) <sup>20</sup>	10\$/habitant <sup>21</sup>
	<b>INFRASTRUCTURES DE DONNÉES (DIGITALISATION, OUTILS ET PLATEFORMES, ETC.)</b>		
12.	Proportion des démarches administratives digitalisées	66 <sup>22</sup> Procédures	100%
13.	Indice de digitalisation (administration)	0,2	0,6

<sup>8</sup> Source : classement ITU, GCI 2020<sup>9</sup> SNNCI 2025<sup>10</sup> Source : classement ITU, GCI 2020<sup>11</sup> SNNCI 2025<sup>12</sup> Source: World bank, ITU, Telegeography, 2020<sup>13</sup> SNNCI-2025<sup>14</sup> Source: Speed Test, 202012<sup>15</sup> Source : ITU, 2021<sup>16</sup> SNNCI 2025<sup>17</sup> Source : ITU, 2021<sup>18</sup> Source : ARTCI<sup>19</sup> Source UIT-2019<sup>20</sup> Source : élément clé de diagnostic secteur économie numérique, Vision CI 2030, Mc Kinsey, février 2019<sup>21</sup> SNNCI 2025<sup>22</sup> Source : rapport SNDI/ANSU, 2020

14.	Indice de Gouvernance Électronique (EGDI)	0.25 < CI < 0.5 <sup>23</sup>	Supérieur à 0,7
15.	Plateformisation des services publics		100%
16.	Serveurs sécurisés par millions d'habitant	3	20
17.	Nombre de Data Centre National installé et aux normes	0	1
18.	Nombre de Cloud National installé et aux normes	0	1
III	<b>INTEROPÉRABILITÉ ET ACCESSIBILITÉ AUX DONNÉES</b>		
19.	Portail unique d'accès au services	0	1
20.	Portail de données ouvertes		25
21.	Nombre de téléchargements d'ensemble de données par an	0	1
22.	Nombre moyen d'appels API par an		
23.	Fréquence moyenne de mise à jour		3 mois
IV	<b>GOVERNANCE DES DONNÉES</b>		
24.	Niveau de maturité en gouvernance des données de l'administration publique	1 (estimé)	4
25.	Nombre de projets créés à partir des données	NC	100/an
26.	Nombre de partenariats pour l'échange de données ou l'harmonisation des cadres réglementaires (CEDEAO, UA...)	NC	5/an
V	<b>INNOVATION</b>		
27.	Indice mondial d'innovation	25,5 <sup>24</sup>	34
VI	<b>DÉVELOPPEMENT DES COMPÉTENCES</b>		
28.	Nombre d'ingénieurs et techniciens spécialisés formés en TIC par an	1 500	Multiplié par 3
29.	Nombre Data steward formé	0	1 000
30.	Nombre de ressources de l'administration formées aux métiers de la gouvernance des données	NC	10 000
31.	Nombre de cadres et dirigeants de l'administration publique formés aux notions de création de la valeur par les données	0	10 000

<sup>23</sup> Source: UNITED NATIONS E-GOVERNMENT SURVEY 2018

<sup>24</sup> Source : GII-2019

---

**PRINCIPES  
DIRECTEURS  
POUR LA  
GESTION ET LA  
GOUVERNANCE  
DES DONNÉES  
DE L'ÉTAT**

---

## VI. PRINCIPES DIRECTEURS POUR LA GESTION ET LA GOUVERNANCE DES DONNÉES DE L'ETAT

Sur la base des bonnes pratiques, mais surtout de l'environnement spécifique de la gouvernance des données, et en ligne avec sa Vision, la Côte d'Ivoire entend s'appuyer sur les principes directeurs suivants :

Tableau VI. Principes directeurs pour la gestion et la gouvernance des données de l'Etat

1	<b>Les données sont un bien, un actif de l'Etat</b> : elles doivent être gérées et valorisées en conséquence.
2	<b>Contrôle et Souveraineté des données</b> : Les données générées en Côte d'Ivoire sont la copropriété de la Côte d'Ivoire quel que soit l'endroit où la société, l'opérateur ou de l'acteur du secteur privé dont les fonds privés ont été utilisés pour les générer. Une copie de ces données sera stockée dans le Cloud national ou le Datacenter National.
3	<b>Localisation des données et transfert transfrontaliers</b> : Toutes les données classifiées ou identifiées comme infrastructures d'information critiques sont traitées et stockées à l'intérieur des frontières de la Côte d'Ivoire par du personnel dont au moins vingt (20%) des effectifs affectés aux tâches de traitement et de stockage de ces données, sont ivoiriens. Le transfert transfrontalier de données ne doit être effectué que dans le respect des politiques et de la législation ivoirienne ou régionale en matière de protection de la vie privée, et conformément aux meilleures pratiques internationales. Une copie de ces données doit être stockée en Côte d'Ivoire à des fins d'application de la loi.
4	<b>Traitement et protection des données</b> : Les données générées par les entités gouvernementales et étatiques et classées non critiques doivent être stockées dans le Data Center ou le Cloud National, conformément aux mesures de sécurité définies et le cadre réglementaire, afin de préserver l'intégrité et la sécurité, et de garantir les droits collectifs sur les données collectives.
5	<b>Format numérique</b> : Toutes les données publiques doivent être saisies par défaut dans un format numérique.
6	<b>Standardisation et interopérabilité</b> : Les données doivent être standardisées, définies sur la base d'un vocabulaire commun, contextualisées, et combinables les unes aux autres.
7	<b>Réutilisation et Accessibilité</b> : Les données doivent être facilement réutilisables, partageables et accessibles à travers les administrations.
8	<b>Open Data</b> : Les données publiques doivent être mises à disposition librement et ouvertement sur internet sur la plateforme d'Open-Data, et mises à jour au moins une fois par trimestre.
9	<b>Classification des données</b> : Chaque structure de l'état doit établir des procédures et des pratiques pour la gestion des actifs informationnels dans ses secteurs d'activité, en parfaite conformité avec le cadre de classification.
10	<b>Niveau de classification</b> : Chaque organisme identifie son patrimoine informationnel et sa sensibilité. Tous les actifs informationnels doivent être classés strictement en fonction de leur niveau de sensibilité.
11	<b>Classification des données gouvernementales</b> : Chaque organisation doit établir un inventaire des données et procéder à des mises à jour annuellement, et doit classer les informations en termes de valeur, d'exigences légales, de sensibilité ou de leur caractère critique. La classification de l'information et les mesures de protection associées tiennent compte des besoins de l'organisation en matière de partage ou de limitation de l'information, ainsi que des exigences légales.

12

**Niveau de sensibilité :****Les niveaux de sensibilité principaux comprennent :**

- **Les données critiques :** Les données critiques sont d'une importance essentielle pour assurer la souveraineté nationale, le fonctionnement de l'État, et la protection des infrastructures vitales. Elles comprennent, entre autres, les informations relatives à la défense et à la sécurité nationale, les informations sur les infrastructures critiques. Ainsi que les Données stratégiques sur les menaces ou les crises nationales (cybersécurité, terrorisme, etc.). Les données critiques requièrent une protection renforcée via des systèmes hautement sécurisés et une limitation stricte d'accès, réservée à des personnels autorisés.
- **Les données sensibles :** Toute information qui, si divulguée, pourrait porter préjudice à des individus, organisations ou institutions.
- **Les données non sensibles :** Les données non sensibles sont considérées n'être ni critiques ni sensibles, peuvent être rendues publiques et réutilisées pour des analyses, des recherches ou le développement d'innovations. Toutes les données non sensibles doivent être publiées à l'état brute sur un portail national de données central ou dans d'autres forums visibles. Les données gouvernementales non sensibles peuvent être stockées dans un cloud public conformément au cadre et à la législation existants en matière de protection et d'accès aux données, afin de permettre un accès universel.

13

**Granularité :** Les données brutes, telles qu'elles sont collectées à la source, seront publiées avec le plus haut niveau de granularité possible, et non sous forme agrégée ou modifiée.

14

**Catégorisation des données :****Les données seront classées en quatre domaines :**

- **Les fichiers de données** seront mis gratuitement à la disposition des utilisateurs sur un portail de données ouvertes ou d'autres forums.
- **Fichiers de données sous licence** nécessitant d'abord une demande de l'utilisateur, mais obtenus gratuitement,
- **Fichiers d'enclave de données dont l'accès** est contrôlé pour fournir un environnement productif de données virtuelles puissant comme des outils analytiques.
- **Fichiers de données payants** nécessitant un paiement de l'utilisateur pour y accéder.

15

**Facilement accessible et utilisable :** Les propriétaires de données doivent les rendre détectables et facilement accessibles afin d'en assurer la disponibilité et l'accessibilité au plus grand nombre d'utilisateurs et à des fins aussi diverses en conformité avec les lois en vigueur.

16

**Exhaustivité et exactitude :** Les données publiées par tous les acteurs clés (publics ou tiers détenteurs de données d'intérêt public) doivent être de haute qualité en termes d'exactitude et d'exhaustivité.

17

**Licence ouverte :** Les données seront publiées dans des formats réutilisables, lisibles par machine et modifiables, afin de permettre une réutilisation gratuite, y compris les aspects commerciaux.

18

**Données et Propriété intellectuelle :** Toute personne utilisant des données reconnaîtra identifiera la source à l'entame du processus de partage et/ou de réutilisation.

19

**Intégrité et justice :** La collecte, le traitement et l'utilisation des données doivent être justes et légaux. Les données ne doivent pas être utilisées pour exercer une discrimination injuste ou porter atteinte aux droits des personnes.

20

**Coopération :** reconnaissant les données comme un apport central de l'économie mondiale et l'importance de l'interopérabilité des systèmes de données pour un marché unique numérique africain dynamique, la Côte d'Ivoire coopère avec les autres états, dans la sous-région, et au niveau continental.

