arpce

AGENCE DE RÉGULATION DES POSTES ET DES COMMUNICATIONS ÉLECTRONIQUES

LIVRE BLANC









IMPORTANCE DES **COMMUNICATIONS ÉLECTRONIQUES** DANS LE DÉVELOPPEMENT DE **L'ÉCONOMIE NUMÉRIQUE**

RÉPUBLIQUE DU CONGO

LIVRE BLANC

IMPORTANCE DES COMMUNICATIONS ÉLECTRONIQUES DANS LE DÉVELOPPEMENT DE L'ÉCONOMIE NUMÉRIQUE

NOTRE VISION

Faire entrer le Congo dans le Top 5 des pays africains leaders des Postes et des Communications Électroniques

® Novembre 2025

TABLE DES **MATIÈRES**

Abréviations 8

Mot du Directeur Général 11

Introduction 13

Résumé exécutif.. 14

I. Télécommunications ou communications électroniques : définition(s) et différence(s) 19

1.1. Définitions de la télécommunication et des communications électroniques 19

1.2. Différence entre les télécommunications et les communications électroniques 20

II. Économie numérique : quelle définition ?. 23

III. Cadre réglementaire et institutionnel... 25

3.1. Réglementation et entités dans le secteur de l'économie numérique 25

3.2. Cadre réglementaire prospectif de l'économie numérique 28

3.3. Matrice des mutations technologiques et réglementaires.. 29

3.4. Positionnement du Congo dans une variante de la matrice ... .32

3.5. Niveau de préparation du Congo à la réglementation du numérique ... .34

3.6. Vers une nouvelle gouvernance : anticiper la régulation du futur 35

IV. Infrastructures énergétiques et résilience numérique 39

4.1. Opérateurs et infrastructures énergétiques 39

4.1.1. Centrales hydroélectriques.. 40

4.1.2. Centrales à gaz 41

4.2. Perspectives de renforcement des infrastructures énergétiques ... .41

4.3. Connexion des sites des opérateurs au réseau électrique : enjeux et disparités 42

4.4. Impacts des coûts de l'énergie dans le secteur des communications électroniques 43

4.4.1. Scénario 1 : Situation de référence (10h E^2C / 14h Diesel) ... .45

4.4.2. Scénario 2 : Mix énergétique du scénario 1 avec hausse du prix du diesel ... .45

4.4.3. Scénario 3 : Transition partielle vers l'électrique (16h E^2C / 8h Diesel) 45

4.4.4. Scénario 4 : Réseau quasi continu (22h E^2C / 2h Diesel) 46

4.4.5. Scénario 5 : Optimisation quasi-maximale (23h E^2C / 1h Diesel) 46

4.4.6. Résumé des scénarios : quelles leçons en tirer ? 46

V. Infrastructures de communications électroniques 49

5.1. Cartographie actuelle des infrastructures de communications électroniques... 49

5.2. Prérequis stratégiques pour les technologies futures de communications électroniques au Congo 50

5.2.1. Expansion et modernisation : une complémentarité indispensable ... .51

5.2.2. Connectivité ultra-rapide et gestion des données : des piliers incontournables 51

5.2.3. Normes et régulation : un enjeu majeur pour les régulateurs.... 52

VI. Technologies de nouvelle génération : quels enjeux pour le Congo ? 57

6.1. Les technologies 5G 57

6.2. Les technologies 6G 58

6.3. Les réseaux non terrestres (NTN) 59

6.4. Quelles bandes de fréquences au Congo pour chaque technologie.... 61

6.5. Déploiements et usages futurs des technologies émergentes. 63

6.6. Déploiement des technologies futures : quelles contraintes pour le Congo ?.... 65

6.7. Gap technologique du Congo dans le déploiement des technologies émergentes... 67

VII. Souveraineté numérique et infrastructures de stockage 73

7.1. Politique de gestion des données : un enjeu de souveraineté numérique.... 73

7.2. Localisation des centres de données 75

7.2.1. Localisation des centres de données de Meta ... .75

7.2.2. Localisation des centres de données de TikTok... 76

7.2.3. Localisation des centres de données de Netflix et Prime Video 76

7.2.4. Localisation des centres de données de Google 77

7.3. Comparaison de quelques modèles de régulation des données. 78

7.3.1. Approche réglementaire 78

7.3.2. Champ d'application 79

7.3.3. Consentement et droits des individus 79

7.3.4. Sanctions.... 79

7.3.5. Rapport de force et souveraineté numérique 81

7.3.6. Principes qui gouvernent la souveraineté numérique.... 81

7.4. Le Congo peut-il prétendre à la souveraineté face aux géants mondiaux de l'économie numérique ? 83

7.5. Données de souveraineté nationale pour le Congo 88

7.6. Limites et leviers de contrôle 89

VIII. Enjeux de cybersécurité. 95

8.1. Importance de la sensibilisation 95

8.2. Importance des équipements et plateformes techniques 97

8.3. Projections sur la maturité du Congo en cybersécurité 99

IX. Identité et culture numériques du Congo 103

9.1. Identité numérique nationale.... 103

9.1.1. Le .cg ou le symbole de la présence du Congo dans l'espace numérique mondial.... 103

9.1.2. Le DNS ou la maîtrise de la sécurité du territoire numérique 103

9.1.3. Les points d'échange Internet du Congo (CGIX) 104

9.1.4. Synthèse sur l'identité numérique nationale... 105

9.2. Identité institutionnelle 105

9.3. Identité numérique individuelle. 107

9.4. Culture numérique et usages 108

X. Inclusion numérique des femmes ? 113

10.1. Couverture réseau : inclusion ou exclusion des femmes ? 113

10.2. Pouvoir d'achat et alphabétisation 113

10.3. Inclusion et promotion des femmes dans le numérique 114

Conclusion 119

Table des illustrations 120

Bibliographie.. 122

ABRÉVIATIONS

1. **ADEN** : Agence de Développement de l'Economie Numérique
2. **ANSSI** : Agence Nationale de Sécurité des Systèmes d'Information
3. **ARPCE** : Agence de Régulation des Postes et des Communications Électroniques
4. **ARPU** : Average Revenue per User (Revenu Moyen par Utilisateur)
5. **AWS** : Amazon Web Services
6. **BEAC** : Banque des États de l'Afrique Centrale
7. **CCPA** : California Consumer Privacy Act (Loi californienne sur la protection de la vie privée des consommateurs)
8. **CEEAC** : Communauté Economique des Etats de l'Afrique Centrale
9. **CEH** : Certified Ethical Hacker (Hacker Ethique Certifié)
10. **CEMAC** : Communauté Economique et Monétaire de l'Afrique Centrale
11. **CERT** : Computer Emergency Response Team (Équipe de réponse aux incidents informatiques)
12. **CGIX** : Points d'échange Internet de Brazzaville et Pointe-Noire
13. **CNPD** : Commission Nationale de Protection des Données
14. **CTI** : Cyber Threat Intelligence (Veille sur les cybermenaces)
15. **DMA** : Digital Markets Act (Règlement sur les marchés numériques)
16. **DNS** : Domain Name System (Système de noms de domaine)
17. **DSA** : Digital Services Act (Règlement sur les services numériques)
18. **DSL** : Data Security Law (Loi sur la sécurité des données)
19. **EDPB** : European Data Protection Bureau
20. **EDR** : Endpoint Detection and Response (Détection et Réponse sur les Terminaux)
21. **EMEA** : Europe, Moyen Orient & Afrique
22. **FAI** : Fournisseur d'accès à Internet
23. **FTP** : File Transfer Protocol (Protocole de transfert de fichiers)
24. **FWA** : Fixed Wireless Access (Accès fixe sans fil)
25. **GE** : Groupe Electrogène
26. **GEO** : Geostationary Earth Orbit (Orbite Géostationnaire)
27. **GSMA** : Global System for Mobile Communications Association
28. **HAPS** : High Altitude Platform Systems (Stations de plateformes à haute altitude)
29. **IA** : Intelligence Artificielle
30. **IAM** : Identity and Access Management (Gestion des Identités et des Accès)
31. **IAPP** : International Association of Privacy Professionals
32. **ICS** : Industrial Control Systems

33. **IMT** : International Mobile Telecommunication
34. **IP** : Internet Protocol (Protocole Internet)
35. **LAN** : Local Area Network (Réseau Local)
36. **LEO** : Low Earth Orbit (orbite basse)
37. **MEO** : Medium Earth Orbit (Orbite Terrestre Moyenne)
38. **MFA** : Multifactor Authentication
39. **ML** : Machine Learning
40. **MW** : Mégawatt
41. **NIU** : Numéro d'Identification Unique
42. **NTN** : Non-Terrestrial Networks (Réseaux Non-Terrestres)
43. **OEM** : Original Equipment Manufacturers (Fabricant d'Équipement d'Origine)
44. **PCA** : Plan de Continuité d'Activité
45. **PIB** : Produit Intérieur Brut
46. **PIPL** : Personal Information Protection Law (Loi sur la protection des informations personnelles)
47. **PND** : Plan National de Développement
48. **PNUD** : Programme des Nations Unies pour le Développement
49. **PPA** : Parité du Pouvoir d'Achat
50. **PRA** : Plan de Reprise d'Activité
51. **RE** : Réseau Electrique
52. **RGPD** : Règlement Général sur la Protection des Données
53. **RNB** : Revenu National Brut
54. **SEC** : Securities and Exchange Commission
55. **SGNIC** : Singapore Network Information Centre
56. **SOC** : Security Operations Center
57. **STEM** : Sciences, Technologies, Ingénierie et Mathématiques
58. **TIC** : Technologies de l'Information et de la Communication
59. **TPE** : Très Petite Entreprise
60. **TPI** : Très Petite Industrie
61. **UE** : Union Européenne
62. **UEAC** : Union des Etats d'Afrique Centrale
63. **UIT** : Union Internationale des Télécommunications
64. **WACS** : West Africa Cable System
65. **XDR** : Extended Detection and Response (Détection et Réponse Étendues)
66. **XR** : Extended Reality (Réalité Etendue)



MOT DU DIRECTEUR GÉNÉRAL



Le numérique ne cesse de prendre une place importante dans la stratégie globale du développement de la République du Congo. Mais il ne peut pleinement jouer ce rôle sans de solides infrastructures de communications électroniques qui soient accessibles à tous.

Le numérique représente donc une opportunité, celle d'accélérer la modernisation des services publics et privés. En même temps, il constitue un défi, celui d'une régulation équilibrée, inclusive et souveraine.

Dans un contexte mondial marqué par la convergence entre télécommunications, énergie, données et souveraineté, le régulateur des postes et des communications électroniques ne doit cesser d'anticiper : anticiper les technologies futures, anticiper les mutations réglementaires et anticiper la gouvernance du futur.

C'est dans cette logique d'anticipation et de construction durable que s'inscrit le présent Livre Blanc qui met en lumière les avancées déjà accomplies, les écarts à combler, ainsi que les leviers à activer pour faire du numérique un pilier de notre développement et de notre souveraineté.

Pour y parvenir, cinq orientations stratégiques englobent notre réflexion :

- Structurer la gouvernance du numérique autour d'un cadre institutionnel intégré, cohérent et prospectif ;
- Renforcer les infrastructures énergétiques et des communications électroniques, dans une logique de complémentarité et de résilience ;
- Garantir, autant que possible, la souveraineté numérique nationale en sécurisant la gestion, le stockage et le traitement des données ;
- Promouvoir l'inclusion et la formation, pour réduire les inégalités, y compris de genre en vue de renforcer l'innovation locale ;
- Anticiper les mutations technologiques grâce à la recherche, à la veille stratégique et à une régulation adaptative.

Ce Livre Blanc constitue, à la fois, un outil d'aide à la décision publique et un cadre d'analyse pour les politiques sectorielles afin de favoriser un espace de dialogue entre pouvoirs publics, opérateurs, chercheurs et citoyens.

C'est donc en unissant les forces des différentes parties prenantes qu'il sera possible de transformer le numérique en un véritable levier de souveraineté, de prospérité et de progrès pour le Congo.

Louis-Marc SAKALA
Directeur Général de L'ARPCE



INTRODUCTION

L'économie numérique s'impose désormais comme un pilier fondamental de la croissance mondiale. Elle redéfinit les modèles économiques, les chaînes de valeur et les modes de gouvernance. Dans ce contexte de mutation rapide, marqué par l'émergence de technologies de rupture telles que la 5G, l'intelligence artificielle ou encore les réseaux non terrestres, les États sont confrontés à un double impératif : anticiper les évolutions technologiques et adapter leurs cadres institutionnels, réglementaires et infrastructurels.

Pour le Congo, la transformation numérique ne se limite pas à une transition technologique puisqu'elle constitue un enjeu de souveraineté, de compétitivité et d'inclusion sociale.

Cependant, l'intégration du pays dans l'économie numérique mondiale nécessite une compréhension fine des dynamiques internationales, mais aussi une évaluation lucide de ses propres capacités : infrastructures énergétiques et télécoms, cadre réglementaire, gestion des données, cybersécurité, identité et culture numériques, préparation du capital humain, etc.

Cet ouvrage dresse un panorama de l'écosystème de l'économie numérique au Congo, en identifiant ses atouts, faiblesses et perspectives de développement à moyen et long terme.

L'analyse met en évidence l'interdépendance entre les innovations technologiques et les besoins de connectivité, tout en soulignant les défis liés à la souveraineté des données, à la cybersécurité et à l'inclusion numérique, entre autres.

Au-delà du diagnostic, ce document vise à proposer quelques orientations stratégiques pour renforcer la résilience du Congo face aux défis du numérique, combler le gap technologique et asseoir une gouvernance proactive et souveraine avec la sécurité du cyberespace congolais comme une absolue nécessité.

En définitive, ce Livre blanc se veut un outil d'aide à la décision et un instrument de prospective au service des pouvoirs publics, des opérateurs économiques, des acteurs du numérique et de la société civile, afin de construire un écosystème numérique congolais fort, sécurisé, inclusif et durable.



RÉSUMÉ EXÉCUTIF

Ce résumé propose, en huit (8) points, une lecture intégrée du secteur des communications électroniques et de l'économie numérique en mettant en perspective les dynamiques technologiques, réglementaires, institutionnelles et sociétales, parmi d'autres.

▶ Un cadre réglementaire et institutionnel qui gagnerait à être consolidé

Le Congo dispose d'un arsenal juridique confortable pour commencer à réguler, autant que possible, les différents contours en lien avec le développement de l'économie numérique. En partant des lois sur les communications électroniques, le secteur postal ou encore sur la cybersécurité, la cybercriminalité, les transactions électroniques et la protection des données à caractère personnel, les efforts consentis par le Congo sont indéniables. En effet, depuis 2009, plus d'une vingtaine **de lois** et **textes d'application** ont été pris dans ce sens.

Cependant, les technologies émergentes, qui se développent à un rythme effréné, nécessitent que le Congo accélère la structuration d'un cadre réglementaire **prospectif**. Cette démarche s'impose afin de mieux anticiper les transformations à venir, telles que celles liées à la 5G, à la 6G et aux réseaux non terrestres (NTN). Les réflexions sur les textes réglementaires relatifs au **métavers,** aux **crypto-monnaies**, à l'**intelligence artificielle (IA)**, à la **réalité étendue** (virtuelle, augmentée et mixte), à l'**Internet des objets (IoT)**, à l'**identité numérique**, aux **plateformes numériques**, aux **neurotechnologies**, etc. devraient déjà se multiplier.