## VII. PLAN D' ACTIONS DÉTAILLÉ DE LA STRATÉGIE NATIONALE DE LA GOUVERNANCE DES DONNÉES PAR AXES STRATÉGIQUES

Tableau VII. Plan d'actions détaillé de la stratégie nationale de la gouvernance des données

AXES STRATEGIQUES	PROJETS Type: R=reforme ; P=projet	RÉSULTATS ATTENDUS	ECHÉANCE	BUDGET (Millions FCFA)	
<b>I. PILIER STRATÉGIQUE 1 : CULTURE ET ETHIQUE</b>					
<b>Objectif spécifique :</b> inculquer une culture des données afin d'engager l'ensemble des agents publics durablement et de façon responsable dans la construction d'une véritable économie de donnée.					
<b>Les réformes relatives à la culture et l'éthique dans la gouvernance des données :</b>					
1	Élaborer des codes d'éthique par tous les groupes de parties prenantes travaillant dans le domaine des données, et spécifiquement les chercheurs, les associations industrielles et les experts en données.	R	Un code d'éthique est mis en place pour chaque partie prenante	2025	200
2	Établir les cadres et lignes directrices sur les limites et les biais des données, les types de technologies, d'algorithmes et de systèmes automatisés utilisés par l'État.	R	Les limites et les biais des données, les types de technologies, d'algorithmes et de systèmes automatisés utilisés par l'État définis par un cadre adopté	2025	200
3	Adapter les organigrammes au sein de la fonction publique avec un leadership et une volonté politique pour s'assurer que les fonctionnaires à tous les niveaux sont équipés d'une compréhension de base de la façon dont les données peuvent être utilisées pour améliorer la prestation de services et la mise en œuvre des politiques.	R	Les responsabilités en matière de gouvernance de données sont identifiées et clairement définies dans l'administration	2026	200

### Les projets relatifs à la culture et à l'éthique dans la gouvernance des données

#### Orientation 1 : Définir le cadre pour une utilisation privilégiée et responsable des données dans l'administration publique

4	Promouvoir une utilisation éthique des données ouvertes par des lignes directrices ou des chartes d'utilisation	P	L'utilisation éthique des données ouvertes est encadrée par des lignes directrices et des chartes	2027	200
5	Promouvoir l'utilisation des données dans chaque organisme d'État et faciliter l'utilisation équitable et fondée sur les données.	P	Les données ouvertes sont utilisées de façon équitable	2026	200
6	Organiser des campagnes de sensibilisation des ressources dirigeantes (Conseils d'administration, Direction Générale, Comité de Direction,) de l'administration publique à l'importance des données comme ressources stratégiques de l'État.	P	La hiérarchie au sein des administrations est sensibilisée à caractère stratégique des données	2026	200
7	Organiser quatre ateliers nationaux par an pour sensibiliser aux enjeux éthiques des données,	P	Les acteurs et l'écosystème est sensibilisé aux enjeux éthiques des données	2030	500
8	Organiser des campagnes nationales de sensibilisation sur l'utilisation éthique des données	P	Les usagers et les citoyens sont sensibilisés à l'utilisation éthique des données	2030	300
9	Elaborer un plan d'action de valorisation au sein de chaque ministère, et Engager les ministères à utiliser les données dans le cadre de priorités politiques	P	Les données sont utilisées dans la définition des politiques	2028	100

<b>10</b>	Doter de compétences techniques, institutionnels et humaines les entités publiques qui conservent divers types de données	P	Les entités publiques conservant les données en ont le pouvoir et les capacités	2027	5,000
<b>11</b>	Instituer une évaluation annuelle ou biannuelle de la maturité de toutes les structures de l'État en matière de gouvernance des données	P	Le niveau de maturité de l'administration en matière de gouvernance des données est établi	2026	200
<b>12</b>	Instituer une évaluation annuelle ou biannuelle de la maturité de toutes les structures de l'État en matière de gouvernance des données	P	La maturité de l'administration publique en matière de gouvernance des données est réalisée de façon régulière	2030	1,500
<b>13</b>	Instituer un mécanisme d'évaluation, de Surveillance et du respect des politiques internes en matière des données, et des procédures afin d'accroître la responsabilité et l'engagement	P	Un mécanisme d'évaluation, de surveillance et de conformité aux règles internes de gestions est mis en place	2029	100

## II. PILIER STRATÉGIQUE 2: INFRASTRUCTURES

**Objectif spécifique :** Finaliser l'interconnexion et la digitalisation de l'administration publique, en vue de la production de données suffisantes pour répondre à la demande, et les doter d'infrastructures de données aux normes et standards (Serveurs, outils, cloud, plateformes, data center, etc.) en vue d'assurer une bonne gouvernance des données le long de leur cycle de vie. Garantir des données de qualité pour la communauté des entrepreneurs, startups, innovateurs, chercheurs, etc.

### Les réformes relatives aux développement des infrastructures

14	Opérationnaliser la Loi d'orientation sur la société d'information (prendre les décrets d'application)	R	Les décrets d'application sont pris	2025	50
15	Adopter et opérationnaliser un cadre normatif pour le précâblage des bâtiments et immeubles en fibre optique pour le très haut débit en Côte d'Ivoire en vue d'accélérer la pénétration du très haut débit	R	Le cadre normatif pour le précâblage des bâtiments et immeubles en FO pour très haut débit est adopté	2025	50
16	Créer une structure publique unique en charge des Infrastructures de l'État (Backbone, satellite, Data Center, Cloud, Plateformes, etc.)	R	Une société publique en charge des infrastructures publiques est créée	2025	50
17	Définir et adopter la structure administrative appropriée pour rendre le Centre National de Calcul accessible à l'écosystème du numérique	R	Le Centre National de Calcul a une existence juridique et un statut qui le rend accessible à la communauté des acteurs de données	2025	50

Les projets relatifs aux infrastructures					
Orientation 1 : l'Accès au haut débit comme un prérequis de la chaîne de valeur de l'économie de données					
18	Poursuivre et étendre la politique de désenclavement par l'extension de la connectivité au haut débit aux zones rurales (ex- PSNDEA)	P	La politique de désenclavement et de desserte des zones rurales en haut débit numérique est poursuivie	2028	40,000
19	Développer des modèles de financement innovants (une combinaison d'obligations de couverture ; d'incitations fiscales ; d'incitations au partage des infrastructures ; de subventions aux investissements, pour stimuler les investissements pour l'extension de la connectivité	P	Les ressources de financement sont mobilisés pour l'extension de la connectivité en zones rurales	2026	
20	Investir dans le Wi-Fi public (10 000 hotspots) et les technologies complémentaires d'accès au haut débit.	P	10 000 hotspots wifi sont opérationnels	2029	10,000
21	Accélérer la mise en œuvre du projet PARAE dans sa composante 2 portant sur les infrastructures numériques de base et e-services d'un financement BAD/KfW/Etat Cote d'Ivoire (111 M euros)	P	Le programme PARAE est exécuté	2026	30,000
22	Étendre les capacités du réseau national de Vsat en vue d'accélérer la pénétration du haut débit en zones rurales	P	Les capacités et ressources techniques du réseau Vsat national sont étendues	2025	6,000
23	Collaborer avec le secteur privé pour accélérer la mise en place de la connectivité et des infrastructures critiques comme la 5G	P	La production et la qualité du réseau d'électricité est améliorée	2029	10,000

24	Adopter des modèles de production d'électricité basé sur les énergies vertes en vue de soutenir les activités de données nationales	P	Des synergies sont créées avec le secteur privé en vue de faciliter et accélérer le déploiement de la 5G	2030	100
<b>Orientation 2 : Assurer la production pour répondre à la demande des données de l'État</b>					
25	Opérationnaliser les piliers stratégiques 1 (développement des infrastructures numériques de la Stratégie nationale du numérique SNNCI 2025 en vue d'accélérer la l'interconnexion et la digitalisation des services publics (détails en annexe 2)	P	Les actions et projets du Pilier développement des infrastructures numériques sont exécutées	2028	250,000
26	Opérationnaliser les piliers stratégiques 2 (Services financiers numériques) de la Stratégie nationale du numérique SNNCI 2025 en vue d'accélérer la digitalisation des services publics (détails en annexe 2)	p	Les actions et projets du Pilier digitalisation des services financiers sont exécutées	2028	100,000
27	Opérationnaliser les piliers stratégiques 3 (Services numériques) de la Stratégie nationale du numérique SNNCI 2025 en vue d'accélérer la digitalisation des services publics (détails en annexe 2)	p	Les actions et projets du Pilier de digitalisation des services publics sont exécutées	2028	15,000
28	Doter toutes les structures de l'administration d'outil de numérisation, de collecte et de stockage sécurisé des données relatives à leur mission	P	Les structures de l'administration sont dotées d'outil de numérisation, de collecte et de stockage sécurisé des données relatives à leur mission	2029	150,000
29	Stimuler la croissance du flux et trafic national de données par l'installation de Points d'Échanges Internet régionaux (Bouaké, San-Pedro, Korhogo)	P	3 Points d'Échange Internet (Civic) sont installés à Bouaké, San-Pedro et Korhogo	2030	5,000

**Orientation 3 : Créer un environnement technique sécurisé pour soutenir la chaîne des valeurs des données de l'État**

<b>30</b>	Réaliser un inventaire et un audit technique détaillée de l'ensemble des Data Center sectoriels de l'Etat	P	Les datacenters publics sont inventoriés et audités	2025	300
<b>31</b>	Créer des standards nationaux pour la collecte, et la structuration des données et labelliser les data centres publics aux normes standards et de durabilité (paramètres de consommation énergétique) pour accélérer l'interopérabilité et l'accessibilité	P	Les datacenters publics audités et validés aux normes et standards sont labellisés	2025	500
<b>32</b>	Equiper les datacenters publics labellisés de sources d'énergies solaires	P	Les sources d'énergie des datacenters publics labellisés sont migrées en énergie renouvelable	2028	2000
<b>33</b>	Accélérer et finaliser le déploiement du Data Centre National	P	Le Data Center National est opérationnel	2026	15,000
<b>34</b>	Doter le Centre National de Calcul de la puissance nécessaire pour devenir le supercalculateur de l'état en vue de soutenir l'économie de données	P	Le Centre National de Calcul est équipé de puissance de calcul suffisant	2026	5,000
<b>35</b>	Réhabiliter les infrastructures hébergeant le Centre National de Calcul	P	Les infrastructures du CNCI sont réhabilitées	2025	3,000

36	Equiper les services publics en infrastructures publiques de Base de données nationales	P	Les administrations publiques sont équipés d'outils adéquats pour la gestion des données sur tout le cycle de vie	2030	10,000
37	Doter l'administration publique de data Warehouse, de Lac de données pour le stockage et faciliter les activités de reporting, d'analyse et d'exploration (data mining) des données publiques	P	Les administrations publiques sont équipées d'outils adéquats pour la gestion des données sur tout le cycle de vie	2030	10,000
38	Mettre en place un Dataspace pour la valorisation des données	P	Un dataspace est mis en place pour la valorisation des données	2030	10,000
39	Mettre en place un centre de données national	P	Un Centre de Données est mis en place et opérationnels		10,000

#### Orientation 4 : Optimiser les ressources d'investissements d'infrastructure de l'État

40	Élaborer un plan directeur pour les plateformes existantes (inventorier et auditer les plateformes existantes)	P	Le plan directeur pour les plateformes publiques existantes est adopté	2025	50
41	Mettre en place d'un Cloud national	P	Le CLOUD National est installé et opérationnel	2027	75,000
42	Mettre en place d'un Data Centre national	P	Le Data Center National est installé et opérationnel	2026	50,000

43	Organiser un cadre bi annuel (business forum, atelier bipartite, etc.) de collaboration avec le secteur privé pour accélérer la mise en place de la connectivité et des infrastructures critiques, les data centers et cloud	P	Le secteur privé est partie prenante de la mise en place des infrastructures critiques de données	2026	250
----	--	---	---	------	-----