C'est pourquoi le cadre institutionnel de l'économie numérique, en construction, gagnerait également à adopter une approche harmonisée afin de mieux articuler la stratégie nationale du numérique. En d'autres termes, une gouvernance avec des **institutions renforcées** et **mieux coordonnées** devrait participer efficacement à la transformation numérique du Congo.

Pour l'instant, le niveau de préparation du Congo à la transformation numérique, selon un classement de l'UIT, le place dans le carré **G5-Transition** (G5-T). Il doit encore fournir plus d'efforts pour se hisser au niveau du Kenya (G5-Avancé) ou encore de la Corée du Sud (G5-Leader).

▶ Infrastructures énergétiques : un socle à renforcer

L'économie numérique, donc la transformation numérique du Congo, doit pouvoir reposer sur des infrastructures fiables, interconnectées et résilientes. Or, les réseaux énergétiques, quoiqu'en développement, présentent encore des vulnérabilités. C'est pourquoi l'insuffisance, voire l'inexistence de la fourniture électrique dans certaines zones, ainsi que les coûts élevés de l'énergie, constituent des freins à une connectivité et une compétitivité optimales.

Cinq scénarios sont présentés dans cet ouvrage, dont le scénario 2 (qui reflète le plus possible la situation actuelle) et le scénario 5 (qui serait la situation d'optimisation maximale des coûts). Actuellement, la source d'énergie la plus utilisée dans l'alimentation des sites (antennes) des opérateurs demeure le diesel. En effet, le temps moyen de l'alimentation des sites en énergie électrique n'est que de 10h au Congo, contre 23h au Ghana et 24h au Sénégal.

Dans le **scénario 2**, les dépenses énergétiques annuelles combinées des deux principaux opérateurs (MTN et Airtel) et de la société Helios, peuvent être estimées à 7,3 milliards de F CFA hors taxes pour le diesel, et 1,2 milliard pour l'électricité. Mais la facture énergétique globale demeure importante : **8,5 milliards de F CFA HT.**

Dans le **scénario 5**, la facture globale baisserait significativement à **4,9 milliards de F CFA HT**, dont 3,4 milliards pour l'électricité et 1,5 milliard pour le diesel. Cette baisse significative serait rendue possible parce que les groupes électrogènes ne fonctionneraient qu'une heure (1h) par jour, contre 14h dans le scénario 2.

Dans l'éventualité où la puissance électrique installée n'augmenterait pas, et que les infrastructures de transport et de distribution resteraient identiques, de nombreux défis liés aux communications électroniques et à la transformation numérique du pays ne pourront être résolus que par des solutions très onéreuses, comme l'usage de groupes électrogènes.

Or, des infrastructures comme les data centers ou encore certaines technologies émergentes comme la 5G, la 6G, l'IoT, etc. sont énergivores et devraient avoir un impact sur les **coûts des services**, à cause des vulnérabilités décrites.



▶ Infrastructures de communications électroniques : des piliers essentiels

En termes d'infrastructures, le Congo dispose aujourd'hui de deux (2) câbles sous-marins (WACS et 2Africa), de deux (2) stations d'atterrage (Congo Télécom et Airtel Congo), d'un backbone en fibre optique entre Pointe-Noire et Ouesso en passant par Brazzaville, de réseaux de communications électroniques 2G/3G/4G/5G, de liaisons transfrontalières en fibre optique et en faisceaux hertziens, de plusieurs data centers, de deux points d'échange Internet (CGIX), entre autres.

D'un point de vue stratégique, l'expansion et la modernisation de ces infrastructures sont indispensables afin de garantir une connectivité ultra-rapide qui favorisera, parmi d'autres, le transport et la gestion des données. Enfin, la maîtrise des **normes** et de la **régulation du futur** devrait permettre d'encadrer la transformation numérique du Congo afin que sa régulation soit la plus adaptée aux bonnes pratiques internationales, tout en contextualisant certaines approches de solutions locales.

▶ Technologies émergentes : niveau de préparation du Congo

Les normes techniques qui préparent à l'adoption des technologies émergentes sont encadrées par l'Union Internationale des Télécommunications (UIT). Pour le Congo, le passage à la 5G, et plus tard à la 6G, représente une opportunité de modernisation du tissu économique et administratif. Ces technologies terrestres commencent, néanmoins, à subir la concurrence des technologies satellitaires (GEO, MEO, LEO, HAPS).

Par rapport à certains pays du monde, le lancement de la 5G au Congo accuse cinq années de retard. Ce gap risque de s'accentuer au point où le Congo pourrait, par exemple, lancer la **6G avancée** en **2040**, alors que son lancement mondial est prévu vers 2030. Pourtant, les bandes de fréquences nécessaires au fonctionnement des technologies émergentes terrestres et satellitaires sont déjà assignées au Congo.

Le retard pourrait être dû, à minima, aux différentes contraintes **économiques** (taille du marché, pouvoir d'achat, etc.), **énergétiques** (fourniture ininterrompue de l'électricité …), en **capital humain** (personnel technique peu ou pas formé aux technologies du futur) et **technologiques** (exigences de latence et de bande passante des applications émergentes …).

▶ Gestion des données, souveraineté numérique et infrastructures de stockage

Le développement actuel des technologies émergentes a permis à certaines entreprises comme Meta, TikTok, Netflix, Prime Video et Google de devenir des acteurs mondiaux du numérique. Leurs politiques de gestion des données ont en commun, la collecte, le profilage, le partage des données avec des prestataires, ainsi que le stockage et transfert des données à l'international.

Le Congo n'échappe donc pas aux problématiques liées à la gestion des données imposées par les géants du numérique. L'impact économique attribué à Google grâce à ses différents outils reste très limité. Il est estimé à environ **48 milliards de F CFA**. Le Congo, pris isolément, ne saurait exercer un contre-pouvoir économique sur Google. Le rapport de force est, en effet, largement asymétrique. L'Union Européenne, en revanche, montre qu'il est possible de faire face aux géants du numérique en imposant et en faisant appliquer de lourdes sanctions.

Il existe, toutefois, des données qui permettraient de constituer un levier de contrôle stratégique. Comme tout pays, le Congo dispose de données critiques (défense…), stratégiques (santé publique …) et fondamentales (statistiques nationales …) qu'il doit identifier et protéger. D'où l'importance des data centers pour l'hébergement en local desdites données.

▶ Enjeux de cybersécurité

Qu'est-ce donc la souveraineté numérique, quand elle peut s'appliquer, en l'absence de cybersécurité ? Sur ce plan, le niveau de maturité du Congo a été évalué par l'UIT. Il se trouve en **Tier 4** ; ce qui équivaut à une note de 45/100, là où le Ghana a une note supérieure à 90/100. La note du Congo traduit surtout de grosses faiblesses en termes de compétences et d'infrastructures techniques. Toutefois, des projections montrent que le Congo pourrait rattraper un pays comme le Ghana d'ici 2035 si la politique nationale de cybersécurité peut être renforcée pour garantir une protection du cyberespace congolais qui soit la plus optimale possible.

▶ Identité numérique : une importance relative au Congo

Protéger le cyberespace congolais signifie également protéger son identité numérique, incarnée par le domaine de premier niveau « .cg ». Ce domaine national permet d'identifier les sites web et les services en ligne comme appartenant à l'espace numérique congolais. Dans ce contexte, les noms de domaine et, plus encore, l'infrastructure DNS qui les soutient jouent un rôle crucial. Le contrôle du domaine .cg et de ses services DNS constitue un élément clé de l'indépendance et de la souveraineté numériques, puisqu'il régit l'accès aux ressources Internet locales ainsi que leur gestion.

Contrairement aux pays de population équivalente comme le Danemark ou Singapour qui ont respectivement 1,3 million et 200 000 noms de domaine enregistrés, le Congo n'en compte que **3 500** à la date de rédaction de ce Livre Blanc. L'économie congolaise, on peut le constater, est encore loin d'avoir atteint une maturité numérique.

Le Numéro d'Identification Unique (NIU), par exemple, pourrait contribuer à accélérer cette maturité parce qu'il devrait relier chaque entité (physique ou morale) aux différents services numériques tels qu'administratifs, sociaux, de santé, économiques, scolaires, d'état civil, etc. ; ce qui obligerait à la création davantage de noms de domaine.

Parce que le .cg représente l'identité numérique du Congo, les data centers assurent l'hébergement des données en local, lesquelles doivent être sécurisées par une politique et des infrastructures/outils de cybersécurité (CERT/SOC) endogènes.

▶ Les aspects de genre dans le numérique au Congo

La transformation numérique ne saurait se concevoir sans une inclusion globale de la population. La répartition par genre de la population congolaise montre une légère majorité féminine (50,3 %). Cependant, on constate de nombreuses inégalités. En effet, elles ne seraient que 75,3 % à avoir accès à l'éducation contre 85,9 % chez les hommes ; 80 % à disposer d'un téléphone contre 84 % chez les hommes ou encore 32,5 % à avoir un compte mobile money contre 41,2 % chez les hommes. Enfin, en termes de **pouvoir d'achat annuel**, les femmes percevraient environ 2,3 millions de F CFA contre 4,2 millions de F CFA pour les hommes.

Une des solutions possibles pour combler ce déficit consisterait à identifier et à valoriser des modèles féminins de réussite de sorte que plus de femmes s'engagent dans les métiers du numérique ; ce qui suppose aussi qu'elles soient plus présentes dans les filières scientifiques et technologiques. Mais elles devraient aussi être plus nombreuses à intégrer les cercles de décisions politiques et économiques.



TÉLÉCOMMUNICATIONS OU COMMUNICATIONS ÉLECTRONIQUES : **DÉFINITION(S) ET DIFFÉRENCE(S)**

1.1. Définitions de la télécommunication et des communications électroniques

Les infrastructures de télécommunications sont au cœur de l'économie numérique. Avec l'évolution des technologies, le terme *télécommunication* a été remplacé, dans certaines législations, par celui de *communication électronique*.

Conformément au *Règlement des Télécommunications Internationales* publié par l'Union Internationale des Télécommunications (UIT), la télécommunication est définie comme :

> *Toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature, par fil, radioélectricité, optique ou autres systèmes électromagnétiques*[1].

Au sein de la Communauté Économique et Monétaire de l'Afrique Centrale (CEMAC), le *Règlement n°21/08-UEAC-133-CM-18 du 19 décembre 2008 relatif à l'harmonisation des réglementations et des politiques de régulation des communications électroniques* a substitué les *communications électroniques* à la *télécommunication*. La CEMAC définit les communications électroniques comme suit :

> *Émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électronique.*

La loi n° 9-2009 du 25 novembre 2009 portant réglementation du secteur des communications électroniques, en République du Congo, en phase avec la réglementation de la CEMAC, définit les *communications électroniques* comme :

> *La transmission, l'émission ou la réception de signes, de signaux, d'écrits, d'images ou de sons ou des renseignements de toute nature par câble, radio, systèmes optiques ou autres systèmes électromagnétiques, que ces signes, signaux, écrits, images, sons ou renseignements aient ou non fait l'objet de réarrangement, calcul ou autres processus de toute sorte, au cours de leur transmission, émission ou réception.*

Les termes « télécommunication » et « communication électronique » peuvent-ils être utilisés de façon interchangeable ou bien existe-t-il des nuances qu'il conviendrait de circonscrire ?

1 Union Internationale des Télécommunications, *Règlement des Télécommunications Internationales*, Actes Finals de la Conférence Administrative Mondiale Télégraphique et Téléphonique, Melbourne,1988 - CAMTT-88), p.5

1.2. Différence entre les télécommunications et les communications électroniques

Il n'y a pas, en réalité, de rupture technique entre les deux domaines. En effet, les télécommunications constituent l'infrastructure de base, tandis que les communications électroniques y ajoutent les services, contenus et applications numériques. En d'autres termes, les **télécommunications** sont incluses dans les communications électroniques.

Tableau 1 : Télécommunications versus communications électroniques

	Télécommunications	Communications Électroniques
Définition simplifiée	Désignent la transmission de la voix, des messages et des données par réseaux fixes, mobiles ou satellitaires.	Désignent l'ensemble des services et usages **numériques** reposant sur les réseaux de télécommunication.
Équipements	▶ Antennes relais ▶ Stations de base (BTS, NodeB, gNodeB) ▶ Câbles sous-marins, fibres optiques ▶ Commutateurs (MSC), routeurs cœur de réseau ▶ Satellites ▶ Faisceaux hertziens	Infrastructures télécoms de base, y compris : ▶ Routeurs IP, commutateurs virtuels (EPC, IMS, 5GC) ▶ Data centers, serveurs applicatifs, plateformes cloud ▶ Systèmes de cybersécurité (pare-feux, IDS, DPI) ▶ Outils de gestion de trafic et de qualité de service (QoS, SDN)
Exemples d'usage	▶ Téléphonie fixe et mobile ▶ Transmission de données entre opérateurs (backbone) ▶ Réseaux de transport, interconnexion ▶ Communications radio (police, aviation, maritime) ▶ Diffusion TV (satellite, câble)	▶ Appels et messageries IP ▶ Visioconférences ▶ Réseaux sociaux ▶ Services en ligne : e-commerce, e-gouvernement, e-santé … ▶ Stockage et traitement des données (cloud, SaaS, IoT) ▶ Plateformes OTT (Netflix …)

Dans le présent document, les termes « télécommunications » et « communications électroniques » sont utilisés de manière interchangeable, sauf indication contraire, pour désigner l'ensemble des réseaux, services et infrastructures de transmission et de traitement numérique permettant l'échange de la voix, des données, d'images et de contenus sur divers supports (fixes, mobiles, satellitaires, Internet).


e-Commerce



ÉCONOMIE NUMÉRIQUE : QUELLE DÉFINITION ?

Le développement de l'économie numérique à l'échelle mondiale est étroitement associé au développement des technologies de l'information et de la communication (TIC). Les nombreux progrès réalisés dans les secteurs des télécommunications, de l'informatique et de l'électronique ont permis, certes, d'améliorer et de fluidifier les activités économiques et industrielles, mais aussi sociales, administratives, etc.

Du fait de sa complexité, il n'est pas aisé de définir de façon holistique l'économie numérique. Par simplicité, on peut d'ailleurs se laisser tenter de l'assimiler au commerce électronique qui n'est qu'une des composantes significatives de l'écosystème de cette économie. Cependant, l'économie numérique reste caractérisée par certains fondamentaux de l'économie classique, à savoir : *produire, distribuer et consommer des biens et des services*. Par contre, cette économie est étroitement liée aux télécommunications, à l'usage de l'Internet, ainsi qu'à d'autres technologies émergentes qui permettent de créer de la valeur économique.

C'est grâce aux infrastructures et réseaux de télécommunications, par exemple, qu'il est possible d'accéder à l'Internet très haut débit, ainsi qu'aux nombreuses plateformes numériques qui garantissent la production et la fourniture de biens et services.