### III. PILIER STRATÉGIQUE 3 : INTEROPÉRABILITÉ ET ACCESSIBILITÉ

**Objectif spécifique :** Partage sécurisé des données et l'amélioration de l'interopérabilité au niveau national, sous-régional et entre les États

#### Les réformes relatives à l'interopérabilité et à l'accessibilité

44	Adapter le corpus juridique (Loi d'accès à l'information publique, Loi d'orientation sur la société de l'information,) pour améliorer les conditions d'interopérabilité et d'accès aux données publiques	R	Une étude d'évaluation du corpus juridique relatif à l'interopérabilité et l'accessibilité aux données publiques est réalisée et les adaptations nécessaires réalisées	2026	60
45	Adapter et Opérationnaliser les lois sur le Cadre commun d'urbanisation du système d'information de l'état	R	La loi sur le Cadre commun d'urbanisation du système d'information de l'état est adaptée et les mécanismes d'opérationnalisation mis en place	2026	60
46	Adapter et Opérationnaliser les lois sur le Cadre Commun d'Architecture des Référentiels de Données	R	La loi sur le Cadre Commun d'Architecture des Référentiels de Données	2027	60
47	Adapter et Opérationnaliser les lois sur le Référentiel Général d'Interopérabilité	R	La loi sur le Référentiel Général d'Interopérabilité	2029	60

48	Adopter une politique de plateformes pour l'avènement d'un « Etat plateforme » pour automatiser la production et le partage des informations issues des administrations et collectivités locales (collecte reposant sur des sources de données multiples)	R	Une politique de plateformes est adoptée	2026	60
49	Adopter une politique du Cloud afin de stimuler et faciliter la réutilisation de données	R	Une politique du Cloud est adoptée	2025	60
50	Adopter une base réglementaire et pratique pour soutenir l'initiative Open Gouvernement/Public Data Initiative)	R		2026	

### Les projets relatifs à l'interopérabilité et l'accessibilité

#### Orientation 1 : Optimiser les ressources d'investissement de l'Etat à travers un environnement intégré

51	Développer des tutoriels ou des exemples d'utilisation ou des guides correcte pour accompagner les données ouvertes	P	Les tutoriels et guides pour les données ouvertes sont disponibles	2027	500
52	Inventorier et identifier les actifs de données de grande valeur et critiques en possession de l'Etat	P	La cartographie des actifs de données de grande valeur et critiques est établie	2026	200
53	Réaliser une cartographie détaillée des systèmes et plateformes actuellement utilisés par les administrations publiques.	P	La cartographie des actifs des systèmes et plateformes de l'administration publique est établie	2026	100

54	Réaliser une étude détaillée d'évaluation et d'inventaire des technologies spécifiques utilisées pour l'interopérabilité au sein des différentes administrations (e.g., systèmes de gestion de données, middleware, API existantes).	P	L'étude détaillée d'évaluation et d'inventaire les technologies spécifiques utilisées pour l'interopérabilité au sein des différentes administrations (e.g., systèmes de gestion de données, middleware, API existantes) est réalisée	2025	65
55	Etablir un catalogue centralisé des données disponibles incluant les métadonnées décrivant les sources, contexte, règles d'usages	P	Le catalogue de données est disponible	2026	25
56	<p>Réaliser une étude afin d'identifier et analyser les normes de données adoptées (e.g., formats de données, protocoles de communication, API RESTful vs SOAP)</p> <p>Définir et adopter une démarche API (interface de programmation applicative)</p> <p>Créer des API sécurisées pour permettre le partage automatique de données entre administrations, collectivités et d'autres systèmes</p> <p>Mettre en œuvre d'un cadre de gestion des API</p>	P	Le cadre normatif des données est adopté	2026	400

**Orientation 2 : Rendre accessibles les services de l'Etat aux citoyens et usagers de l'administration publique**

57	Mettre en place une plateforme open data pour chacun des 15 secteurs identifiés prioritaires pour l'économie nationale	P	Chacun des 15 secteurs prioritaires de l'économie nationale dispose d'une plateforme Open Data de données disponibles à travers la plateforme nationale	2030	3,000
58	Mettre en place une plateforme nationale intégrée d'interopérabilité	P	La plateforme intégrée de paiement est opérationnelle	2028	5,000
59	Lancer une plateforme nationale intégrée d'interopérabilité de sites pilotes : ONECI, CEPICI, CNPS, DOUANES, IMPÔTS, CAIDP	P	La plateforme pilote d'interopérabilité est implémentée	2028	10,000
60	Mettre en place une plateforme intégrée de paiement	P	La plateforme intégrée de paiement est opérationnelle	2028	2,500
61	Mettre en place un portail unique des services de l'administration publique qui regroupera tous les services digitaux informationnels et transactionnels offerts par l'administration aux usagers et aux entreprises	P	Le portail unique des services publics est opérationnel	2025	3,000
62	Définir des politiques de gestion des droits d'accès et des rôles pour le contrôle	P	Une politique de gestion des droits d'accès est définie	2026	

<b>63</b>	Créer un répertoire de métadonnées commun	P	Le répertoire commun de métadonnées est créé	2027	60
<b>64</b>	Mettre en place des solutions de collecte automatisée basée sur les technologies avancées (IoT), les flux de données en temps réel et les bases de données	P	Des solutions basées sur l'IA, IIoT sont utilisées pour la collecte automatisée de donnée	2028	3,000
<b>65</b>	Utiliser l'IA pour le traitement des données collectées et générer des rapports, alertes ou prévisions dans le cadre de l'analytique	P	L'IA est utilisée pour le traitement des données et la génération de rapport, alertes et prévisions	2029	10,000
<b>66</b>	Intégrer des mesures de sécurité avancée (chiffrement, authentification à deux facteurs, etc.)	P	Les mesure de chiffrement et d'authentification sont adoptées	2025	200
<b>67</b>	Développer une couche d'interopérabilité entre les plateformes existantes et la plateforme d'identification numérique unique	P	Une couche d'interopérabilité est développé avec les plateformes existantes	2026	1,000
<b>68</b>	Mettre en place un mécanisme d'actualisation continue des standards du référentiel d'interopérabilité afin de garantir la cohérence et la facilité des échanges.	P	Un mécanisme d'actualisation continue des standards du référentiel d'interopérabilité est en place	2030	100
<b>69</b>	Mettre en place un mécanisme d'actualisation continue des règles de conception des services du cadre d'urbanisation des SI	P	Un mécanisme d'actualisation continue des règles de conception des services du cadre d'urbanisation des SI est en place	2029	100

70	Mettre en place un mécanisme de gestion des métadonnées et de normalisation entre les différents acteurs publics.	P	Un mécanisme de gestion des métadonnées et de normalisation est mis en place	2029	100
71	Accélérer et finaliser le projet d'Identité Numérique Unique	P		2027	5,000

#### IV. PILIER STRATÉGIQUE 4 : GOUVERNANCE DES DONNÉES

**Objectif spécifique :** adopter les principes et le cadre normatif approprié, en vue de libérer le potentiel des données, et faciliter l'interopérabilité et l'accessibilité

#### Les réformes relatives à la gouvernance des données

72	Harmoniser les différentes branches du droit, les régimes réglementaires et les organismes de contrôle qui traitent des données ;	R	Les différentes branches du droit, les régimes réglementaires et les organismes de contrôle qui traitent des données sont harmonisés ;	2026	
73	Renforcer le cadre législatif en mettant à jour les lois existantes, notamment la Loi sur les données personnelles et (i) d'y inclure un volet plus conséquent relatif au traitement des données par les ou pour le compte des personnes morales de droit public ou dans le cadre de la fourniture d'un service public	R	Le cadre législatif des DCP est mis à jour	2025	65

<b>74</b>	Opérationnaliser la mise en conformité dans le cadre des Données à Caractère Personnel	R	La conformité selon la loi sur les DCP est opérationnalisée	2025	65
<b>75</b>	Créer une Autorité Administrative Indépendante de Protection des Données à Caractère Personnel, conformément à l'obligation découlant de l'Acte additionnel de la CEDEAO et aux normes internationalement reconnues.	R	Une Autorité Administrative Indépendante de DCP est mis en place	2025	5,000
<b>76</b>	Définir des règles de cybersécurité par une loi dédiée à la cybersécurité et des décrets d'application et autres règlements et normes impératives imposant des mesures de sécurité de l'information en fonction des catégories de données, telles que définies dans la nomenclature	R	Les règles de cybersécurité par une loi dédiée à la cybersécurité et des décrets d'application et autres règlements et normes impératives imposant des mesures de sécurité de l'information en fonction des catégories de données, telles que définies dans la nomenclature sont définies	2027	50
<b>77</b>	Mettre en place un organe de gouvernance des données et de l'Intelligence Artificielle	R	L'Organe national de gouvernance des données et de l'IA est mis en place	2025	
<b>78</b>	Légiférer sur les principes directeurs de la stratégie nationale de gouvernance des données	R	Des textes juridiques et réglementaires affirment les principes directeurs de la SNGD 2030	2025	100

### Les projets relatifs à la gouvernance des données

#### Orientation 1 : Créer de la valeur en libérant le potentiel des données à travers des principes, normes et règles de gouvernance proactives

79	Réaliser une étude des coûts et des bénéfices du cadre juridique actuel pour évaluer son efficacité.	P	Étude est réalisée	2027	30
80	Réaliser une étude d'analyse critique des chevauchements ou des lacunes dans toutes les lois traitant de principes directeurs de la gouvernance des données afin d'identifier des améliorations nécessaires dans le cadre législatif.	P	Étude est réalisée	2026	30
81	Mettre en place un mécanisme et évaluer la conformité des pratiques des administrations publiques avec les principes directeurs.	P	La conformité des pratiques des administrations publiques avec les principes directeurs est évaluée	2026	100
82	Réaliser la classification du patrimoine informationnel de toute l'administration publique selon le niveau sensibilité	P	La classification du patrimoine informationnel de toute l'administration publique selon le niveau sensibilité est réalisée	2026	100
83	Réaliser un audit des actifs informationnels de l'administration publique en conformité avec la cadre de classification	P	L'audit des actifs informationnels de l'administration publique en conformité avec la cadre de classification est réalisé	2026	100

84	Accompagner toutes les structures publiques pour la mise en place de procédures et pratiques de gestion des actifs informationnels en conformité avec le cadre de classification	P	Des procédures et pratiques de gestion des actifs informationnels en conformité avec le cadre de classification est mise en place	2027	350
----	--	---	---	------	-----

### Orientation 2 : Définir un cadre sécurisé pour des données de qualité

85	Opérationnaliser l'Autorité Administrative Indépendante de Protection des Données à Caractère Personnel, conformément à l'obligation découlant de l'Acte additionnel de la CEDEAO et aux normes internationalement reconnues.	P	Les missions de l'AAI des DCP selon les directives de la CEDEAO sont ajustées	2025	5,000
86	Opérationnaliser la mise en place de l'ANSSI	P	L'ANSSI est opérationnelle	2025	3,000
87	Opérationnaliser l'organe de gouvernance des données et de l'Intelligence Artificielle	P	L'Organe national de gouvernance des données et de l'IA est opérationnel	2025	3,000
88	Créer le centre national de supervision de la cybersécurité (SOC)	P	Le SOC est opérationnel	2026	5,000
89	Organiser des campagnes de sensibilisation des citoyens et usagers à la cybersécurité et aux cyber risques et sur les mesures de sécurité dans le cyberspace	P	Les citoyens sont sensibilisés	2029	250

**V. PILIER STRATÉGIQUE 5: INNOVATION**

**Objectif spécifique :** Stimuler le développement de l'innovation basée sur les données pour la création d'emplois dans les domaines public et privé.