Cette économie se distingue aussi par la *dématérialisation* de certains actes ou services, comme les transactions électroniques (paiement, transmission de données, etc.). Ces actes se répandent un peu plus chaque jour à travers le monde, y compris au Congo. C'est ainsi qu'on peut, par voie électronique, acheter un billet d'avion ou des vidéos à la demande (VoD), régler une facture d'électricité ou d'eau, etc.

Cette dématérialisation intègre également la rapidité des échanges ou des transactions, la facilité d'accès au contenu, ainsi que la personnalisation des services. Sans que la liste ne soit exhaustive, les caractéristiques de cette dématérialisation ont contribué et continuent de contribuer à la mutation des modèles d'affaires traditionnels. Qu'est-ce donc l'économie numérique ? À défaut d'une définition complète, on notera qu'elle ne se limite pas à un secteur d'activité en particulier, bien au contraire. Il faudrait prendre en compte la dynamique des secteurs et acteurs qui s'appuient sur les communications électroniques, sur les producteurs de biens et de services numériques, ainsi que sur les utilisateurs ou consommateurs de ces biens et services.

Ensuite, il faudrait sans doute tenir compte, dans cette définition, des acteurs clés de l'écosystème du numérique tels que les équipementiers, les opérateurs de téléphonie mobile, les fournisseurs d'accès à Internet, les fournisseurs de services et de contenu, les régulateurs, les usagers (personnes morales et personnes physiques), les administrations (e-gouvernement), etc. La République du Congo n'échappe pas à cette réalité mondiale qui doit, néanmoins, s'intégrer dans un contexte local ; ce qui nécessite des adaptions ou ajustements structurels et réglementaires face à un écosystème numérique en rapide évolution.



III CADRE RÉGLEMENTAIRE ET INSTITUTIONNEL

Cette section présente les principaux instruments juridiques, les structures et les dynamiques d'adaptation du Congo face aux mutations technologiques afin d'évaluer son niveau de préparation, ainsi que les perspectives d'une régulation prospective.

3.1. Réglementation et entités dans le secteur de l'économie numérique

La réglementation du secteur des postes, des télécommunications et de l'économie numérique a quelque peu évolué depuis le premier Livre Blanc publié en 2021 par l'Agence de Régulation des Postes et des Communications Electroniques (ARPCE). En effet, de nouvelles dispositions complètent la législation en vigueur.

Tableau 2 : Cadre législatif du secteur des postes, des télécommunications et de l'économie numérique

Année	Référence et intitulé	Objet / portée principale
2009	Loi n° 9-2009 du 25 nov. 2009	Réglementation du secteur des communications électroniques
2009	Loi n° 10-2009 du 25 nov. 2009	Réglementation du secteur postal
2009	Loi n° 11-2009 du 25 nov. 2009	Création de l'Agence de Régulation des Postes et des Communications Électroniques (ARPCE)
2019	Loi n° 29-2019 du 10 oct. 2019	Protection des données à caractère personnel
2019	Loi n° 30-2019 du 10 oct. 2019	Création de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)
2019	Loi n° 37-2019 du 12 déc. 2019	Transactions électroniques et confiance numérique.
2020	Loi n° 26-2020 du 5 juin 2020	Cybersécurité
2020	Loi n° 27-2020 du 5 juin 2020	Lutte contre la cybercriminalité
2022	Loi n° 69-2022 du 16 août 2022	Création de l'Agence de Développement de l'Économie Numérique (ADEN)
	Loi n° 71-2022 du 16 août 2022	Attribution du label « startup du numérique et de l'innovation technologique »
2025	Loi n° 5-2025 du 29 mars 2025	Création de la Commission nationale pour la protection des données à caractère personnel.

Concernant les textes d'application, le secteur s'est enrichi, depuis, d'au moins une dizaine de décrets.

Tableau 3 : Cadre réglementaire du secteur des postes, des télécommunications et de l'économie numérique

Année	Références	Objet / domaine concerné
2009	Décret n° 2009-476 du 24 déc. 2009	Création de la Direction générale des postes et télécommunications (DGPT)
2010	Décret n° 2010-554 du 26 juil. 2010	Identification des souscripteurs d'abonnements aux services de téléphonie fixe et mobile et conservation des données de communications électroniques
2011	Décret n° 2011-734 du 7 déc. 2011	Conditions d'établissement et d'exploitation des réseaux et services à très haut débit
2015	Décret n° 2015-242 du 4 fév. 2015	Modalités d'encadrement des tarifs des services de communications électroniques
	Décret n° 2015-243 du 4 fév. 2015	Interconnexion des réseaux de télécommunication ouverts au public
	Décret n° 2015-244 du 4 fév. 2015	Gestion du plan national de numérotation et conditions d'utilisation des ressources en numérotation
	Décret n° 2015-245 du 4 fév. 2015	Conditions d'installation et d'exploitation des réseaux et services postaux
	Décret n° 2015-253 du 19 fév. 2015	Approbation du plan national d'attribution des bandes de fréquences radioélectriques
	Décret n° 2015-254 du 19 fév. 2015	Homologation des équipements terminaux et radioélectriques, vérification de conformité et contrôle technique à l'importation
	Décret n° 2015-255 du 19 fév. 2015	Conditions d'établissement et d'exploitation des réseaux et services de communications électroniques et de distribution d'équipements
2018	Décret n° 2018-111 du 21 mars 2018	Organisation du ministère des Postes, des Télécommunications et de l'Economie numérique
2019	Décret n° 2019-172 du 1er juil. 2019	Modalités de gestion et d'utilisation du spectre de fréquences radioélectriques
2022	Décret n° 2022-76 du 28 fév. 2022	Modalités d'approbation des tarifs des services postaux universels et réservés
	Décret n° 2022-77 du 28 fév. 2022	Désignation de l'opérateur postal en charge du service universel
	Décret n° 2022-78 du 28 fév. 2022	Liste des objets interdits dans les envois postaux
	Décret n° 2022-79 du 28 fév. 2022	Poids limite des envois relevant des services réservés
2023	Décret n° 2023-158 du 10 mai 2023	Nouvelles modalités de gestion du FASUCE (actualisation du décret 2019-123)
2024	Décret n° 2024-118 du 27 mars 2024	Règles de gestion de l'offre de service public, incluant le numérique

Tableau 3 : Cadre réglementaire du secteur des postes, des télécommunications et de l'économie numérique (suite)

Année	Références	Objet / domaine concerné
2025	Décret n° 2025-279 du 2 Juil. 2025	Approbation des statuts du centre africain de recherche en intelligence artificielle
	Décret n° 2025-280 du 2 Juil. 2025	Procédure de retrait du label startup du numérique et de l'innovation technologique
	Décret n° 2025-281 du 2 juil. 2025	Création de la commission de labellisation des startups du numérique (application de la loi n° 71-2022)
	Décret n° 2025-317 du 23 juil. 2025	Codification postale nationale et réforme du secteur postal

Enfin, la cartographie[2] ci-après des entités qui jouent un rôle important dans l'économie numérique a été mise à jour.

Figure 1 : Entités dans le secteur des postes, des télécommunications et de l'économie numérique

Ministère des Postes, des Télécommunications et de l'Economie Numérique

Exécute la stratégie de développement de l'économie numérique

Entité	Sigle	Mission	Situation
Direction générale des postes et télécommunications	DGPT	Met en œuvre la politique des postes et télécommunications	Fonctionnelle
Inspection des postes, des télécommunications et du numérique	IPTEN	Contrôle le fonctionnement des structures sous la tutelle du ministère	Fonctionnelle
Agence de régulation des postes et des communications électroniques	ARPCE	Régule, suit et évalue les secteurs des postes et des communications électroniques	Fonctionnelle
Agence de développement de l'économie numérique	ADEN	Met en œuvre la politique nationale de développement de l'économie numérique	Fonctionnelle
Agence congolaise des systèmes d'information	ACSI	Elabore et met en œuvre des systèmes d'information	Fonctionnelle
Agence nationale de sécurité des systèmes d'information	ANSSI	Veille sur le cyberespace national en vue de parer aux cyberattaques	En cours d'opérationnalisation
Centre d'informatique et de recherche de l'armée et de la sécurité	CIRAS	Promeut la politique des TIC en matière de défense nationale et de sécurité	Fonctionnelle
Commission nationale pour la protection des données à caractère personnel	CNPD	Veille à la mise en œuvre des traitements des données à caractère personnel	Non fonctionnelle

2 ARPCE, *Livre blanc des postes, des télécommunications et de l'économie numérique*, 2021, p.23.

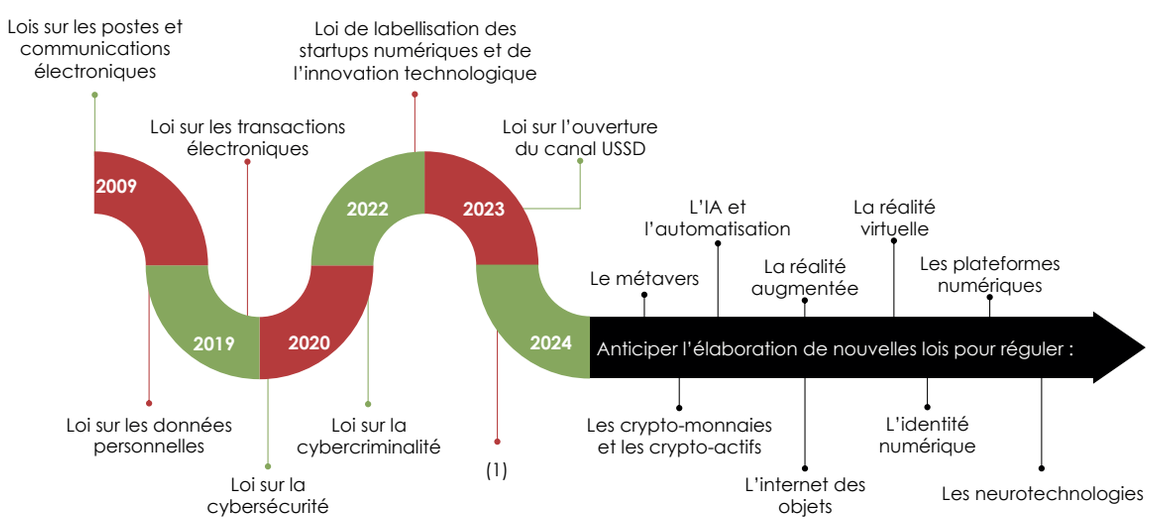
L'Agence de Développement de l'Economie Numérique (ADEN), créée en août 2022[3], n'est devenue opérationnelle qu'en septembre 2023[4]. Elle assure, pour le compte de l'Etat, la mise en œuvre de la politique nationale en matière d'économie numérique.

Quant à l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), créée en 2019[5], son opérationnalisation n'a débuté qu'en décembre 2024[6]. Cet établissement public administratif, doté de la personnalité juridique et de l'autonomie financière, a pour mission de contrôler et de suivre les activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques afin de garantir la protection du cyberespace national. En fonction de son développement et de sa gestion, l'ANSSI devrait devenir l'une des entités les plus influentes de l'écosystème numérique en République du Congo. Enfin, la Commission Nationale de Protection des Données à Caractère Personnel (CNPD), inexistante en 2021, a été créée en mars 2025[7]. Aux côtés de l'ANSSI, elle jouera un rôle essentiel, notamment dans la protection de la souveraineté numérique de la République du Congo[8].

3.2. Cadre réglementaire prospectif de l'économie numérique

Entre 2009 et 2023, la République du Congo a adopté au moins dix (10) textes de lois majeurs dans les secteurs des postes, des télécommunications et de l'économie numérique.

Figure 2 : Évolution prospective du cadre légal de l'économie numérique



(1) En 2024, aucune loi supplémentaire ne semble avoir été adoptée dans les secteurs des postes, des télécommunications et de l'économie numérique.

3 Loi n°69-2022 du 16 août 2022 portant création de l'Agence de Développement de l'Economie Numérique.

4 Décret n°2023-1572 du 15 septembre 2023 portant nomination du directeur général de l'Agence de Développement de l'Economie Numérique.

5 Loi n°30-2019 du 10 octobre 2019 portant création de l'Agence Nationale de Sécurité des Systèmes d'Information.

6 Décret n°2024-2879 du 20 décembre 2024 portant nomination du directeur général de l'Agence Nationale de Sécurité des Systèmes d'Information.

7 Loi n°5-2025 du 29 mars 2025 portant création de la Commission Nationale de Protection des Données à caractère personnel.

8 Au moment de la rédaction de cet ouvrage, la CNPD n'est pas encore fonctionnelle.

Si certaines lois adoptées en République du Congo permettent déjà d'anticiper des aspects de la régulation du futur, d'autres devront encore être élaborées afin de favoriser une régulation à même de garantir les intérêts des différentes parties prenantes de son écosystème numérique.

Est-il trop tôt pour le Congo, compte tenu de son niveau de développement économique et industriel, de concevoir des textes de loi qui aborderaient les problématiques relatives :

- à la régulation du **métavers**, afin de mieux encadrer les droits numériques des « mondes » immersifs ;
- à la régulation des **crypto-monnaies[9] et des crypto-actifs[10]** pour, par exemple, encadrer le fonctionnement des plateformes d'échange ;
- à **l'intelligence artificielle**, notamment pour clarifier la question de la responsabilité liée aux algorithmes qui sont au cœur des décisions ou actions automatisées générées par elle ;
- au cadre juridique de la **réalité virtuelle, augmentée** et **mixte** afin d'assurer la protection des données (y compris biométriques), et d'encadrer les droits d'auteur dans les espaces virtuels, parmi d'autres ;
- aux normes de **l'Internet des objets (IoT)** sur la sécurité des objets connectés et interconnectés, entre autres ;
- à la régulation des **identités numériques** (e-identités) afin de sécuriser l'identification en ligne, protéger les données personnelles, prévenir l'usurpation d'identité et renforcer les droits des utilisateurs ;
- à l'encadrement des **plateformes numériques** pour préserver un environnement numérique sûr et transparent pour les utilisateurs ;
- à l'encadrement des **neurotechnologies**, en particulier les interfaces cerveau-machine, afin de protéger les données cérébrales des individus — notamment dans le domaine médical — et de définir des principes éthiques pour guider les interactions entre l'humain et la machine ?

La liste ci-dessus n'est pas exhaustive. Cependant, les Etats qui prendront des dispositions avant-gardistes, et qui les peaufineront au fur et à mesure des évolutions technologiques, seront mieux préparés à réguler leur économie numérique par opposition à ceux qui demeureront passifs ou attentistes ; se contentant ainsi de subir les évolutions ou mutations technologiques, plutôt que de les anticiper.