**Les réformes relatives à l'innovation**

<b>90</b>	Adopter des réformes juridiques et réglementaires clés pour améliorer les conditions d'accès et stimuler l'utilisation des données	R	Les réformes sont identifiées et réalisées	2027	50
<b>91</b>	Adopter et implémenter un cadre de qualité des données	R	Un cadre de la qualité des données est adopté	2027	50
<b>92</b>	Adapter la loi 2016-555 du 26 juillet 2016 (droit d'auteur et droits voisins) au contexte de la propriété intellectuelle dans une économie de données	R	La loi est adaptée	2026	30
<b>93</b>	Adapter l'Ordonnance 2013-662 du 20 septembre 2013 sur la concurrence au contexte d'une économie par les données	R	La loi est adaptée	2026	30
<b>94</b>	Adapter la loi n°2016-412 du 15 juin 2016 sur la protection des consommateurs au contexte d'une économie par les données	R	La loi est adaptée	2026	30

**Les projets relatifs à l'innovation****Orientation 1 : Faire des données un catalyseur de l'innovation**

<b>95</b>	Doter l'ESATIC, l'INPHB, L'Université virtuelle, les Universités publiques et les Lycée d'excellence d'outils, de moyens et de ressources adéquates afin d'en faire la "base de connaissances" dans laquelle l'économie locale des données peut puiser des connaissances scientifiques et technologiques suffisantes	P	Les établissements et institutions de formation sont équipés	2028	10,000
-----------	--	---	--	------	--------

<b>96</b>	Stimuler l'utilisation de Données dans des secteurs spécifiques pour créer de la valeur publique : Santé, Éducation, Énergie, Infrastructure géospatiale	P	Les données sont appliquées aux secteurs prioritaires	2030	5,000
<b>97</b>	Promouvoir la recherche, le développement et l'innovation dans divers domaines liés aux données, notamment l'analyse des données massives, l'intelligence artificielle, l'informatique quantique et la block-Chain.	P	La recherche, l'innovation sont promues dans les domaines liés à l'analyse des données	2027	200
<b>98</b>	Mettre en place une stratégie nationale pour le développement de l'IA en vue d'accélérer la libération du potentiel socioéconomique des données, et les conditions d'une croissance inclusive	P	La stratégie de développement de l'IA est adoptée	2025	0
<b>99</b>	Instituer un Forum annuel national d'innovation des données afin de sensibiliser les décideurs politiques au potentiel des données en tant que moteur d'une économie et d'une société numériques	P	Un forum annuel est institué	2025	500
<b>100</b>	Mettre en place un programme annuel de prix pour l'innovation liée aux données (par des financements des projets) de startups qui utilisent les données ouvertes pour stimuler l'innovation	P	Un programme annuel de prix pour l'innovation liée aux données (par des financements des projets) de startups utilisant les données ouvertes est mis en place	2030	500

**Orientation 2 : Les Données Outils de prises de décision moteur d'inclusion socio- économique**

<b>101</b>	Doter les structures publiques de moyens et de ressources adéquates pour produire des interprétations rigoureuses des données	P	Les structures sont équipées d'outils performants d'analyse	2029	5,000
<b>102</b>	Doter le pays d'équipements de production et l'utilisation de données géospatiales accessibles en appui à la future agence spatiale en soutien au développement de technologies et applications consommatrices d'informations géographiques/géolocalisation, référencement temps et lieux, etc.	P	Les structures sont équipées d'outils performants d'analyse	2028	5,000

**Orientation 3 : Promouvoir des données de qualité pour un développement durable**

<b>103</b>	Doter les structures publiques de moyens de validation et formalisation de sources faisant autorité	P	Les structures publiques disposent de moyens de validation et de formalisation de source faisant autorité	2026	1,500
<b>104</b>	Doter toutes les institutions d'outils, de capacité et ressources de gestion des métadonnées	P	Les institutions sont équipées	2029	350
<b>105</b>	Valider et exécuter le programme de nettoyage des données	P	Programme de nettoyage de données est en place	2030	50
<b>106</b>	Examiner et maintenir les mesures de qualité des données de façon continue	P	Examen et maintenance de la qualité des données est assurée de façon continue	2030	50
<b>107</b>	Mettre en place des procédures pour assurer la fiabilité et la certification des données diffusées	P	Les procédures de fiabilisation et de certification des données diffusées sont mises en place	2026	250

108	Stimuler et encourager des universités pour des projets en IA et Big Data dans le cadre de la recherche et du développement	P	Des projets de R&D sur l'IA et les Big Data sont développés par les universités nationales	2030	1,000
-----	---	---	--	------	-------

## VI. PILIER STRATÉGIQUE 6: DEVELOPPEMENT DES COMPETENCES

**Objectif spécifique :** Établir un cadre pour développer et renforcer la capacité des ressources humaines et techniques pour soutenir l'industrie des données afin de créer durablement de la valeur à partir des données

109	Créer un corps de Data Stewards en charge de la gouvernance, de l'influence sur les normes et les processus de données au niveau de chaque structure publique	R	Le corps des Datas stewards est créé	2025	
-----	---	---	--------------------------------------	------	--

### Les projets relatifs au développement des compétences

#### Orientation 1 : Doter les responsables d'une culture de données

110	Introduire des curricula de formation basique sur les données dans les établissements de formation des élèves-fonctionnaires (ENA, INFAS, CAFOP, INJS, Centre de Perfectionnement des Cadres de la FP, etc.)	P	Le curricula de formation des élèves fonctionnaires au rôle et à l'importance des données est mis en place	2026	100
111	Renforcer les capacités des équipes dirigeantes de l'administration en interopérabilité et en gestion des données	P	Les équipes dirigeants de l'administration sont formées	2027	1,000

## Orientation 2 : Former des ressources aux métiers des données

<b>112</b>	Former 5 000 data scientistes	P	5000 data scientistes sont formés pour l'écosystème et l'administration publique	2030	7,500
<b>113</b>	Former 5000 data analystes	P	5000 data analystes sont formés pour l'écosystème et l'administration publique	2030	7,500
<b>114</b>	Organiser des ateliers nationaux/régionaux pour accompagner les universités et grandes écoles privées de technologies afin d'aligner les programmes d'enseignement supérieur avec les besoins de l'écosystème et l'économie des données	P	Les programmes d'enseignement supérieur dans les universités et grandes écoles privées de technologies sont alignées avec les besoins de l'écosystème et l'économie des données	2028	1,500
<b>115</b>	Former et responsabiliser 1000 data stewards pour l'administration publique	P	1000 data stewards sont formés	2029	2,000
<b>116</b>	Former et mettre en place des mécanismes de rétention pour 5 000 agents de l'Etat aux métiers de la gouvernance des données	P	500 agents de l'état sont formés	2030	2,500
<b>117</b>	Former et recruter 500 ressources dédiées à l'exploitation et la maintenance des infrastructures de données de l'administration publique	P	500 ressources spécialisées en maintenance des infrastructures de données sont formés	2028	500

<b>118</b>	Former 5000 agents publics à l'utilisation de la plateforme d'interopérabilité	<b>P</b>	5000 agents de l'etat sont formés à l'utilisation des plateformes d'interopérabilité	<b>2030</b>	<b>2,500</b>
<b>119</b>	Former 10 000 élèves -fonctionnaires aux notions de bases des données dans une économie de données (ENA - INFAS - INFS - INJS - CAFOP - CPC, etc.)	<b>P</b>	10 000 élèves -fonctionnaires sont formés	<b>2030</b>	<b>3,500</b>
<b>120</b>	Sensibiliser les citoyens à l'usage et aux avantages de la plateforme d'interopérabilité	<b>P</b>	Les citoyens elecitoyens sont sensibilisés aux avantages de l'interopérabilité	<b>2026</b>	<b>1,000</b>
					<b>912, 490</b>

---

# **CARACTÉRISTIQUES DU BUDGET DE RÉALISATION DE LA STRATÉGIE**

---

## VIII. CARACTÉRISTIQUES DU BUDGET DE RÉALISATION DE LA STRATÉGIE

### a. Résumé du plan d'actions

Le plan d'action de la Stratégie Nationale de Gouvernance des Données de la Côte d'Ivoire à l'horizon 2030 – SNGD + 2030 se décline comme suit :

- Six (6) piliers stratégiques :
  - Culture et Ethique
  - Infrastructure
  - Interopérabilité et accessibilité
  - Gouvernance des données
  - Innovation
  - Développement des compétences
- Vingt (20) principes directeurs
- Quinze (15) orientations stratégiques
- Vingt Sept (27) réformes
- Quatre vingt treize (93) projets
- Budget Total Estimé : 912.490 milliards FCFA sur 5 ans dont 70 % au titre des infrastructures d'accès au haut débit, de digitalisation de l'administration publique.

### b. Financement du budget de la SNGD – 2030 :

En lieu et place du schéma traditionnel de financement Etat-Bailleur, du fait de la nature du secteur à fort potentiel de création de valeur portée par l'innovation, mais également de l'intérêt particulier du privé pour une gouvernance des données de qualité, il convient d'imaginer un mécanisme hybride Etat – Secteur Privé – Bailleurs institutionnels. Le secteur privé doit y prendre toute sa part.