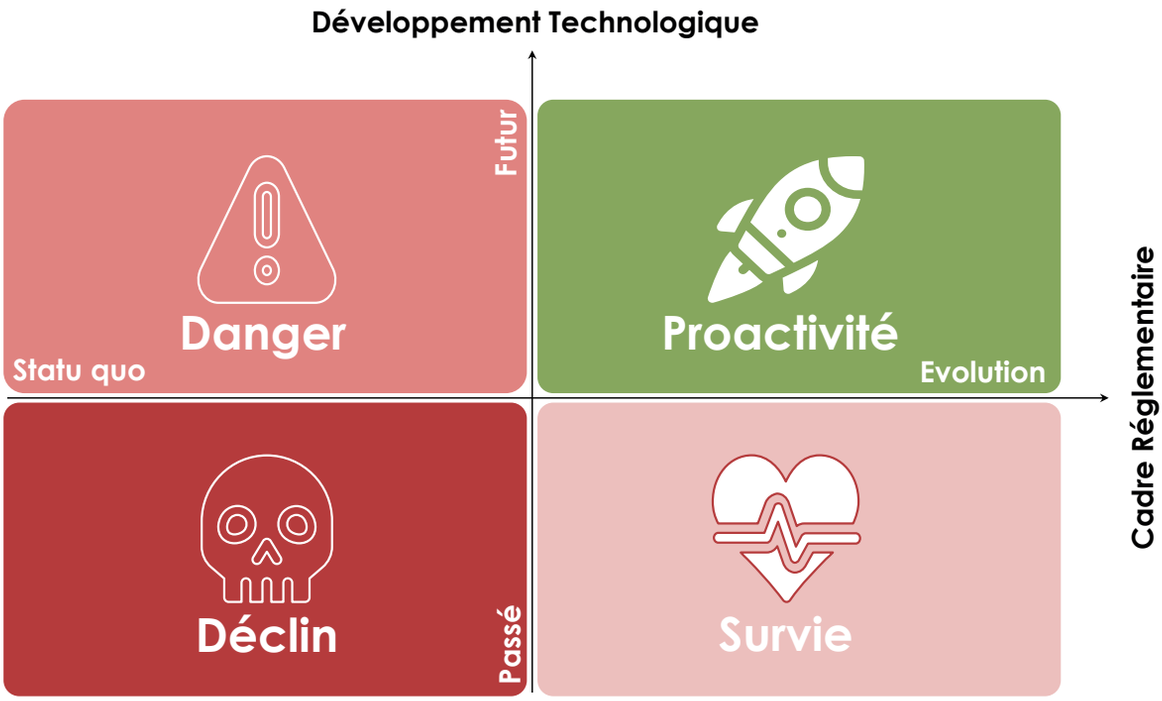
3.3. Matrice des mutations technologiques et réglementaires

Le Congo pourrait dynamiser son économie numérique par une approche proactive qui consisterait à anticiper les évolutions technologiques, ainsi que la réglementation qui les accompagne. C'est dans ce cadre que l'Agence de Régulation des Postes et des Communications Électroniques (ARPCE) a développé une matrice des mutations technologiques dont l'axe horizontal représente le *cadre réglementaire*, et l'axe vertical les *évolutions technologiques*.

9 Les crypto-monnaies n'obéissent pas à la réglementation des banques centrales ou à celles d'autres institutions internationales de régulation monétaire. Elles sont donc décentralisées et reposent sur la technologie blockchain. Le « Bitcoin » demeure, à date, la plus connue des crypto-monnaies.

10 Les crypto-actifs sont des actifs numériques qui englobent les crypto-monnaies. Cependant, tous les crypto-actifs ne sont pas des crypto-monnaies. Les *NFT (jetons non fongibles)*, par exemple, sont des actifs numériques uniques (non reproductibles) utilisés dans l'art, tandis que les *Security Tokens (Jetons de sécurité)* sont la représentation numérique d'actifs financiers tels que des actions.

Figure 3 : Enjeux des mutations technologiques



Cette matrice propose quatre scénarios :

- **Scénario 1 : Déclin (cadran inférieur gauche)**

Dans ce scénario, le positionnement du Congo dans le cadran inférieur gauche indiquerait qu'il n'aurait pas réussi sa transformation numérique ; ce qui sous-entendrait que le gouvernement et les opérateurs privés n'investiraient plus dans les infrastructures technologiques.

L'absence de renouvellement des infrastructures technologiques paralyserait le fonctionnement de nombreux secteurs (santé, finance, éducation, etc.) puisque la connectivité et les échanges d'informations ne répondraient plus aux exigences de la modernité. Les institutions financières, par exemple, pourraient rencontrer des difficultés liées à la sécurité et fiabilité des transactions qui deviendraient vulnérables aux cyberattaques, tandis que le système éducatif peinerait à intégrer des outils éducatifs modernes (limitant, entre autres, l'apprentissage en ligne ou l'accès à certaines ressources pédagogiques à caractère numérique).

Dans ce scénario, le législateur ne ferait plus ou pas évoluer son arsenal juridique qui deviendrait ainsi obsolète et inadéquat en rapport avec les mutations technologiques mondiales.

*Le scénario du **déclin** est très peu probable en République du Congo.*

- **Scénario 2 : Survie (cadran inférieur droit)**

Le positionnement du Congo dans le cadran inférieur droit serait la résultante d'une incohérence en termes de politique globale de transformation numérique. En effet, dans ce scénario, le législateur aura fait évoluer son arsenal juridique, en le modernisant en rapport avec les mutations technologiques mondiales. Par contre,

le gouvernement n'investirait plus dans les infrastructures technologiques, et serait également parvenu, par cet état de fait, à décourager les opérateurs privés qui cesseraient alors de renouveler ou de construire de nouvelles infrastructures de communications électroniques.

Quel intérêt aurait le législateur à moderniser l'arsenal juridique du Congo pour l'arrimer aux TIC si, en même temps, des mesures contraires étaient prises quant à la modernisation des infrastructures de télécommunications, ainsi que des technologies associées ?

*Le scénario de **Survie** montre une incohérence dans les politiques et stratégies de développement des TIC.*

- **Scénario 3 : Danger (cadran supérieur gauche)**

Dans ce scénario, le Congo n'aurait pas fait évoluer son cadre réglementaire pour faire face aux mutations technologiques. Cependant, le gouvernement n'aurait pas cessé d'investir dans le développement des infrastructures technologiques nécessaires à l'essor de l'économie numérique. De même, les opérateurs privés continueraient d'investir dans le renouvellement de leurs réseaux de communication électronique, en bonne intelligence avec les autorités locales.

Toutefois, en l'absence d'une évolution du cadre réglementaire, il faudrait craindre, parmi d'autres, que les droits des citoyens et des personnes morales ne soient pas toujours préservés. De même, il se pourrait que certains acteurs de l'économie numérique profitent de cette faiblesse réglementaire pour ne pas se conformer aux meilleures pratiques concurrentielles internationales, y compris en matière de normes techniques.

*Ce scénario est-celui du **Danger**, certes, mais il est réversible si l'axe horizontal suit la cohérence de l'axe vertical.*

- **Scénario 4 : Proactivité (cadran supérieur droit)**

Dans ce scénario, le Congo aurait fait évoluer son arsenal juridique en réponse aux évolutions et mutations technologiques. L'essentiel des conditions de l'arrimage du Congo aux TIC seraient remplies. La société numérique au Congo serait en phase, non pas de développement, mais de consolidation et d'anticipation.

Sur le plan technologique, le Congo serait reconnu comme un État dans lequel on investit dans l'éducation numérique, dans l'innovation, la recherche & développement (R&D) et l'industrialisation. Il passerait à une phase plus délicate qui est celle de la conception et fabrication de certains équipements technologiques, et participerait davantage aux prises de décisions internationales sur les normes à adopter sur le plan technologique.

Sur le plan réglementaire, le Congo tiendrait compte des réalités locales, voire africaines, dont il serait un des porte-voix au niveau des instances internationales comme l'UIT pour faire évoluer la réglementation internationale. Il pourrait, certes, continuer de s'inspirer de grandes nations ou ensembles politiques et technologiques comme la Chine, les États-Unis ou l'Union Européenne. Toutefois, il s'abstiendrait de toute forme de mimétisme coupable qui occulterait la nécessaire prise en compte du contexte local.

*Ce scénario est celui de la **Proactivité** ou de l'anticipation. Le Congo deviendrait, à tout le moins en Afrique, une référence en matière de progrès technologique et réglementaire.*

Cette matrice est un outil de portée stratégique qui peut s'adapter à différents contextes, créant ainsi autant de variantes que nécessaire afin d'aider à la prise de décision.

3.4. Positionnement du Congo dans une variante de la matrice

Le cadre réglementaire en vigueur en République du Congo peut-il favoriser la régulation du secteur des postes, des télécommunications et de l'économie numérique au regard de l'évolution des technologies et de l'écosystème complexe qui se construit autour du numérique ? Cette question, d'ordre mondial, ne se pose pas qu'au Congo. En effet, la transition numérique - avec ses multiples répercussions sociales, économiques et technologiques - oblige les décideurs politiques à faire évoluer la ou les réglementation(s).

À cet effet, l'UIT a développé un modèle qui permet d'évaluer l'évolution de la réglementation des pays membres. Ce modèle, intitulé *Générations de Réglementation*, comporte cinq (5) maillons compris entre G1 et G5, définis succinctement ci-après :

- la **Génération 1** (G1) ou réglementation de première génération est celle où le régulateur se caractérise surtout par le *commandement* et le *contrôle (monopole d'État)* ;
- la **Génération 2** (G2) ou réglementation de deuxième génération est celle qui a favorisé la *libéralisation/privatisation partielle* des secteurs régulés ;
- la **Génération 3** (G3) ou réglementation de troisième génération est celle qui facilite ou encourage *les investissements*, *l'innovation* et *l'accès* aux secteurs régulés ;
- la **Génération 4** (G4) ou réglementation de quatrième génération est dite *intégrée* en ce qu'elle tient aussi compte des objectifs et politiques socio- économiques d'un État ;
- la **Génération 5** (G5) ou réglementation de cinquième génération[11] se veut collaborative (multi-régulation) afin de prendre en compte les différentes répercussions de l'économie numérique dans les autres secteurs.

Les Générations 1 à 4 permettent d'évaluer *la maturité de la réglementation* des marchés des *télécommunications* au sein d'un pays membre de l'UIT, tandis que la Génération 5 permet d'apprécier le niveau de préparation des États à la Transformation Numérique. La G5 comporte ainsi quatre sous-catégories, à savoir :

- **G5 limitée** (G5-L) : une politique sectorielle étroite sans gouvernance concertée ;
- **G5 en transition** (G5-T) : approche fragmentaire de la politique numérique ;
- **G5 avancée** (G5-A) : approche holistique de la politique et de la gouvernance numériques ;

11 https://app.gen5.digital/benchmark/concepts, site consulté le 04/09/2024.

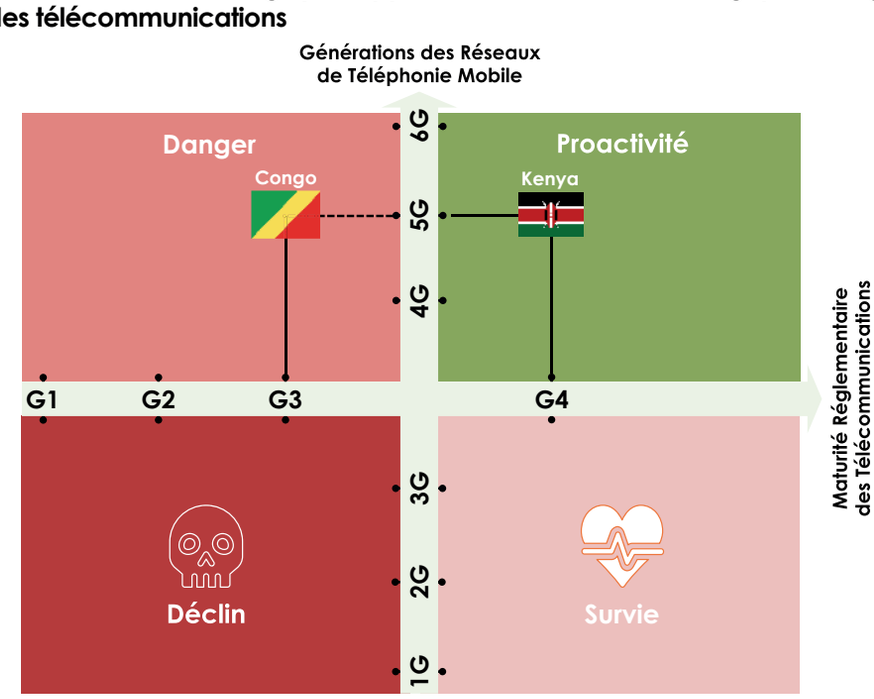
- **G5 leader** (G5-Ld) : cohérence politique et gouvernance allégée[12].

À partir du classement 2022 du Congo dans le *ICT Regulatory Tracker* de l'UIT, relatif à la maturité réglementaire des États dans le secteur des télécommunications (G1 à G4), il est possible de positionner le Congo dans la matrice des mutations technologiques en rapport avec les différentes générations des réseaux de téléphonie mobile (2G à 5G).

Dans la matrice ci-après, l'hypothèse retenue est que les niveaux de maturité réglementaire G1 à G3 sont globalement surannés ; ce qui explique pourquoi ils sont placés à gauche de la matrice. Par contre, la G4 étant une réglementation télécom qui est en phase avec *la politique* et *les objectifs socio-économiques des gouvernements*, elle est placée à droite de la matrice. C'est donc, à date, le degré de maturité réglementaire le plus important desdites générations réglementaires pour le secteur des télécommunications.

Pour ce qui est de l'évolution des générations des réseaux télécoms, les générations 1G à 3G sont placées dans la partie inférieure de la matrice. Un État qui veut amorcer une réelle transformation numérique ne saurait y parvenir avec ces technologies qui tombent progressivement en désuétude. En effet, n'avoir que la technologie 3G dans une économie qui veut se transformer digitalement n'est pas possible. Il faudrait, au minimum, qu'elle adopte la technologie 4G. C'est pourquoi les technologies 4G, 5G et au-delà sont placées dans la partie supérieure de la matrice.

Figure 4 : Positionnement du Congo par rapport aux évolutions technologiques et réglementaires des télécommunications



Sources : UIT[13][14] - Safaricom[15]

12 Mode de gestion et de régulation des organisations ou institutions visant à simplifier les processus décisionnels et administratifs tout en préservant une efficacité opérationnelle, notamment dans le cadre de la multi-régulation de l'économie numérique.

13 Union Internationale des Télécommunications et Banque Mondiale, *Manuel sur la réglementation du numérique*, 2020

14 https://app.gen5.digital/tracker/metrics, site consulté le 02/09/2024

15 https://internet.safaricom.co.ke/5g-wireless/coverage, site consulté le 02/09/2024

- **Le Congo dans le cadran supérieur gauche (Danger)**

Sur la base des données publiées par l'UIT en 2022, le Congo se situe, *en termes de maturité de la réglementation* des télécommunications, dans la catégorie G3. En termes *d'évolution des technologies* des réseaux de téléphonie mobile, le Congo a déployé la 2G, la 3G, la 4G et la 5G depuis le 21 novembre 2024. La matrice fait ressortir la technologie de téléphonie mobile la plus avancée parce qu'elle couvre au-delà des fonctionnalités des technologies précédentes.

En conséquence, le Congo se situe dans le cadran « Danger » de la matrice parce que son arsenal réglementaire doit encore évoluer pour qu'il soit plus à même de répondre aux challenges induits par le développement des technologies de nouvelle génération telle que la 5G. En revanche, la situation actuelle du Congo permet d'affirmer qu'il y a très peu de chance qu'il bascule dans le cadran « Déclin ».

Pour que le Congo bascule vers le cadran « Proactivité », il devra faire évoluer l'écosystème des communications électroniques, aussi bien sur le plan réglementaire que sur le plan des infrastructures de communications électroniques. Il devra aussi renforcer le niveau de formation dans les métiers des communications électroniques, créer les conditions idoines à l'éclosion d'un environnement propice aux innovations technologiques, etc.

En conclusion, le basculement du cadran supérieur gauche vers le cadran supérieur droit de la matrice nécessite une approche globale et cohérente au niveau gouvernemental.

- **Le Kenya dans le cadran supérieur droit (Proactivité)**

Le Kenya, en comparaison, se situe dans la catégorie G4 pour ce qui est de la maturité de la réglementation des télécommunications. En termes d'évolution des technologies des réseaux de téléphonie mobile, ce pays a déployé la 2G, la 3G, la 4G et la 5G dont l'expansion se poursuit.

Le Kenya a anticipé et adapté le cadre juridique des télécoms en adéquation avec certains objectifs globaux du gouvernement, notamment pour ce qui est du développement technologique. Le Kenya ne cesse, non plus, d'être avant-gardiste en termes de déploiement d'infrastructures de communications électroniques. Pour preuve, l'écosystème technologique du Kenya était estimé à 1 milliard de dollars[16] en 2021, et accueille des entreprises de classe mondiale comme Google, IBM, Facebook, Intel, Microsoft, etc. Le Kenya se classe ainsi en tête des cinq (5) destinations d'investissement les plus populaires en Afrique pour les startups[17].

3.5. Niveau de préparation du Congo à la réglementation du numérique

La transformation numérique d'un État ne dépend pas seulement des infrastructures de communications électroniques, quoiqu'elles soient un pilier indissociable du développement des TIC. Les technologies émergentes continuent de prendre de l'ampleur, et favorisent l'ouverture vers de nouvelles frontières grâce, mais sans que la liste ne soit exhaustive, à l'intelligence artificielle, à l'Internet des objets, à la réalité augmentée, à la réalité virtuelle, à la 5G en cours de déploiement au Congo, à la 6G en cours de développement chez les équipementiers ou OEM[18], etc.

16 https://www.s-ge.com/fr/article/global-opportunities/20213-c6-kenya-tech-hub-fint1?ct, site consulté le 06/09/2024

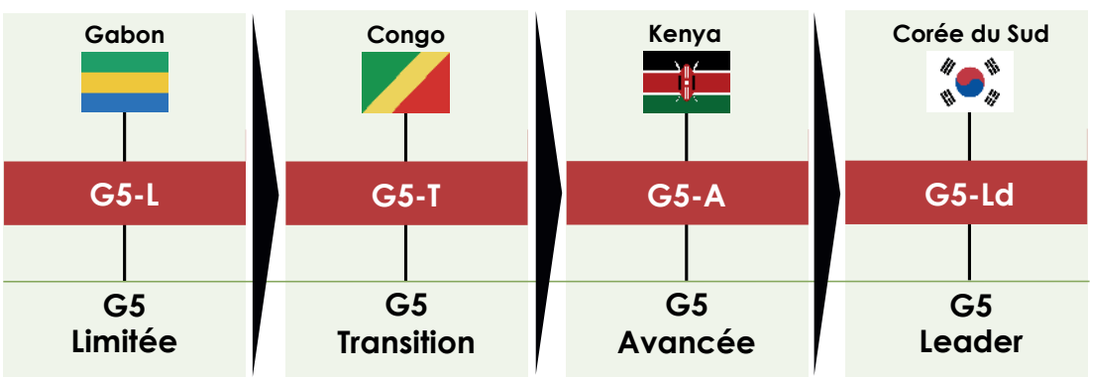
17 https://kippra.or.ke/building-a-robust-digital-economy-in-kenya/, site consulté le 06/09/2024

18 *Original Equipment Manufacturers* pour désigner les équipementiers industriels.

La régulation actuelle a donc ses limites, y compris la régulation de 4e Génération (G4) du fait qu'elle ne saurait encadrer tous les défis associés à cette nouvelle donne qu'est la *régulation du futur*. C'est pourquoi les États s'évertuent à mettre en place le cadre réglementaire qui soit le plus large possible afin de répondre aux attentes, intérêts et/ou préoccupations des consommateurs, des opérateurs et de l'État.

Une classification de cette évolution de la réglementation existe, comme présentée supra, avec les sous-catégories de la G5. C'est ce qui permet de voir, dans la figure ci-après, le positionnement du Congo, en comparaison avec d'autres pays.

Figure 5 : Niveau de préparation du Congo à la transformation numérique



Source : UIT (G5 Benchmark)[19]

On notera, cependant, que cette catégorisation de l'UIT tient compte des *déclarations* faites par les Etats membres. C'est donc essentiellement sur une base déclarative, en fonction des textes de lois qu'ils ont pris, que les Etats sont évalués et positionnés.

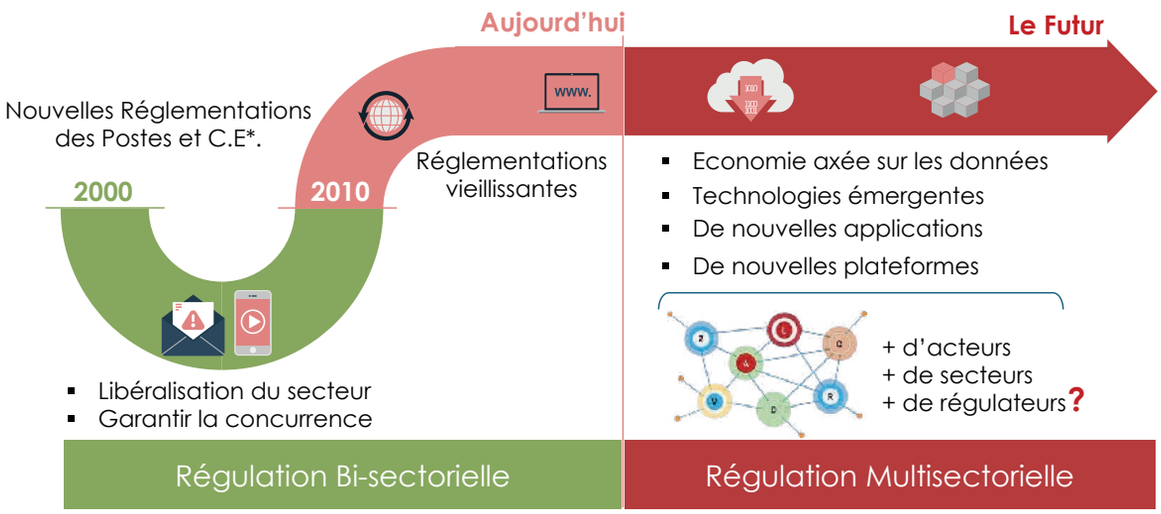
L'évolution actuelle du cadre légal dans le secteur des postes, des télécommunications et de l'économie numérique place le Congo dans la catégorie « G5-Transition » par l'UIT. Cependant, le cadre légal ne saurait être le seul critère de préparation effective à la transformation numérique du Congo.

3.6. Vers une nouvelle gouvernance : anticiper la régulation du futur

La République du Congo, à l'image d'un grand nombre de pays à travers le monde, doit préparer le futur, c'est-à-dire la réglementation des dix (10) prochaines années. La libéralisation des secteurs des postes et des communications électroniques, dans les années 2000, avait pour enjeu majeur d'encourager l'exercice de la libre concurrence entre opérateurs. De 2010 à nos jours, il est établi que l'actuel cadre réglementaire du secteur des communications électroniques doit évoluer pour mieux répondre aux enjeux du futur.

19 https://app.gen5.digital/benchmark/metrics, site consulté le 02/09/2024

Figure 6 : Enjeux de la régulation du futur



*C.E = Communications Electroniques

La régulation bi-sectorielle repose sur la collaboration entre deux régulateurs de secteurs distincts mais complémentaires. Un simple protocole d'accord entre eux peut suffire à cette co-régulation, en l'absence de cadre légal.

La régulation multisectorielle, par nature complexe, mobilise divers acteurs issus de nombreux secteurs, certains étant sous la tutelle d'une autorité de régulation, d'autres non. Il est essentiel de parvenir à encadrer efficacement les technologies émergentes ainsi que les plateformes et applications qui en découlent. Cependant, cette régulation présente de nombreux défis, notamment en raison d'une organisation encore à définir :

- **complexité accrue** : réguler plusieurs secteurs simultanément requiert une coordination étroite entre différentes agences et autorités qui peut causer des inefficacités et des retards de mise en œuvre ;
- **conflits d'intérêts** : tenir compte des objectifs et priorités qui peuvent varier d'un secteur à l'autre. Les régulations applicables pour protéger les consommateurs dans le secteur des télécommunications pourraient ne pas être totalement alignées avec celles du secteur financier ou bancaire, par exemple[20] ;
- **ressources limitées** : la régulation multisectorielle pourrait se heurter à un manque de moyens humains et financiers susceptible de réduire son efficacité. Même si certaines institutions disposent de compétences techniques avérées, cela ne suffit pas toujours à couvrir l'ensemble des secteurs de l'économie numérique ;
- **adaptabilité** : s'assurer que les réglementations multisectorielles soient suffisamment flexibles afin de tenir compte de la rapidité des évolutions ou mutations technologiques. Une approche multisectorielle peut parfois manquer de flexibilité, et retarder l'adoption de nouvelles innovations ;

20 La réglementation dans les communications électroniques favorise des règles assez contraignantes sur la gestion des données à caractère personnel et la confidentialité des communications. Or, cette réglementation peut entrer en contradiction avec certaines exigences du secteur financier qui requiert l'accès aux données personnelles des clients afin de prévenir la fraude et le blanchiment d'argent, entre autres.

- **transparence et responsabilité** : se rendre à l'évidence que la multiplicité des régulateurs dans une approche multisectorielle peut avoir un impact sur la transparence et la responsabilité[21].

La régulation multisectorielle apparaît comme une nécessité face aux défis qu'imposent les technologies du futur. Toutefois, ces limites soulignent l'importance d'une conception rigoureuse avant une mise en œuvre efficace. Pour autant, cela ne signifie pas qu'il faille multiplier les autorités de régulation, au risque de créer des redondances et d'amplifier les difficultés déjà identifiées. Ainsi, *un manque de cohérence réglementaire* au sein de l'écosystème de l'économie numérique pourrait freiner son développement en République du Congo.

21 Une entreprise qui propose des paiements mobiles va être soumise à la régulation des télécommunications pour l'aspect technologique, et à celle du secteur bancaire pour les transactions financières. Les consommateurs peuvent se retrouver dans une situation dans laquelle, en cas de litige (fraude, problème de remboursement, etc.), ils pourraient ne pas savoir s'ils doivent s'adresser à l'autorité de régulation des télécommunications ou à celle du secteur financier. Cette confusion peut nuire à leur confiance dans le système et ralentir la résolution des problèmes.



IV. INFRASTRUCTURES ÉNERGÉTIQUES ET RÉSILIENCE NUMÉRIQUE

La production et la distribution d'une électricité de qualité, et en quantité suffisante, sont essentielles au bon fonctionnement des infrastructures de télécommunications. Sans une fourniture régulière et stable du courant électrique, l'accès à Internet, la digitalisation des services publics, le développement de l'Internet des objets (IoT) ou encore la promotion de l'usage des technologies cloud serait soumis à de fortes contraintes.

Sur la base des données disponibles dans le Plan National de Développement 2022-2026[22], seuls 44 % de la population avaient accès à l'électricité en 2022. Estimé à 54 %, le taux de perte d'énergie produite dans le réseau électrique demeurait déjà un des plus élevés au monde en 2016[23]. Est-il possible, dans ces conditions, de réussir l'inclusion numérique ?

Les opérateurs des réseaux de communications électroniques, pour faire face aux délestages et à l'absence de fourniture électrique dans certaines zones, doivent investir dans des systèmes de secours très élaborés (groupes électrogènes, panneaux solaires, onduleurs, stabilisateurs, etc.) afin de continuer à fournir leurs services aux usagers. Cette contrainte les oblige à répercuter les coûts d'exploitation y relatifs sur le pouvoir d'achat des consommateurs.

La transformation numérique du Congo repose en grande partie sur un accès fiable à l'énergie électrique. C'est en cela que les producteurs et distributeurs d'électricité sont des acteurs importants de cette transformation.

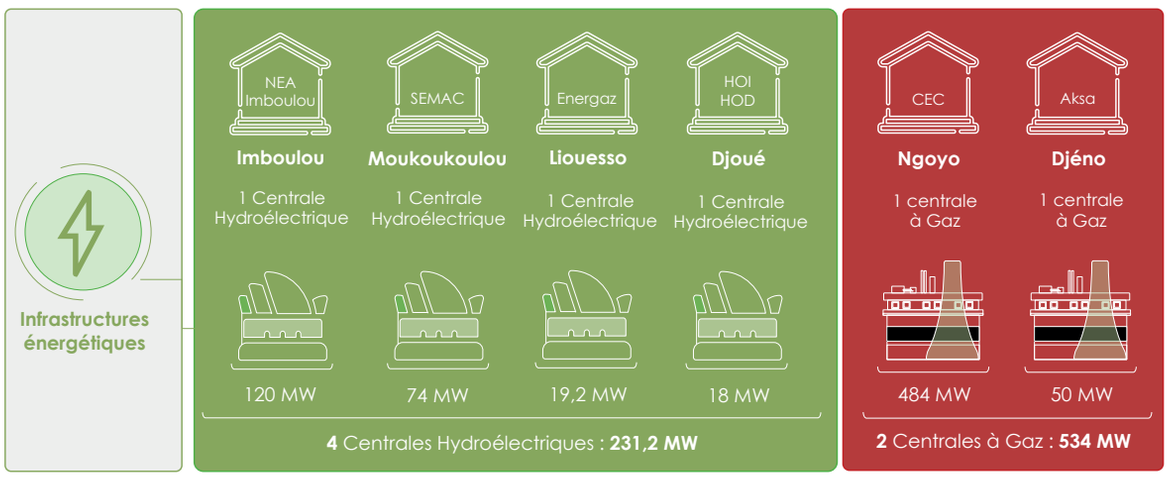
4.1. Opérateurs et infrastructures énergétiques

La production de l'électricité en République du Congo, comme le montre la figure ci-après, est essentiellement assurée par deux types de centrales : les centrales hydroélectriques et les centrales à gaz.

22 Plan National de Développement, PND 2022 - 2026, *Annexe N°2, Programme Pluriannuel des Actions Prioritaires*, p.49.

23 Plan National de Développement, PND 2022 - 2026, *Cadre Stratégique de Développement (CSD)*, p.9.

Figure 7 : Cartographie des centrales de production énergétique



4.1.1. Centrales hydroélectriques

Il existe actuellement quatre (4) centrales ou barrages hydroélectriques qui cumulent une puissance nominale maximale d'environ 231,2 MW.