Exemple de participation hybride (la clé de contribution est purement indicative) :

PARTENAIRES	PART (%) DU BUDGET	Estimation en Milliards FCFA
État	10%	91,249
Secteur Privé	25%	273,747
Bailleurs institutionnels	65%	547,494
<b>TOTAL</b>	<b>100%</b>	<b>912.490</b>

## c. L'impact général

L'implémentation effective de la SNGD permettra à la Côte d'Ivoire de réaliser à l'horizon 2030 d'atteindre ses objectifs stratégiques, à savoir :

- Établir un cadre institutionnel de gouvernance des données.
- Établir des normes et des principes pour la gestion des données en Côte d'Ivoire.
- Consacrer les Données comme une ressource stratégique, et créer les conditions pour en libérer le potentiel socio-économique, et en faire un catalyseur de l'innovation en vue d'accélérer la croissance inclusive et le développement durable de la Côte d'Ivoire
- Exploiter la valeur et la capacité des données pour en faire l'outil privilégié de prise de décision de l'Etat, en d'améliorer les services aux citoyens et usagers, et le niveau de maturité de gestion des Données de l'administration publique à l'horizon 2030
- Garantir l'ouverture des données et des informations dérivées stockées au sein des institutions, afin de les rendre accessibles facilement aux communautés de recherche, aux universitaires et à d'autres groupes d'innovation.
- Accroître la transparence dans la gestion des ressources naturelles et revenus publics du pays, gestion des affaires gouvernementales par l'analyse et l'utilisation des données.
- Consacrer un cyber espace sécurisé et dynamique
- Stimuler le développement d'innovations basées sur les données pour la création d'emplois dans les domaines public et privé.
- Créer le cadre pour un développement sécurisé de l'IA en Côte d'Ivoire
- Favoriser et faciliter les flux de données transfrontaliers et en augmentant les opportunités commerciales tout en garantissant un niveau adéquat de données personnelles et de vie privée ;

Et établira la Côte d'Ivoire comme un hub de l'innovation en Afrique.

## IX. GOUVERNANCE ET MISE EN ŒUVRE DE LA STRATÉGIE LA SNGD – 2030

### a. ORGANE DE GOUVERNANCE

Au regard de la volonté politique clairement affichée de donner plus d'impulsion afin de tirer profit du pouvoir et du potentiel des données en tant qu'actif, et de partager et valoriser les données, il convient de proposer un organisme fort disposant des pouvoirs et moyens appropriés pour la conduite de la gouvernance des données et de l'Intelligence Artificielle, qui aura la responsabilité ultime de façon stratégique de :

- **Coordonner les actifs de données du secteur public pour extraire ou exploiter la valeur des données dans le secteur public.**
- **Soutenir le partage de données entre les entités gouvernementales**
- **Stimuler et encourager le développement de l'IA**

Cet organe pourra combiner les aspects gouvernance des Données et Développement de l'Intelligence Artificielle, en dehors du champ de la régulation.

#### i. Ancrage

Pour tenir compte de l'impact socio-économique transversal sur l'économie entière, l'organe sera idéalement rattaché à la Primature ou à défaut, autonome sous la tutelle administrative de la du ministère en charge de l'économie numérique.

#### ii. Attributions

- Coordonner la mise en œuvre de la stratégie de l'État dans le domaine de la donnée.
- Coordonner la mise en œuvre de la stratégie nationale développement de l'intelligence artificielle.
- Accompagner les administrations dans la conception et la mise en œuvre de leurs stratégies d'ouverture et de partage de données.
- Mettre à disposition des plateformes interministérielles comme data.gouv.ci sur lesquelles les administrations devront référencer leurs données pour en favoriser la réutilisation et le partage.
- Promouvoir en partenariat avec le ministère en charge de l'économie numérique, et les ministères sectoriels la dématérialisation des formalités administratives et veiller à la qualité des services numériques proposés au public par les administrations.
- Coordonner, organiser et promouvoir l'action de l'Etat et des organismes placés sous sa tutelle en matière d'inventaire, de gouvernance, de production, de circulation, d'exploitation et d'ouverture des données, et notamment des algorithmes et des codes sources.

- Concourir à la mise en œuvre du service public des données de référence.
- Aider les organismes du secteur public et assurer le point d'information unique pour les accès aux fins de la réutilisation des catégories de données.
- Conduire des projets d'exploitation de données pour renforcer l'efficacité des politiques publiques et améliorer les services rendus aux usagers.
- Administrer le portail unique interministériel destiné à rassembler et à mettre à disposition librement l'ensemble des informations publiques de l'Etat, de ses établissements publics, étendues aux collectivités territoriales et aux personnes de droit public ou de droit privé chargées d'une mission de service public.
- Le Directeur Général de l'Agence exerce la fonction d'Administrateur Général des Données, des algorithmes et des codes source. Il anime le réseau des administrateurs ministériels des données, des algorithmes et des codes source. Il peut être saisi par toute personne morale de droit public de toute question portant sur la circulation ou l'exploitation de ces données.
- Veiller à l'opérationnalisation et l'implémentation effective des principes et règles **selon le décret sur le Cadre commun d'urbanisation du système d'information de l'État** à en préserver la maîtrise, la pérennité et l'indépendance.
- Veiller à l'adaptation et l'opérationnalisation et l'implémentation effective des principes et règles **selon le décret sur le Référentiel Général d'Interopérabilité**.
- Veiller à l'adaptation et l'opérationnalisation et l'implémentation effective des principes et règles **selon le décret sur le Cadre Commun d'Architecture des Référentiels de Données**.
- Organiser et animer la concertation nécessaire à la constitution et à l'évolution des règles et référentiels en matière d'interopérabilité et d'accessibilité, et, en liaison avec l'Agence nationale de la sécurité des systèmes d'information, des règles et référentiels en matière de sécurité.
- Promouvoir l'innovation, l'expérimentation, les méthodes de travail ouvertes, agiles et itératives, ainsi que les synergies avec la société civile pour décloisonner l'administration et favoriser l'adoption des meilleures pratiques.
- Soutenir le développement des compétences de l'Etat et des organismes placés sous sa tutelle dans les métiers de la donnée.
- Conseiller le gouvernement sur la prise en compte des données dans les politiques publiques mises en œuvre par les ministères.

- Piloter en collaboration avec l'organe chargé des infrastructures publiques, de la politique de mutualisation des infrastructures de données de l'Etat.
- Construire, mettre à disposition et opérer des infrastructures et services numériques d'usage partagé, dont la stratégie de résilience et de sécurité est définie conjointement avec l'ANSSI, ainsi que des outils numériques à destination des agents publics.
- Contribuer, en appui de la direction des achats de l'Etat, à l'élaboration des stratégies et politiques interministérielles relatives à l'achat de matériels, de logiciels et des prestations intellectuelles informatiques, d'outils et infrastructures de données.
- Contribuer à la définition des positions ivoiriennes dans les instances internationales et communautaires compétentes en matière de gouvernance des données, et, le cas échéant, participe aux dites instances.

#### **Au niveau des structures de l'administration :**

- Chaque structure et organismes d'État est tenu de mettre en œuvre une gouvernance interne des données en établissant les autorités, les rôles, les structures organisationnelles et les ressources nécessaires pour soutenir la gestion, l'utilisation et la maintenance des données en tant qu'actif stratégique tout au long de leur cycle de vie.
- Chaque structure nommera à minima un Gestionnaire de données : pour agir en tant que couche opérationnelle du programme de gouvernance des données. Le nombre total de gestionnaires de données dépend de la taille de l'agence et de l'écosystème de données. Les structures peuvent choisir de définir des rôles supplémentaires au sein de leur organisation en fonction du volume de données et des domaines de données identifiés dans le plan de gouvernance des données de la structure.

- Avoir l'autorité de position appropriée pour gérer leurs domaines de données.
- Documenter les règles de classification des données, de conformité et les règles commerciales et s'assurer que les règles sont communiquées à toutes les parties prenantes et aux gestionnaires de données dans leur domaine.
- Soumettre un Plan de Gouvernance des Données à l'Administrateur General des Données, contenant a minima :
- Élaboration de procédures, de normes et de documentation technique portant sur la qualité, la gestion, l'utilisation et la réutilisation des données tout au long de leur cycle de vie au sein de l'organisation.

### iii. Financement

En plus du financement institutionnel, le caractère stratégique des données auprès d'acteurs de l'écosystème pourrait offrir des opportunités de financement complémentaire du secteur privé.

## X. SUIVI EVALUATION

Le plan de suivi-évaluation définit comment les résultats, les activités et les ressources allouées à la stratégie seront suivis et évalués et comment l'information générée sera prise en compte et utilisée pour améliorer les performances dans la mise en œuvre.

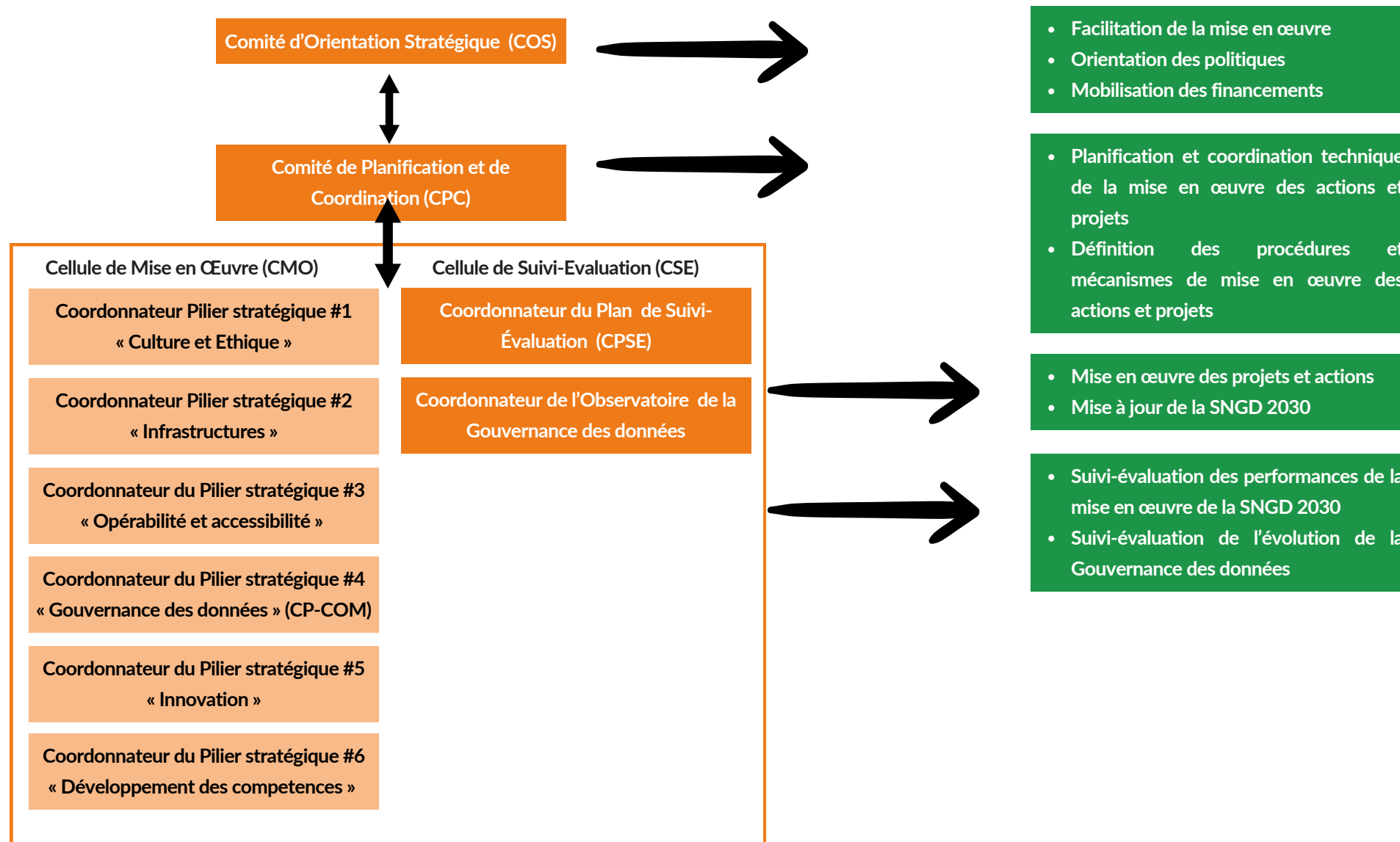
En attendant la mise en place de l'organe de gestion de la gouvernance des données

Le plan de suivi-évaluation proposé devra couvrir :

- le but et la portée du système de suivi et d'évaluation ;
- l'identification des acteurs et définition des rôles ;
- les procédures, les modalités, le circuit et le calendrier de collecte, de traitement, d'analyse et de diffusion des données ;
- les méthodes de vérification et d'analyse des données ;
- les modalités de dissémination et d'utilisation des données et des analyses ;
- les ressources humaines nécessaires ;
- le renforcement des capacités ;
- la définition du budget du suivi et évaluation.