- **Centrale hydroélectrique d'Imboulou (NEA Imboulou)**

D'une puissance maximale nominale de 120 MW, la centrale hydroélectrique d'Imboulou[24] a été concédée à la société privée de droit congolais dénommée *NEA Imboulou* qui, entre autres, en assure l'exploitation.

- **Centrale hydroélectrique de Moukoukoulou (SEMAC)**

La centrale hydroélectrique de Moukoukoulou[25] est désormais exploitée par la *société d'électricité de Moukoukoulou au Congo*, en sigle SEMAC. Elle est dotée d'une puissance maximale nominale de 74 MW.

- **Centrale hydroélectrique de Liouesso (Energaz)**

Energaz est la société qui exploite la centrale hydroélectrique de Liouesso[26], la seule d'envergure, à date, dans le septentrion congolais. Sa puissance maximale nominale est de 19,2 MW.

- **Centrale hydroélectrique du Djoué (HOI et HOD)**

Deux entreprises ont en charge l'exploitation de la centrale hydroélectrique du Djoué[27] dont la puissance maximale nominale est de 18 MW. Il s'agit de *Hydro Operation International* (HOI) et de *Hydro Operation Djoué* (HOD).

24 Décret n° 2024-122 du 27 mars 2024 portant approbation de la convention de concession pour la révision, la réhabilitation et l'exploitation de la centrale hydroélectrique d'Imboulou.

25 Décret n° 2024-121 du 27 mars 2024 portant approbation de la convention de concession pour la révision, la modernisation et l'exploitation de la centrale hydroélectrique de Moukoukoulou.

26 Décret n°2024 -123 du 27 mars 2024 portant approbation de la convention de concession pour l'exploitation de la centrale hydroélectrique de Liouesso.

27 Décret n°2024-120 du 27 mars 2024 portant approbation de la convention de concession pour la réhabilitation, l'extension et l'exploitation de la centrale hydroélectrique du Djoué.

4.1.2. Centrales à gaz

Il existe deux centrales à gaz en République du Congo, implantées à Pointe-Noire, dans la capitale économique. Elles cumulent une puissance nominale maximale d'environ 534 MW.

- **Centrale électrique du Congo (Etat et Eni Congo)**

La Centrale électrique du Congo (CEC) est une société anonyme détenue à 80 % par l'Etat et à 20 % par la société pétrolière Eni Congo[28]. Elle est détentrice d'une licence[29] de producteur indépendant valable pour la période 2019-2039 ; soit 20 ans. La CEC détient également une licence[30] d'exportation de l'électricité valable pour la période 2021-2031 ; soit 10 ans. Elle produit 484 MW[31] d'électricité à partir du gaz naturel en provenance de certains champs pétroliers off-shore.

- **Centrale à gaz de Djéno (Aksa)**

Depuis novembre 2022[32], la Centrale à gaz de Djéno, exploitée par la société anonyme Aksa Energy Company Congo[33], produit 25 MW sur une capacité installée de 50 MW. La concession accordée à Aksa s'étend sur 30 ans (2021 à 2051). Par ailleurs, cette société détient une licence provisoire de producteur[34] indépendant d'électricité et s'engage à porter la capacité de la centrale à 100 MW.

4.2. Perspectives de renforcement des infrastructures énergétiques

La puissance maximale *nominale* des centrales hydroélectriques et à gaz est d'environ 765,2 MW. Conformément aux objectifs du plan national de développement 2022-2026 dans le secteur de l'énergie, il est prévu que cette puissance atteigne 3 825 MW en 2026 ! Si ce pari pouvait être atteint en 2026, cette hausse de la production permettrait de contribuer à l'augmentation du taux d'accès des populations à l'électricité. Ce taux passerait ainsi de 44 % à 60 % sur la même période, tandis que les pertes techniques et commerciales baisseraient de façon sensible de 54 % à 26 %.

28 https://www.finances.gouv.cg/fr/articles/rencontre-eni, site consulté le 25/10/2024

29 Décret n° 2019-170 du 1er juillet 2019 portant attribution d'une licence de producteur indépendant de l'électricité à la centrale électrique du Congo S.A.

30 Arrêté n° 8656 du 3 mai 2021 portant attribution de la licence d'exportation de l'électricité à la Centrale Electrique du Congo S.A.

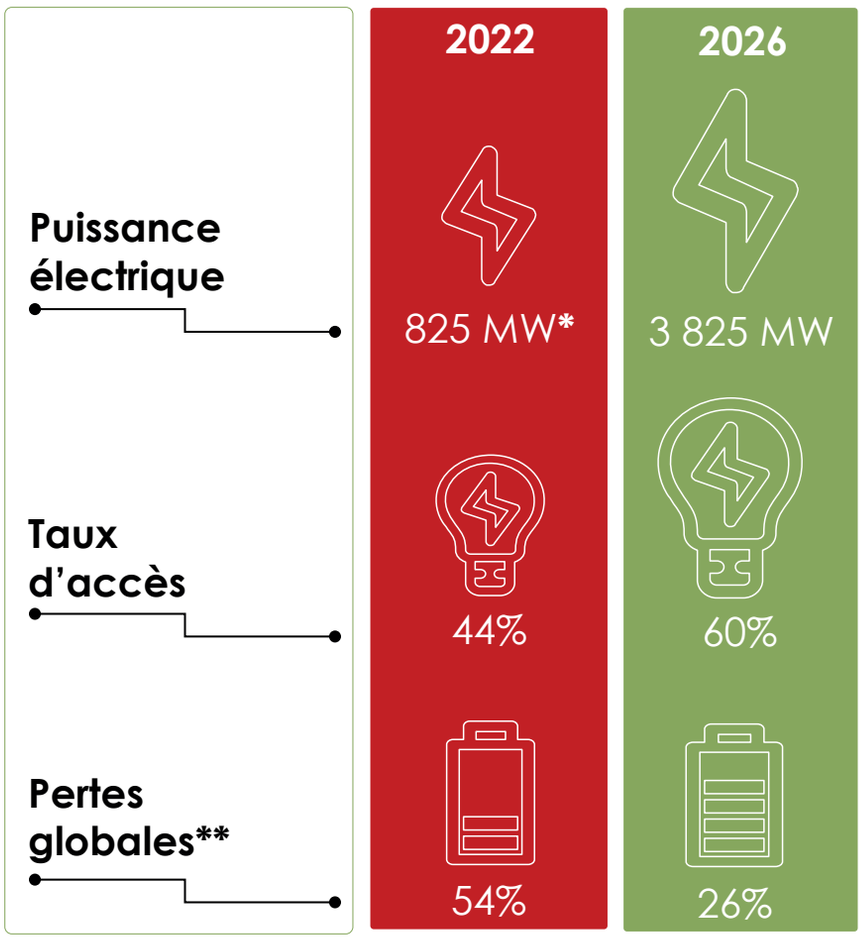
31 https://www.adiac-congo.com/content/energie-la-centrale-electrique-du-congo-passe-de-314-484-megawatts-113021, site consulté

32 https://gouvernement.cg/energie-remise-en-service-de-la-centrale-a-gaz-de-djeno/, site consulté le 25/10/2024

33 Décret n° 2021-450 du 14 septembre 2021 portant approbation du contrat de concession signé le 21 janvier 2021 entre la République du Congo et la société Aksa Energy Compagy Congo S.A.

34 Arrêté n° 871 du 11 mars 2022 accordant une licence provisoire de producteur indépendant de l'électricité à Aksa Energy Company Congo S.A.

Figure 8 : Évolution planifiée de certains indicateurs électriques



** Puissance telle qu'indiquée dans le PND 2022-2026*

*** Techniques et commerciales*

Source : PND 2022-2026

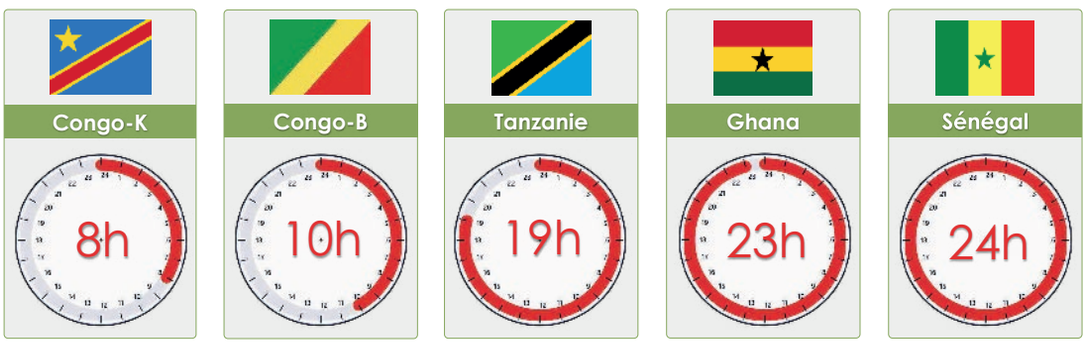
Dans l'éventualité où la puissance installée n'augmenterait pas, et que les infrastructures de transport et de distribution resteraient inchangées, certains défis liés aux communications électroniques et à la transformation numérique ne pourront être résolus qu'à travers des solutions *onéreuses*, comme l'usage de groupes électrogènes.

4.3. Connexion des sites des opérateurs au réseau électrique : enjeux et disparités

Le réseau de distribution électrique n'est pas suffisamment maillé sur l'ensemble du territoire congolais. Par conséquent, tous les sites des opérateurs exerçant dans le secteur des télécommunications ne sont pas directement connectés au réseau électrique. À cause de cette défaillance, les opérateurs de communications électroniques ou leurs contractants sont obligés de produire de l'énergie de façon autonome. Quant aux sites qui sont connectés au réseau électrique, ils ne sont pas épargnés par les délestages. Aussi, des opérateurs tels que MTN, Airtel ou Congo Télécom, pour ne citer que certains des plus importants dans l'écosystème des télécommunications au Congo, doivent s'adapter à cette réalité.

En 2023, Helios Towers[35] Congo gérait 537 sites, un chiffre porté à 550 en 2024. Selon le rapport annuel 2023 de la société Helios Towers Plc[36], la disponibilité quotidienne moyenne du réseau électrique national (E²C) sur un site était de seulement 10 heures[37] en République du Congo.

Figure 9 : Disponibilité moyenne quotidienne du réseau électrique (en heures) sur les sites et par pays



Source : Helios Towers

La figure ci-dessus permet de comparer la fourniture quotidienne d'électricité aux sites des opérateurs de télécommunications. Si le Congo-Kinshasa affiche des résultats inférieurs à ceux du Congo-Brazzaville, des pays comme la Tanzanie, le Ghana et le Sénégal se démarquent nettement. Cependant, comparée à 2023, la disponibilité moyenne au Congo est passée de 8h[38] à 10h par jour en 2024 ; ce qui représente une progression d'environ 25 %.

Ces efforts sont louables, mais encore très insuffisants. En effet, les opérateurs sont contraints de recourir au gasoil qui est une source d'énergie alternative chère et polluante. Quelle est, dans ce cas, la différence de coûts quand les sites sont directement alimentés par le réseau électrique national et par les groupes électrogènes ?

4.4. Impacts des coûts de l'énergie dans le secteur des communications électroniques

Dans le cadre de la transition énergétique et de la maîtrise des coûts opérationnels dans le secteur des communications électroniques, cinq (5) scénarios d'approvisionnement énergétique des sites télécoms ont été modélisés. Ces scénarios intègrent les données techniques de consommation, les coûts énergétiques hors taxes et les évolutions tarifaires, afin d'identifier les leviers d'optimisation des sites télécoms.

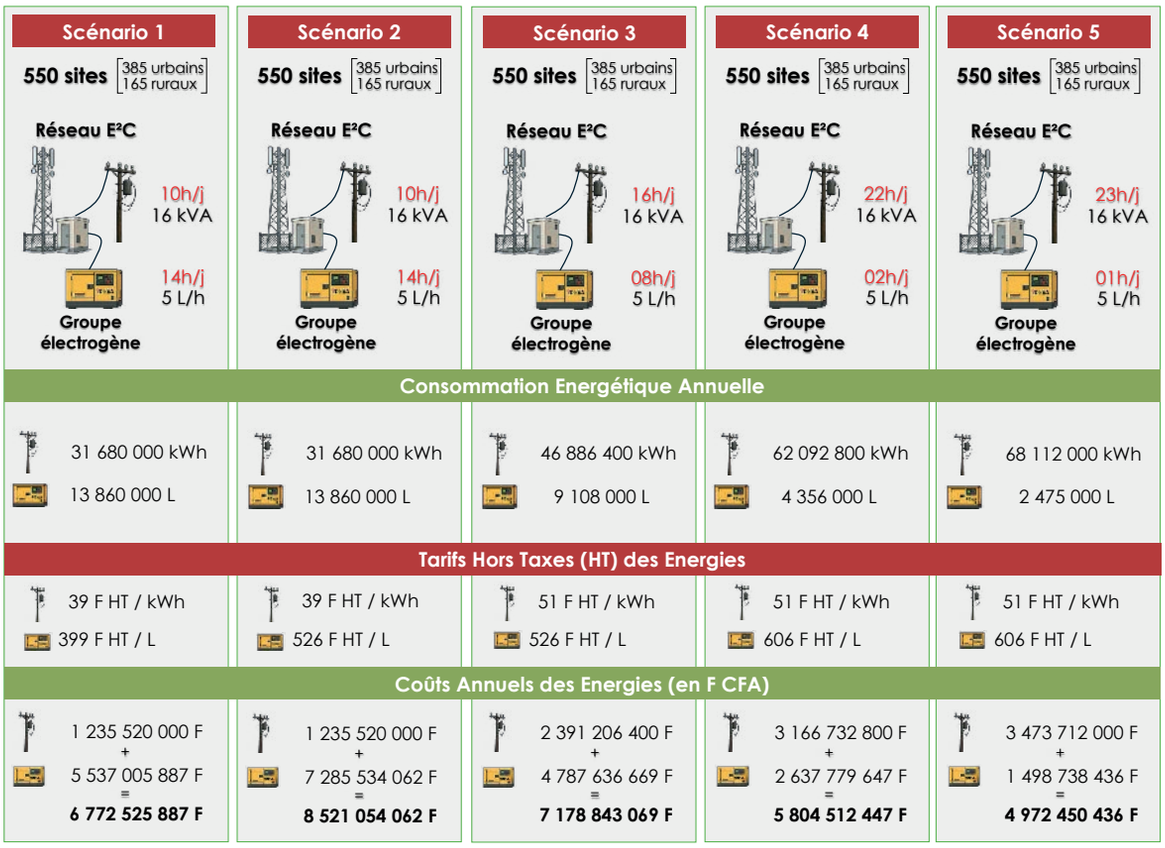
35 Helios Towers est une entreprise indépendante spécialisée dans les infrastructures de télécommunications, opérant en Afrique et au Moyen-Orient. Elle est implantée au Congo et se distingue par la construction, la possession et la gestion de tours de télécommunications. Ces infrastructures jouent un rôle essentiel pour les opérateurs de téléphonie mobile en leur permettant d'assurer une couverture réseau et une connectivité optimale.

36 Elle est la maison-mère de Helios Towers Congo.

37 Helios Towers, *Annual Report and Financial Statements 2024*, p.17.

38 Helios Towers, *Annual Report and Financial Statements 2023*, p.4.

Figure 10 : Scénarios d'alimentation des sites télécoms



Sur 550[39] sites opérés par la société Hélios Towers Congo, l'hypothèse retenue est qu'environ 70 % des sites sont localisés en zones urbaines ; soit 385 sites. Chaque site nécessiterait en moyenne une puissance active de 16 kVA[40] pour fonctionner avec le réseau électrique national. En utilisant des groupes électrogènes, il faudrait environ 5 litres de gasoil par heure pour alimenter ces mêmes sites.

Figure 11 : Évolution du mix et des coûts énergétiques

	Scénario 1	Scénario 2	Scénario 3	Scénario 4	Scénario 5
Tarifs (HT) des Energies					
Coût du kWh (HT)	**39**	**39**	**51**	**51**	**51**
Coût du litre de Gasoil (HT)	**399**	**526**	**526**	**606**	**606**
Évolution Prix kWh (%)	-	-	30,8%	-	-
Évolution Prix Gasoil (%)	-	31,6%	-	15,2%	-
Coûts Annuels Hors Taxes (En Millions)	**6 773**	**8 521**	**7 179**	**5 805**	**4 972**
Evolution par rapport au **scénario 2**	-	-	-16%	-32%	-42%
Part des Coûts dans le Mix Energétique					
Réseau Electrique – RE (kWh)	18%	14%	33%	55%	70%
Groupe Electrogène – GE (Litres)	82%	86%	67%	45%	30%
Ratio RE/GE	**0,22**	**0,17**	**0,50**	**1,20**	**2,32**

39 Des 550 sites gérés par Helios Towers, 263 sont effectivement partagés entre plusieurs opérateurs, favorisant ainsi une optimisation des coûts.

40 [20 kVA X 0,8], avec 0,8 comme facteur de puissance pour des équipements électriques industriels et télécoms.

4.4.1. Scénario 1 : Situation de référence (10h E²C / 14h Diesel)

Dans ce scénario, les sites sont alimentés en moyenne 10 heures par jour par le réseau électrique national, puis pendant 14 heures par les groupes électrogènes de secours des opérateurs de communications électroniques. Cette structure du mix énergétique engendre une dépendance économique au gasoil qui représente 82 % du coût de l'énergie, contre 18 % pour l'électricité. Cela explique la faiblesse du ratio RE/GE (réseau électrique/groupe électrogène), qui s'établit à seulement 0,22.

Sur la base d'une estimation de la consommation énergétique selon la répartition des sites entre zones rurales et urbaines, le coût global annuel pour 550 sites est évalué à 6,77 milliards F CFA, avec des tarifs unitaires HT de 39 F/kWh pour l'électricité et 399 F/litre pour le gasoil. Ainsi, malgré un coût unitaire du kWh relativement bas, le coût énergétique global demeure très élevé en raison de la prédominance du diesel dans le mix énergétique.

Le prix du gasoil retenu dans ce scénario correspond à celui en vigueur avant la hausse généralisée des prix des carburants en 2023.

4.4.2. Scénario 2 : Mix énergétique du scénario 1 avec hausse du prix du diesel

Bien que les paramètres techniques restent inchangés dans ce deuxième scénario, le prix du gasoil a augmenté de 31,6 %, passant à 526 F/litre HT. Cette évolution se traduit par une facture énergétique annuelle de 8,52 milliards de F CFA, en hausse de 26 % par rapport au premier scénario.

De ce fait, la structure des coûts se déséquilibre, et la part du diesel dans le mix énergétique atteint 86 %, contre seulement 14 % pour l'électricité fournie par le réseau électrique. Cette répartition économique impacte également le ratio RE/GE qui se détériore davantage, passant de 0,22 à 0,17.

Ce scénario met en lumière la vulnérabilité financière du modèle ainsi que sa dépendance critique à une ressource particulièrement onéreuse. Étant le plus proche de la réalité, il servira de référence pour les trois scénarios suivants.

4.4.3. Scénario 3 : Transition partielle vers l'électrique (16h E²C / 8h Diesel)

À partir du troisième scénario, la modélisation se base sur différentes hypothèses, notamment l'amélioration de la fourniture électrique qui se traduit par une disponibilité du réseau qui passe à 16 heures par jour. Le recours aux groupes électrogènes est ainsi limité à 8 heures par jour. Par contre, le tarif de l'électricité augmente à 51 F/kWh, soit une hausse de 30,8 % par rapport au deuxième scénario.

Malgré la hausse du tarif de l'électricité, le coût total annuel baisserait de 16 % pour atteindre 7,18 milliards de F CFA. Le diesel représenterait alors 67 % du coût global, contre 33 % pour l'électricité. Cette évolution se traduirait par une nette amélioration du ratio RE/GE, qui atteindrait 0,50 contre 0,17 dans le scénario précédent.

Ces hypothèses montrent que l'amélioration du mix énergétique compense l'augmentation du tarif électrique, et que la transition vers un plus grand approvisionnement par le réseau électrique serait une stratégie efficace pour réduire les coûts énergétiques des opérateurs.

4.4.4. Scénario 4 : Réseau quasi continu (22h E²C / 2h Diesel)

Dans le quatrième scénario, les sites seraient alimentés par le réseau électrique pendant 22 heures par jour, ne recourant aux groupes électrogènes que pendant deux (02) heures. Cette configuration permettrait une forte réduction de la consommation de gasoil, malgré une augmentation supplémentaire de 15,2 % du prix du gasoil qui s'établirait à 606 F/litre HT.

Par rapport au scénario 2 qui sert de référence, les coûts annuels baisseraient de 32 % pour atteindre 5,80 milliards de F CFA. L'électricité représenterait désormais 55 % du coût énergétique total contre 45 % pour le diesel. Ainsi, le ratio RE/GE progresserait fortement pour atteindre 1,20.

Ce scénario montre qu'une électrification soutenue à l'échelle nationale permettrait de réduire à la fois la dépendance aux fluctuations du prix du gasoil et la facture énergétique globale des opérateurs.

4.4.5. Scénario 5 : Optimisation quasi-maximale (23h E²C / 1h Diesel)

Enfin, le cinquième scénario correspondrait au modèle optimal. Les sites seraient alimentés par l'électricité du réseau électrique pendant 23 heures par jour, avec un recours très marginal au diesel pendant une (01) heure.

Malgré le maintien de prix élevés de l'électricité et du gasoil, la facture énergétique annuelle baisserait de 42 % par rapport au scénario de référence, pour s'établir à 4,97 milliards de F CFA. L'électricité représenterait désormais 70 % du coût global du mix énergétique, contre 30 % pour le diesel. Le ratio RE/GE atteindrait 2,32, soit le plus élevé de l'ensemble des scénarios étudiés.

Ce scénario représente l'option la plus aboutie car il réduit la facture énergétique, limite fortement l'usage du diesel, et s'aligne sans conteste avec les priorités de transition énergétique.

4.4.6. Résumé des scénarios : quelles leçons en tirer ?

L'analyse comparée de ces cinq (5) scénarios montre que la dépendance au gasoil constitue un handicap majeur pour la soutenabilité financière du secteur en raison de son importance dans la structure des coûts (scénarios 1 et 2). Par contre, les hypothèses prospectives, *qui dépendent d'une mise en œuvre accélérée de la matérialisation de la politique énergétique du Congo*, montrent qu'il est possible de baisser la facture énergétique du secteur de façon considérable (scénarios 3 à 5).

Le ratio RE/GE constitue un indicateur de maturité énergétique important à observer. En effet, sa progression de 0,17 à 2,32, en fonction des scénarios, reflète l'optimisation du modèle économique et énergétique du secteur. Plus ce ratio est élevé, plus les sites des opérateurs sont alimentés par une source stable, économique et moins polluante.

On ne saurait donc imaginer une baisse importante des tarifs dans le secteur des communications électroniques si la structure des coûts du mix énergétique actuel ne suit pas une tendance similaire à celle du scénario 5. Mais il s'agit d'un enjeu politique sur lequel les acteurs du secteur des télécommunications n'ont aucune prise.

En somme, la fourniture continue d'une énergie électrique de qualité est donc indispensable au plein essor des réseaux de télécommunications, et notamment des technologies émergentes. Sans une infrastructure énergétique fiable, le Congo risquerait de ne pas bénéficier de tout le potentiel qu'elles pourraient offrir.





V INFRASTRUCTURES DE COMMUNICATIONS ÉLECTRONIQUES

Le développement de l'économie numérique repose sur une *connectivité* fiable, une *transmission* rapide des données et des *plateformes numériques* performantes. Les infrastructures de communications électroniques et numériques dont dispose actuellement la République du Congo sont ou seront-elles suffisantes pour soutenir sa transformation numérique ?

5.1. Cartographie actuelle des infrastructures de communications électroniques

Les infrastructures ci-après constituent l'ossature actuelle du réseau national de communications électroniques, ainsi que du développement de l'économie numérique en République du Congo :

- **Les câbles sous-marins WACS et 2Africa**

La connectivité internationale est un facteur clé de l'économie numérique. Les câbles sous-marins WACS (West Africa Cable System) et 2Africa (de Meta) permettent une connexion à haut débit avec le reste du monde.

- **Les stations d'atterrage de Congo Télécom et d'Airtel Congo**

Les stations d'atterrage de Congo Télécom et d'Airtel Congo jouent un rôle important dans l'écosystème numérique du pays. Elles assurent la réception des câbles sous-marins afin de garantir une connectivité internationale stable et performante.

- **Le backbone en fibre optique entre Pointe-Noire et Ouesso**

L'interconnexion nationale s'effectue via un backbone en fibre optique, essentiel pour relier les principales zones urbaines et rurales. Il contribue ainsi à l'amélioration de la couverture réseau, tout en favorisant la diffusion rapide des services numériques à travers le pays. Il constitue l'épine dorsale des télécommunications nationales et transfrontalières. Son rôle est pivotal dans le développement de l'économie numérique au Congo.

- **Les réseaux 2G/3G/4G/5G des opérateurs de téléphonie mobile**

La téléphonie mobile demeure le premier canal d'accès à Internet pour une grande partie de la population congolaise. Les réseaux 4G et 5G, notamment, garantissent actuellement cette connectivité qui favorise, parmi d'autres, le développement du commerce électronique et des services financiers numériques.

- **Les liaisons transfrontalières en fibre optique et en faisceaux hertziens**

L'interconnexion régionale est indispensable pour renforcer l'intégration économique et la collaboration numérique entre pays voisins (CEMAC), y compris au sein de l'espace CEEAC. Les liaisons transfrontalières, plus spécifiquement en fibre optique, ont pour objectif de favoriser une meilleure fluidité du trafic des données et des transactions numériques sécurisées.

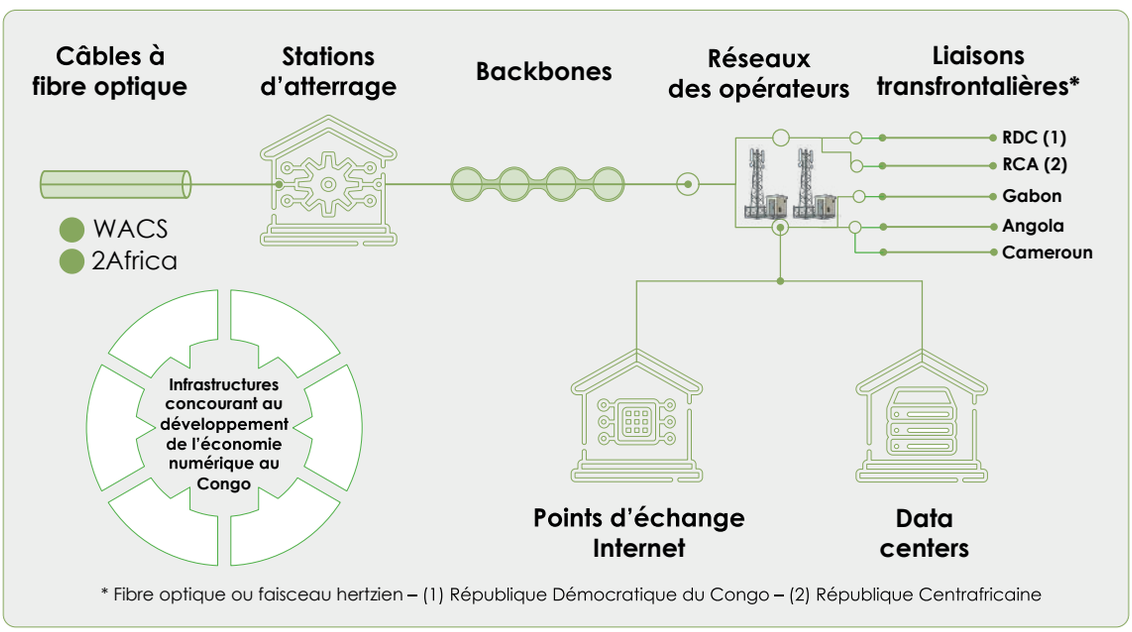
▶ Les data centers : hébergement et sécurité des données

Avec la numérisation des services publics et privés, les data centers sont devenus un élément clé de l'économie numérique à travers le monde. Le Congo n'échappe pas à cette tendance. Ces infrastructures garantissent un hébergement sécurisé des données, soutiennent les applications et devraient contribuer, autant que possible, à une forme de souveraineté numérique au Congo.

▶ Les points d'échange Internet de Brazzaville et Pointe-Noire (CGIX)

Les deux (2) points d'échange Internet du Congo jouent un rôle important dans l'amélioration des performances et de la résilience des réseaux numériques nationaux. Les CGIX peuvent s'apparenter à une forme d'Intranet à l'échelle nationale dans lequel le trafic s'échange en local ; ce qui permet de garantir une certaine indépendance du réseau national en cas de rupture des câbles WACS ou 2Africa, par exemple.