## XI. DISPOSITIF INSTITUTIONNEL DE MISE EN ŒUVRE DE LA SNGD 2030

Tableau XI.1. du DISPOSITIF INSTITUTIONNEL DE MISE EN ŒUVRE DE LA SNGD 2030



## COMPOSITION DES ORGANES DU DISPOSITIF INSTITUTIONNEL ET DÉSIGNATION DES MEMBRES

Tableau XI.2. Composition des organes du dispositif institutionnel et désignation des membres

	Organes	Attributions et responsabilités	Périodicité des réunions	Composition et désignation
1	Comité d'Orientation Stratégique (COS)	<ul style="list-style-type: none"> <li>Facilitation de la mise en œuvre</li> <li>Orientation des politiques</li> <li>Mobilisation des financements</li> </ul>	Trimestrielle	<p>Président : MTND</p> <p>Membres :</p> <ul style="list-style-type: none"> <li>Primature</li> <li>Président du CPC</li> <li>Ministère du plan et du développement</li> <li>Ministère de l'économie et des finances</li> <li>Ministère du budget</li> <li>Ministères des secteurs prioritaires (agriculture, santé, éducation et enseignement supérieur, sécurité, administration, transport, routes)</li> <li>UNETEL</li> <li>GOTIC</li> </ul>
2	Comité de Planification et de Coordination (CPC)	<ul style="list-style-type: none"> <li>Planification et coordination technique de la mise en œuvre des projets et programmes</li> <li>Définition des procédures et mécanismes de mise en œuvre des projets et programmes</li> </ul>	Mensuelle	<p>Président : <b>A designer</b></p> <p>Membres :</p> <ul style="list-style-type: none"> <li>Coordonnateurs CMO</li> <li>Coordonnateurs CSE</li> <li>ARTCI (APD)</li> <li>CAIDP</li> <li><b>A compléter</b></li> </ul>
2.1	Cellule de Mise en Œuvre (CMO)	<ul style="list-style-type: none"> <li>Mise en œuvre des projets et programmes</li> <li>Mise à jour de la SNGD 2030</li> </ul>	Mensuelle	<ul style="list-style-type: none"> <li>Coordonnateurs CMO</li> </ul>

	Organes	Attributions et responsabilités	Périodicité des réunions	Composition et désignation
2.1.1	Coordonnateur du Pilier « Culture et Ethique »	<ul style="list-style-type: none"> <li>Mise en place d'une équipe inclusive pour la mise en œuvre du programme</li> <li>Réalisation des missions de prospective, d'expertise, d'étude et de consultation pour mettre en œuvre le programme</li> </ul>	Autant que nécessaire	A designer
2.1.2	Coordonnateur du Programme « Infrastructures »			A designer
2.1.3	Coordonnateur du Programme « Interopérabilité et Accessibilité »			A designer
2.1.4	Coordonnateur du Programme « Gouvernance des données »			A designer
2.1.5	Coordonnateur du Programme « Innovation »			A designer
2.1.6	Coordonnateur du Programme « Développement des compétences »			A designer
2.2	Cellule de Suivi-Évaluation (CSE)	<ul style="list-style-type: none"> <li>Suivi-évaluation des performances de la mise en œuvre de la SNGD 2030</li> <li>Suivi-évaluation de l'évolution de l'économie numérique</li> </ul>		<ul style="list-style-type: none"> <li>Coordonnateurs CSE</li> </ul>
2.2.1	Coordonnateur du Plan de Suivi-Évaluation (CPSE)	<ul style="list-style-type: none"> <li>Réalisation du plan de suivi-évaluation des performances de la mise en œuvre de la SNGD 2030</li> <li>Elaboration des rapports de suivi-évaluation et proposition de mesures correctives</li> </ul>		<ul style="list-style-type: none"> <li>Direction des Etudes, de la Planification et de la Statistique</li> </ul>



## XII. CHRONOGRAMME DES PROCHAINES ÉTAPES DE LA MISE EN ŒUVRE DE LA SNGD – 2030

Tableau XII. du chronogramme des prochaines étapes de la mise en oeuvre de la SNGD - 2030

	ACTIVITÉS	OBJECTIFS	RESPONSABLES	ÉCHÉANCES
1	Mettre en place les organes et les budgets du pilotage de la SNGD 2030	Mettre en œuvre la SNGD 2030	MTND	1Q2025
2	Faire la cartographie des politiques et réglementations en vigueur et celles devant être adaptées au nouveau cadre de la gouvernance des données	Adapter le cadre réglementaire au contexte de la gouvernance des données	Comité de Planification et de Coordination (CPC)	1Q2025
3	Elaborer le plan de suivi-évaluation de la SNGD 2030	Mettre en place les outils permettant une évaluation systématique et objective des résultats de la SNGD 2030	Coordonnateur du Plan de Suivi-Évaluation (CPSE)	1Q2025
4	Initier la mise en place de l'observatoire de la Gouvernance des données	Identifier et établir les référentiels de mesure de l'impact de la mise en œuvre de SNGD 2030 sur l'innovation, et le développement de l'Intelligence artificielle	Coordonnateur de l'Observatoire de la Gouvernance des données	3Q2025
5	Faire des fiches détaillées pour chaque réforme et projet de la SNGD 2030	Susciter l'intérêt des investisseurs en leur donnant de la visibilité sur le portefeuille de projets de la SNGD	Les coordonnateurs de la Cellule de Mise en Œuvre (CMO)	2Q2025
6	Analyser le portefeuille de projet et actions et adopter la feuille de route de mise en œuvre de SNGD 2030 : classer les projets en fonction de leur priorité, de leur délai de mise en œuvre, les ressources requises (privé, PPP, public), leur importance stratégique, leur impact sur la population	Mobiliser les financements pour la mise en œuvre de la SCIN-2025	Comité de Planification et de Coordination (CPC)	2Q2025

7	Organiser une table ronde des investisseurs et des bailleurs potentiels	Adopter un plan de mobilisation des financements pour la mise en œuvre de la SNGD 2030	Comité d'Orientation Stratégique (COS)	3Q2025
8	Identifier les ressources de financement et mettre en place l'Organe de Gouvernance de Données et de l'IA	Assurer la mise en place effective de l'organe de gouvernance de données	Comité d'Orientation Stratégique (COS)	3Q2025

## XIII. ANNEXES: GLOSSAIRE – DÉFINITIONS

### ANNEXE 1: GLOSSAIRE – DEFINITIONS

- **Disponibilité** : Assurer un accès et une utilisation fiables et en temps opportun de l'information. (Source : Glossaire du NIST)
- **Confidentialité** : Préserver les restrictions autorisées sur l'accès et la divulgation de l'information, y compris les moyens de protéger la vie privée et les renseignements exclusifs. (Source : Glossaire du NIST)
- **Données** : Faits non traités, chiffres bruts, chiffres, images, mots, sons, dérivés d'observations ou de mesures. Les données sont la matière première de l'information. (Source : Politique de gouvernance des données de l'EIS)
- **Information** : Données qui ont été traitées pour ajouter un contexte, une signification et/ou une interprétation. Les ressources informationnelles peuvent être des documents, des rapports, des produits analytiques, des tableaux de bord ou d'autres produits et existent sous forme numérique et analogique.
- **Classification des données** : désigne généralement le processus d'organisation des données par catégories pertinentes afin de pouvoir les utiliser et les protéger plus efficacement.
- **L'infrastructure des données fondamentales** : désigne les technologies avancées qui facilitent l'utilisation intensive de données de qualité. Il peut s'agir de réseaux à large bande, de centres de données et de services en nuage, de matériel et de logiciels électroniques, ainsi que d'applications numériques disponibles sur l'internet.
- **Écosystème de données** : aux fins du présent document, il s'agit non seulement des langages de programmation, des progiciels, des algorithmes, des services informatiques en nuage et de l'infrastructure générale qu'une organisation utilise pour recueillir, stocker, analyser et exploiter des données, mais aussi de la chaîne de valeur sous-jacente associée aux données en tant que facteur de production, de la gouvernance des systèmes de données et de la protection des personnes concernées.
- **Minimisation des données** : désigne un principe des cadres de protection des données qui prévoit la collecte de la quantité minimale des données à caractère personnel nécessaires pour la prestation d'un élément individuel d'un service ou d'un produit.
- **Donnéification** : désigne le processus par lequel les interactions quotidiennes des êtres vivants peuvent être rendues sous forme de données et utilisées à des fins sociales et économiques.
- **L'identité numérique** : désigne un ensemble d'attributs et/ou de renseignements d'identification saisis et stockés électroniquement, qui identifient une personne de manière unique et permettent de distinguer un individu d'un autre.
- **La capacité numérique** : désigne le terme utilisé pour décrire les compétences, l'alphabétisation, les normes sociales et les attitudes dont les individus et les organisations ont besoin pour prospérer, pour vivre, apprendre et travailler dans une société et une économie numérique.
- **Le consentement de la personne** : concernée désigne toute volonté librement exprimée, spécifique, informée et univoque de la personne concernée par laquelle celle-ci, par une déclaration ou par un acte positif clair, manifeste son accord au traitement des données à caractère personnel la concernant.
- **Cybercriminalité** : actes illicites qui portent atteinte à la confidentialité, à l'intégrité, à la disponibilité et à la survie des systèmes de technologies de l'information et de la communication, aux données qu'ils traitent et à l'infrastructure de réseau sous-jacente (Convention de Malabo).
- **La cybersécurité** : désigne l'ensemble des technologies, processus et pratiques conçus pour protéger les réseaux, les dispositifs, les programmes et les données contre les attaques, les préjudices ou les accès non autorisés. (<https://digitalguardian.com/blog/what-cyber-security>).
- **Le responsable du traitement des données** : désigne toute personne physique ou morale, publique ou privée, toute autre organisation ou association qui, seule ou conjointement avec d'autres, décide de collecter et de traiter des données à caractère personnel et en détermine les finalités.
- **La protection des données** : consiste à réglementer la manière dont les données sont utilisées ou traitées et par qui, et à garantir aux citoyens des droits sur leurs données. Elle est particulièrement importante pour garantir la dignité numérique, car elle permet de remédier directement au déséquilibre de pouvoir inhérent entre les « personnes concernées » et les institutions ou les personnes qui ont collecté les données.
- **L'interopérabilité** : désigne la capacité de différentes unités fonctionnelles - par ex., des systèmes, des bases de données, des dispositifs ou des applications - à communiquer, à exécuter des programmes ou à transférer des données d'une manière qui exige que l'utilisateur ait peu ou pas de connaissances de ces unités fonctionnelles (adapté de la norme ISO/CEI 2382 :2015).

- **Commerce électronique** : désigne les transactions commerciales effectuées par des canaux électroniques qui permettent d'acheter et de vendre des biens ou des services via l'internet, ainsi que le transfert d'argent et de données pour réaliser les ventes - par des méthodes spécifiquement conçues pour recevoir ou passer des commandes.
- **Les services en nuage ou Cloud** : sont utilisés à la demande, à tout moment, via n'importe quel réseau d'accès, à l'aide de n'importe quel appareil connecté qui utilise les technologies de l'informatique en nuage, ils utilisent des logiciels et des applications qui se trouvent dans le nuage et non sur les appareils des utilisateurs.
- **Données à caractère personnel** : désigne toute information relative à une personne physique identifiée ou identifiable par laquelle cette personne peut être identifiée, directement ou indirectement notamment par référence à un numéro d'identification ou à plusieurs éléments spécifiques à son identité physique, physiologique, psychique, économique, culturelle ou sociale.
- **Le respect de la vie privée et la sécurité dès la conception** : consistent à intégrer de manière proactive des mécanismes de respect de la vie privée et de sécurité dans la conception et le fonctionnement des produits et services, qu'il s'agisse de systèmes informatiques ou non, d'infrastructures en réseau ou de pratiques commerciales. Cela exige que la gouvernance de la vie privée et de la sécurité soit prise en compte tout au long du processus d'ingénierie et du cycle de vie du produit.
- **Les normes ouvertes** : désignent des normes mises à la disposition du grand public et sont développées (ou approuvées) et maintenues via un processus collaboratif et consensuel. Les normes ouvertes facilitent l'interopérabilité et l'échange de données entre différents produits ou services et sont destinées à être largement adoptées (adopté de l'UIT-T).
- **Données ouvertes** : Ouvert signifie que tout le monde peut librement accéder, utiliser, modifier et partager à toutes fins (sous réserve, tout au plus, d'exigences préservant la provenance et l'ouverture. (<http://opendefinition.org/>)
- **La pseudonymisation** désigne le traitement des données de manière qu'elles ne puissent être associées à un individu sans informations supplémentaires.
- **Data steward** : ou gestionnaire de données surveille la qualité, résoud les problèmes liés aux données et veille au respect des exigences réglementaires. Leur rôle est essentiel pour maintenir l'intégrité et la fiabilité des données d'une organisation.
- **Gouvernance des données** : la spécification des droits de décision et un cadre de redevabilité pour assurer le comportement approprié dans la valorisation, la création, la consommation et le contrôle des données
- **Les données gouvernementales** : sont toutes les informations produites, collectées ou détenues spécifiquement par des entités gouvernementales. Elles incluent à la fois des données accessibles au public et des données restreintes ou confidentielles.

## ANNEXE 2 : DÉTAILS DES PROJETS PILIERS 1,2 ET 3 DE LA STRATÉGIE NATIONALE DU NUMÉRIQUE – SNNCI 2021

#	Projets	Résultats attendus	Durée	Date début	Priorité	Lien PND 21-25	Budget (Millions FCFA)	Financement E= État B = Bailleur	Statut de l'activité
Orientation 1 : Assurer la couverture du territoire en réseaux à haut et très haut débit									
1.	Finaliser le contrat de gestion pour rendre opérationnel les 5 000 km de fibre optique du réseau public large bande (backbone national)	Rentabiliser les investissements publics déjà déployés et contribuer au remboursement des emprunts en cours	6 mois	2021-T3	P1	E1/P2/AN1	100	E= 100 B = 0	Études en cours
2.	Réaliser le Projet Last Miles portant sur le raccordement des Administrations publiques au RNHD sur le territoire national	Assurer la connectivité des administrations publiques au RNHD	48 mois	2022-T2	P1	E1/P2/AN1 / AT3	95 000	E= 10 000 B = 85 000	Non Démarré
3.	Achever le Projet de Réseau National Haut Débit (Backbone) extension de 5 000 à 7 000 km de fibre optique	Achever le réseau dorsal en fibre optique qui contribuera à préparer la Côte d'Ivoire à déployer la technologie 5G sur tout le territoire	24 mois	2023-T1	P2	E1/P2/AN1 / AT1	50 000	E= 0 B = 50 000	Démarré
4.	Réaliser l'extension du Réseau National Haut Débit (Backbone) jusqu'aux sous-préfectures en fibre optique (extension de 7 000 à 13 000 Km)		48 mois	2023-T1	P2	E1/P2/AN1	75 000	E= 5 000 B = 70 000	Études en cours

5	Mettre en place un programme spatial national pour les besoins de services de télécommunications numériques et services d'application à la météorologie, à l'agriculture, à la surveillance de l'environnement, et à la sécurité	Offrir les services spécifiques et diversifier les systèmes de communications pour accroître leur disponibilité, et disposer de technologies alternatives pour assurer l'accès aux services numériques dans les zones difficilement accessibles, l'observation météorologique et la sécurité, et accélérer l'innovation	36 mois	2023-T3	P2	E1/P2/AN1 / AT6	100 000	E= 25 000 B = 75 000	Non Démarré
6	Investir dans la construction d'un point d'atterrissage d'un câble sous-marin	Garantir la souveraineté numérique et promouvoir la concurrence par une diversité des offres	36 mois	2023-T3	P2	E1/P2/AN1 / AT7	20 000	E= 0 B = 20 000	Non Démarré
#	Projets	Résultats attendus	Durée	Date début	Priorité	Lien PND 21-25	Budget (Millions FCFA)	Financement E= État B = Bailleur	Statut de l'activité
Orientation 2 : Promouvoir l'accès à l'Internet à haut et très haut débit									
7.	Étendre la couverture des réseaux de télécommunications dans les localités rurales non desservies	Assurer l'accès des populations rurales aux services numériques pour accroître leur productivité	24 mois	2021-T4	P1	E1/P2/AN1 / AT5	10 000	E= 1 000 B = 9 000	Études en cours

8.	Réaliser le projet de création de points d'accès internet dans 5000 localités	Vulgariser l'usage et l'accès à internet	36 mois	2022-T1	P1	E1/P1/AN2 / AT3	30 000	E= 5 000 B = 25 000	Non Démarré
9.	Réaliser 200 cybers centres communautaires dans les bureaux de poste		36 mois	2022-T1	P2	E1/P1/AN2			Non démarré
10.	Poursuivre la réalisation d'infrastructures (dont le Wi-Fi) et la fourniture d'équipements informatiques dans 12 universités et grandes écoles publiques	Promouvoir l'usage des technologies numériques et d'internet dans l'enseignement supérieur public	12 mois	2022-T1	P1	E1/P1/AN3 / AT4	9 600	E= 600 B = 9 000	Études en cours
11	Assurer la couverture Wifi gratuit du District d'Abidjan et de 10 autres chefs-lieux de districts régionaux	Accélérer la pénétration du haut débit accessible pour tous	36 mois	2022-T2	P2	E1/P2/AN1 / AT7			Non démarré
12	Mettre en œuvre le programme e-Handicap	Accroître l'accès des personnes vulnérables au numérique	36 mois	2023-T2	P2	E1/P1/AN3 / AT4	15 000	E= 3 000 B = 12 000	Non démarré

#	Projets	Résultats attendus	Durée	Date début	Priorité	Lien PND 21-25	Budget (Millions FCFA)	Financement E= État B = Bailleur	Statut de l'activité
<b>Orientation 3 : Renforcer l'infrastructure numérique de l'administration</b>									
13.	Construire un Datacenter de l'État	Sécuriser le stockage et l'archivage des données de l'État	24 mois	2021-T4	P1	E1/P3/AN2 / AT6			Études en cours
14.	Construire de nouveaux Datacenter mutualisés de l'Administration publique	Sécuriser le stockage et l'archivage des données de l'État	24 mois	2021-T4	P1	E1/P3/AN2 / AT6	250 000	E= 50 000 B = 200 000	Études en cours
15.	Mutualiser et optimiser les infrastructures réseaux et services de l'administration	Réduire les coûts et les factures de communication électronique de l'Administration et des services publics	12 mois	2022-T1	P1	E1/P3/AN2 / AT4	25 000	E= 5 000 B = 20 000	Études en cours
16.	Réhabiliter et étendre le Réseau Interne de l'Administration (réseau haut débit)	Améliorer la capacité de la bande passante de l'Administration et l'utilisation de l'intranet gouvernemental	24 mois	2021-T4	P1	E1/P3/AN2			Etudes en cours
17.	Mettre en œuvre le plan national de migration de l'IPv4 vers l'IPv6	Moderniser les réseaux de télécommunication existant de l'Administration pour assurer leur pérennité	12 mois	2022-T1	P1	E1/P3/AN2 / AT11			Études en cours
18.	Mettre en œuvre la feuille de route de lancement de la 5G		12 mois	2022-T1	P1	E1/P3/AN2 / AT9			Études en cours

19.	Promouvoir et vulgariser les cas d'usage de la 5G appliqués aux secteurs prioritaires	Moderniser les réseaux de télécommunications et accélérer le déploiement de la 5G en adéquation avec les objectifs prioritaires de l'état	48 mois	2023 - T2	P1	E1/P3/AN2 / AT5			Non démarré
20.	Construire un système de gestion de continuité des activités de l'État	Garantir la continuité des activités de l'État en cas de sinistre	12 mois	2022-T1	P1	E1/P3/AN2 / AT7	4 500	E= 5 00 B = 4 000	Études en cours
21.	Construire un réseau de télécommunication d'urgence	Maintenir les communications de l'État en cas de sinistre	12 mois	2022-T1	P1	E1/P3/AN2	5 000	E= 1 000 B = 4 000	Études en cours
22.	Construire des stations côtières pour le système mondial de sécurité et de détresse en mer (SMDSM)	Renforcer le système de sécurité et de surveillance des activités en mer	12 mois	2021-T4	P1	E1/P2/AN3 / AT4	11 000	E= 3 000 B = 8 000	Non démarré
23.	Acquérir un système de gestion et de contrôle automatisé du spectre de fréquence (SGCAS)	Contrôler l'utilisation des fréquences qui sont allouées aux usagers afin de prévenir et relever les interférences	12 mois	2022-T3	P1	E1/P2/AN3 / AT1	1 000	E= 0 B = 1 000	Non démarré
24.	Créer 15 stations de contrôle de fréquences en régions et rénover celle d'Abidjan		36 mois	2023-T2	P2	E1/P2/AN3 / AT6	9 500	E= 2 500 B = 7 000	Non démarré
25.	Renforcer les équipements de surveillance du niveau de champs électromagnétique	Contrôler les émissions d'ondes radio pour préserver la santé publique	24 mois	2023-T3	P2	E1/P2/AN3 /	5 000	E= 1 000 B = 4 000	Démarré
26.	Mettre en place un centre régional de tests de conformité et d'interopérabilité	Homologuer les équipements aptes à être connectés au réseau national	36 mois	2023-T1	P2	E1/P2/AN3 / AT5	5 300	E= 1 000 B = 4 300	Non démarré

#	Projets	Résultats attendus	Durée	Date début	Priorité	Lien PND 21-25	Budget (Millions FCFA)	Financement E= État B = Bailleur	Statut de l'activité
<b>Orientation 1 : Renforcer la capacité technique et opérationnelle de l'Administration</b>									
27.	Créer une plateforme mutualisée des paiements électroniques gouvernementaux	Intégrer tous les moyens de paiement électroniques utilisés par les usagers afin de simplifier les procédures et accroître la transparence transactions	24 mois	2022-T1	P1	E1/P3/AN2 / AT8	4 900		Démarré
28.	Construire de nouveaux Datacenter mutualisés de l'Administration publique	Sécuriser le stockage et l'archivage des données de l'État	24 mois	2021-T4	P1	E1/P3/AN2 / AT6	250 000	E= 50 000 B = 200 000	Études en cours
29.	Mutualiser et optimiser les infrastructures réseaux et services de l'administration	Réduire les coûts et les factures de communication électronique de l'Administration et des services publics	12 mois	2022-T1	P1	E1/P3/AN2 / AT4	25 000	E= 5 000 B = 20 000	Études en cours
30.	Réhabiliter et étendre le Réseau Interne de l'Administration (réseau haut débit)	Améliorer la capacité de la bande passante de l'Administration et l'utilisation de l'intranet gouvernemental	24 mois	2021-T4	P1	E1/P3/AN2			Études en cours
31.	Mettre en œuvre le plan national de migration de l'IPv4 vers l'IPv6	Moderniser les réseaux de télécommunication existant de l'Administration pour assurer leur pérennité	12 mois	2022-T1	P1	E1/P3/AN2 / AT11			Études en cours
32.	Mettre en œuvre la feuille de route de lancement de la 5G		12 mois	2022-T1	P1	E1/P3/AN2 / AT9			Études en cours

#	Projets	Résultats attendus	Durée	Date début	Priorité	Lien PND 21-25	Budget (Millions FCFA)	Financement E= État B = Bailleur	Statut de l'activité
<b>Orientation 1 : Renforcer la capacité technique et opérationnelle de l'Administration</b>									
27.	Créer une plateforme mutualisée des paiements électroniques gouvernementaux	Intégrer tous les moyens de paiement électroniques utilisés par les usagers afin de simplifier les procédures et accroître la transparence transactions	24 mois	2022-T1	P1	E1/P3/AN2 / AT8	4 900		Démarré
28.	Construire de nouveaux Datacenter mutualisés de l'Administration publique	Sécuriser le stockage et l'archivage des données de l'État	24 mois	2021-T4	P1	E1/P3/AN2 / AT6	250 000	E= 50 000 B = 200 000	Études en cours
29.	Mutualiser et optimiser les infrastructures réseaux et services de l'administration	Réduire les coûts et les factures de communication électronique de l'Administration et des services publics	12 mois	2022-T1	P1	E1/P3/AN2 / AT4	25 000	E= 5 000 B = 20 000	Études en cours
30.	Réhabiliter et étendre le Réseau Interne de l'Administration (réseau haut débit)	Améliorer la capacité de la bande passante de l'Administration et l'utilisation de l'intranet gouvernemental	24 mois	2021-T4	P1	E1/P3/AN2			Études en cours
31.	Mettre en œuvre le plan national de migration de l'IPv4 vers l'IPv6	Moderniser les réseaux de télécommunication existant de l'Administration pour assurer leur pérennité	12 mois	2022-T1	P1	E1/P3/AN2 / AT11			Études en cours
32.	Mettre en œuvre la feuille de route de lancement de la 5G		12 mois	2022-T1	P1	E1/P3/AN2 / AT9			Études en cours

33.	Mettre en place un système intégré de gestion de données statistiques de l'état (CEPICI, INS, CNPS, INIE, DGE, DGI, DGMP ; chambre de commerce).	Disposer de données statistiques fiables et harmonisées sur les PME, les artisans et les acteurs du secteur informel.	48 mois	2022-T1	P1	E1/P3/AN2			Non démarré
34.	Mettre en œuvre le projet d'appui au renforcement de l'administration électronique (PARAE)	Renforcer les capacités opérationnelles de l'État	24 mois	2022-T1	P1	E1/P3/AN1 /10			Démarré
35.	Créer une plateforme fournissant des informations sur la supervision des activités et la mise en œuvre des réglementations sur les télécommunications et les services financiers numériques	Disposer d'informations d'aide à la décision pour l'élaboration des réglementations ainsi que la planification des infrastructures de télécommunications, des services numériques et des services financiers numériques	12 mois	2022-T2	P1	E1/P3/AN2 / AT10			Non démarré
36.	Attribuer un identifiant unique électronique à toute personne vivant sur le territoire.	1/ Concevoir et mettre en place une administration connectée au service du citoyen et des entreprises 2/ Accélérer la diffusion des services numériques dans les secteurs économiques prioritaires, soutenir l'objectif (iv) du PND 2021-2025, l'innovation et la modernisation conforme à l'ordonnance n°2017-500 du 2 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives	24 mois	2022-T1	P1	E1/P3/AN1 /10			Démarré

#	Projets	Résultats attendus	Durée	Date début	Priorité	Lien PND 21-25	Budget (Millions FCFA)	Financement E= État B = Bailleur	Statut de l'activité
Orientation 2 : Dématérialiser les procédures administratives									
37.	Mettre en place un système d'archivage électronique mutualisé de l'Etat dans tous les ministères	Sécuriser le stockage et l'archivage des documents administratifs pour améliorer la productivité de l'administration	36 mois	2021-T4	P2	E1/P3/AN1 /AT2	5 000		Non démarré
38.	Mettre en place une plateforme des applicatifs gouvernementaux (ONE Gouvernement)		12 mois	2023-T1	P2	E1/P3/AN1 /AT9	1 500		Non démarré
39.	Dématérialiser les procédures administratives (marchés publics, commerce extérieur, justice, relations extérieures ...)	Créer une administration connectée pour faciliter l'obtention de documents administratifs par les citoyens	12 mois	2022-T1	P1	E1/P3/AN1 /AT1	1 563		Non démarré
40.	Digitaliser les bases de données et interconnecter des services de la Police	Contribuer au renforcement de la sécurité intérieure et de l'efficacité des services de police	36 mois	2023-T1	P2	E1/P1/AN3 /AT8			Non Démarré
41.	Digitaliser les services et interconnecter les bases de données des services consulaires représentations diplomatiques et les services de police de l'immigration	Créer une administration connectée et sécuriser et coordonner les actes et services consulaires de la Côte d'Ivoire à travers le monde	36 mois	2022-T3	P2	E1/P1/AN3			Non démarré
42.	Dématérialiser les timbres fiscaux à l'aide de la technologie blockchain	Améliorer la transparence et productivité des services fiscaux	12 mois	2023-T1	P2	E1/P3/AN1 /AT11			Non Démarré

43.	Mettre en place une plateforme digitale du suivi des marchés publiques	Améliorer la compétitive des PME ivoiriennes.	12 mois	2023-T2	P2	E1/P3/AN1			Non démarré
44.	Mettre en place une plateforme digitale de donneur d'ordres fournisseurs		12 mois	2023-T2	P2	E1/P3/AN1			Non démarré
#	Projets	Résultats attendus	Durée	Date début	Priorité	Lien PND 21-25	Budget (Millions FCFA)	Financement E= État B = Bailleur	Statut de l'activité

## Orientation 3 : Accélérer la transformation numérique dans les secteurs prioritaires

45.	Poursuivre le Projet de Solutions Numériques pour le Désenclavement des zones rurales et E-Agriculture(PSNDEA)	Améliorer la productivité des agriculteurs et accroître leur accès aux marchés.	60 mois	T1-2021	P2	E1/P1/AN3 / AT6	45 000		Démarré
46.	Numériser la chaîne de valeur agricole dans certaines filières (ex : cacao, noix de cajou, riz, manioc)	Améliorer les coûts de production, la commercialisation, et la disponibilité des produits de bases	48 mois	2021-T1	P1	E1/P1/AN3			Non démarré
47.	Réaliser une plateforme digitale mutualisée des transactions et créer un espace de marché électronique	Faciliter la vente des produits agricoles	12 mois	2022-T1	P1	E1/P1/AN3 / AT7	5 500		Non démarré
48.	Réaliser la digitalisation des activités du système de santé	Améliorer l'accès aux soins des populations	48 mois	2021-T4	P1	E1/P1/AN3 / AT5	41 000		Non démarré
49.	Mettre en place l'identité numérique (eID) des personnes physiques	Fournir aux citoyens des documents d'identité sécurisés et leur permettre d'effectuer des échanges sécurisés sur internet	48 mois	2021-T4	P1	E1/P3/AN3 / AT11			Non démarré

50.	Créer 3 300 espaces libres-services (bornes) dédiés aux services dématérialisés de l'Etat (200 bureaux de postes / 31 régions)	Vulgariser et rendre accessible les services dématérialisés de l'état aux populations	48 mois	2022-T3	P2	E2/P2/AN2			Non démarré
51.	Développer 100 nouveaux Services Publics Numériques Prioritaires		60 mois	2021-T1	P2	E1/P1/AN2			Démarré
52.	Rendre les plateformes de services numériques accessibles (personnes en situation de handicap)		12 mois	2022-T2	P2	E1/P1/AN1			Non démarré
53.	Améliorer l'accès à l'éducation par le développement des formations à distance	Faciliter l'accès à la formation	48 mois	2021-T1	P1	E1/P1/AN3			Démarré