Figure 12 : Cartographie des principales infrastructures télécoms de l'économie numérique



* Fibre optique ou faisceau hertzien – (1) République Démocratique du Congo – (2) République Centrafricaine

5.2. Prérequis stratégiques pour les technologies futures de communications électroniques au Congo

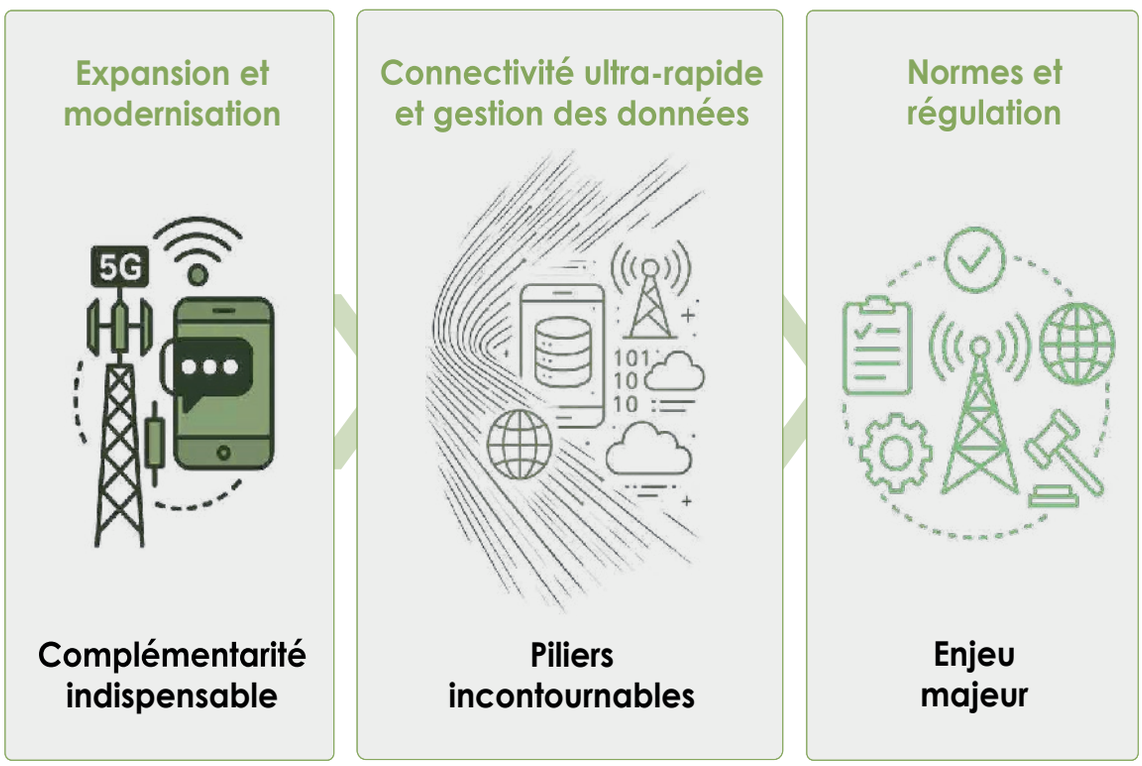
L'essor de l'économie numérique repose sur une vision stratégique globale, alliant *expansion* et *modernisation* des infrastructures pour relever les défis liés à la *connectivité* et à la *gestion des données*. Sans une connectivité à la pointe de la technologie, un pays comme le Congo risquerait de ne pas bénéficier des avancées technologiques majeures portées par des entreprises innovantes telles que Microsoft, Meta, Nvidia ou Neuralink.

Aujourd'hui, la connectivité ultra-rapide et l'optimisation de la gestion des données sont des piliers essentiels du développement numérique. Ces évolutions s'appuient sur des normes et standards de plus en plus complexes qui nécessitent une régulation adaptée afin de préserver au mieux les intérêts des Etats.

Le Congo devrait donc anticiper les évolutions technologiques et les adapter au contexte local afin de devenir un acteur clé de son propre développement numérique. Bien que l'écart technologique avec les pays industrialisés soit significatif, les innovations développées par ces puissances, combinées au génie congolais, offrent une occasion unique pour assurer une mise en œuvre souveraine de solutions numériques locales.

En résumé, le Congo ne pourra pas échapper à cette dynamique mondiale qui repose à minima sur trois axes stratégiques majeurs ; ce que décrit la figure ci-après.

Figure 13 : Prérequis stratégiques pour le déploiement des technologies émergentes



5.2.1. Expansion et modernisation : une complémentarité indispensable

L'expansion permet d'étendre la couverture des réseaux aux zones moins connectées ; *l'inclusion numérique en dépendra.* Cette expansion devra aussi tenir compte des technologies non terrestres, parmi d'autres.

La modernisation garantit que les infrastructures restent performantes face aux nouvelles exigences technologiques. *Le cadre légal devra, tout en veillant aux intérêts nationaux, favoriser les investissements des acteurs numériques au Congo.*

5.2.2 Connectivité ultra-rapide et gestion des données : des piliers incontournables

La connectivité ultra-rapide devra garantir une transmission instantanée des données, notamment pour les services exigeant une faible latence. *Ce sera une des conditions à remplir pour soutenir les efforts d'innovation technologique et numérique, mais aussi d'accélération de la transformation digitale du pays.*

La gestion des données dépend de leur collecte, traitement et stockage. La maîtrise de *chacun de ces maillons de la chaîne de valeur, lorsqu'elle sera possible, permettra de jouer un rôle clé dans le processus de souveraineté numérique en République du Congo.*

5.2.3. Normes et régulation : un enjeu majeur pour les régulateurs

L'évolution rapide des technologies rend les standards plus complexes ; ce qui nécessite une harmonisation internationale pour assurer leur compatibilité et leur adoption. *Des normes ouvertes et partagées sont essentielles pour éviter une fragmentation*[41] *des systèmes et favoriser l'intégration des innovations.*

La régulation doit également évoluer pour encadrer les technologies émergentes, ainsi que l'usage des données afin qu'elle s'adapte aux nouveaux modèles économiques numériques. *Elle joue un rôle clé dans la protection des utilisateurs, la gestion des infrastructures critiques et le maintien d'un équilibre entre innovation et contrôle, parmi d'autres.*

La maîtrise des normes et de la régulation du futur constitue un outil stratégique **fondamental** pour encadrer et contribuer à la transformation numérique du Congo en s'appuyant, sans que la liste ne soit exhaustive, sur les fondements suivants :

1. Alignement international

S'aligner sur les standards de l'Union Internationale des Télécommunications (UIT) et autres organismes pour éviter l'isolement technologique. Ce qui passera par l'adoption de normes techniques communes afin de garantir la compatibilité entre *équipements, opérateurs et services.* Cela facilitera, par exemple, l'importation de matériel certifié.

2. Neutralité technologique

Adopter des règles qui ne favorisent pas une technologie spécifique afin de permettre aux opérateurs de choisir la solution la plus adaptée en fonction de leurs activités. Cela encouragera l'innovation et la concurrence.

3. Gestion du spectre

Attribuer et surveiller l'utilisation des fréquences radio de manière équitable et efficace. Une bonne régulation du spectre des fréquences contribuera à réduire ou éviter les interférences ; ce qui permettra d'optimiser l'exploitation de cette ressource rare (limitée).

4. Qualité de service (QoS)

Imposer des indicateurs mesurables (débit, latence, disponibilité) pour éviter une dégradation des services, notamment à l'ère du numérique où les ruptures de service engendrent souvent de graves conséquences (financières, sanitaires, économiques, etc.). Ces obligations contribueront à renforcer la confiance des usagers, ainsi que la compétitivité du marché.

41 L'adoption de normes différentes par les entreprises et/ou les développeurs peut faire que des technologies ne communiquent pas entre-elles. Ces incompatibilités pourraient contrevenir aux innovations technologiques.

5. Sécurité des réseaux

Établir des règles strictes de cybersécurité pour protéger les réseaux contre les cyberattaques. Une régulation claire garantit la résilience des infrastructures critiques et la confidentialité des données.

6. Inclusion numérique

Fixer des obligations de couverture et du type de technologie minimum pour réduire la fracture numérique, notamment dans les zones rurales. Des normes minimales doivent garantir l'accès universel aux communications électroniques, de même qu'aux services numériques.

7. Protection du consommateur

Protéger les usagers contre les abus tarifaires et l'exploitation de leurs données personnelles par une régulation qui soit la plus efficace possible. Les opérateurs et les administrations devront respecter la transparence contractuelle et garantir l'accessibilité permanente aux services dans un monde où les données à caractère personnel ou stratégiques seront davantage gérées et stockées par des plateformes ou administrations puissantes.

8. Attractivité pour les investisseurs

Garantir un cadre réglementaire stable et prévisible afin d'attirer les investissements étrangers et locaux. La clarté sur l'attribution des licences et leurs procédures, ou le paiement des taxes, par exemple, contribuera à réduire le risque pays.

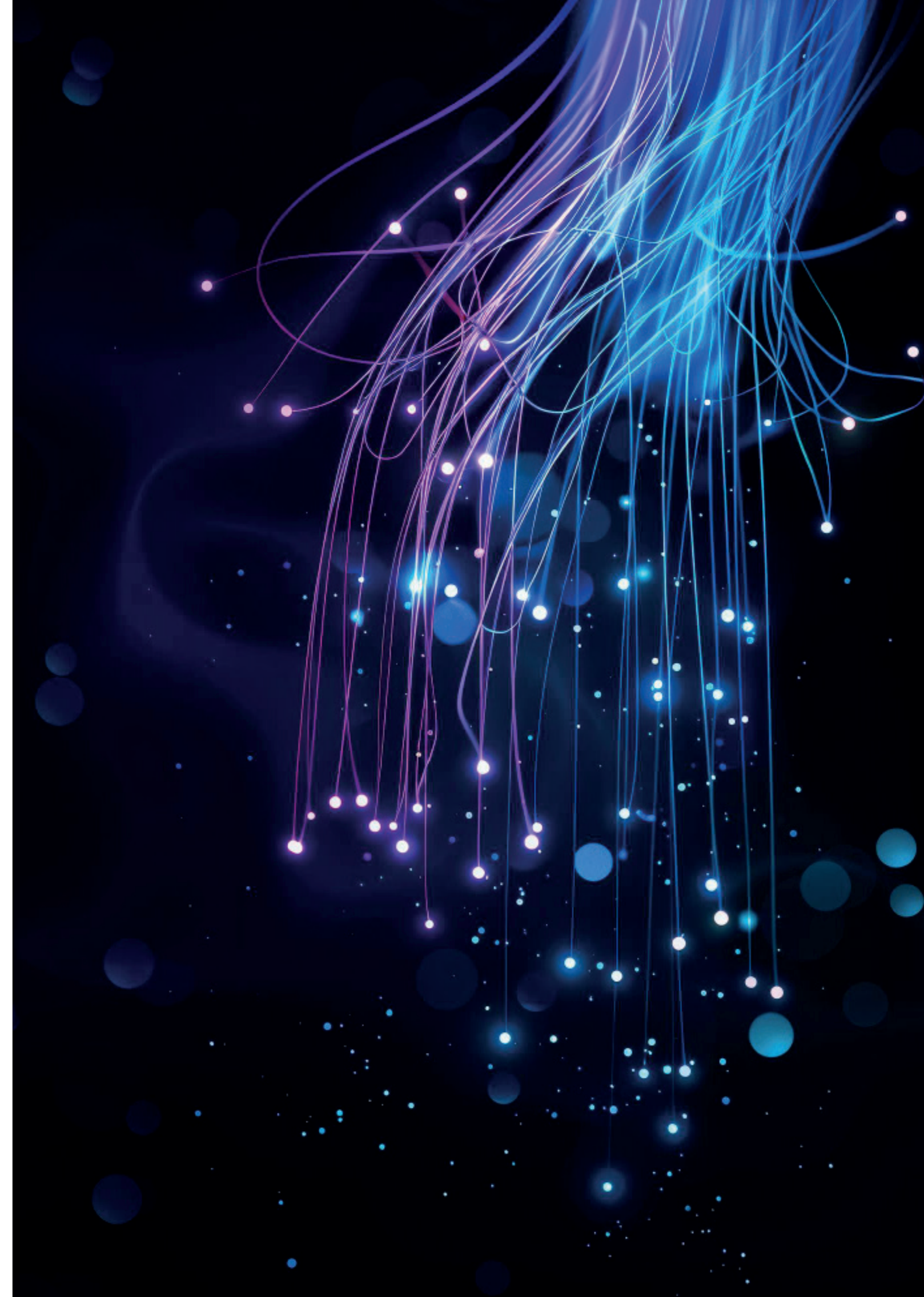
9. Préparation aux technologies 5G et au-delà

Anticiper les besoins normatifs pour intégrer rapidement la 5G, l'IoT et les futures évolutions technologiques. Cela inclut la modernisation des infrastructures et la mise à jour des licences d'exploitation des opérateurs. C'est pourquoi la modernisation des infrastructures constitue bien un axe stratégique majeur.

La figure ci-après résume les 9 fondements, cités supra, en lien avec certaines normes qui influent sur la régulation des technologies émergentes.

Figure 14 : Quelques fondamentaux de la régulation numérique







VI TECHNOLOGIES DE NOUVELLE GÉNÉRATION : QUELS ENJEUX POUR LE CONGO ?

Les technologies de nouvelle génération ouvrent la voie à une transformation profonde des infrastructures et des usages numériques. Cette section examine les enjeux spécifiques pour le Congo, depuis la 5G jusqu'aux réseaux non terrestres, en abordant les aspects techniques, spectraux et économiques, ainsi que les contraintes et le gap technologique à surmonter.

6.1. Les technologies 5G

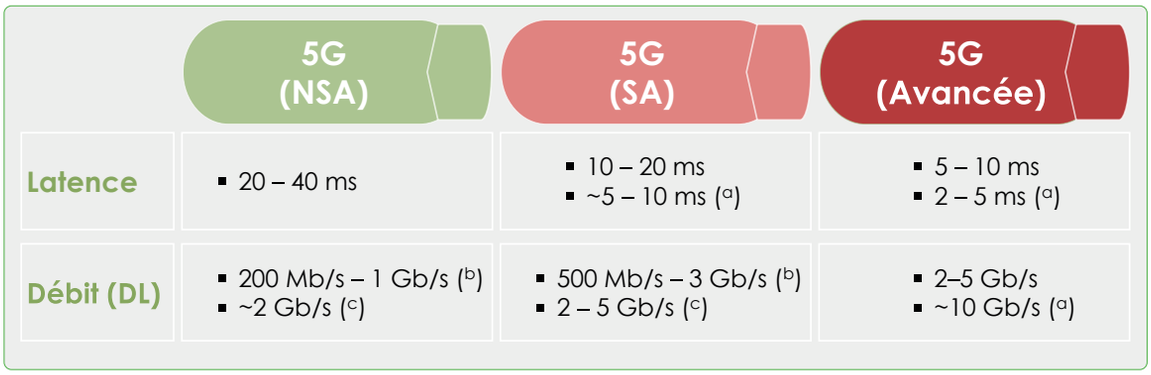
La 5G[42] est en cours de déploiement et transforme déjà la connectivité mondiale grâce à des vitesses nettement améliorées et des temps de latence réduits. Toutefois, une latence réduite ne signifie pas son absence totale. La 5G ne se limite pas, non plus, à une simple évolution des réseaux mobiles ; elle représente un écosystème technologique regroupant diverses caractéristiques et intégrant des services innovants. On distingue les évolutions suivantes :

- **la 5G NSA (Non-Standalone)** qui désigne une architecture de transition dans laquelle l'accès radio repose sur la technologie 5G, tandis que la gestion du trafic et des services continue de s'appuyer sur le cœur de réseau 4G. En termes plus simples, la 5G NSA est une 5G où les données passent par des antennes 5G, tandis que le cœur de réseau reste en 4G. La latence de la 5G NSA est comprise entre 20 et 40 millisecondes (ms), alors que les débits peuvent varier entre 200 Mb/s et 2 Gb/s. A date, le Congo n'a déployé que la 5G NSA ;
- **la 5G SA (Standalone)** qui fonctionne sur une infrastructure complètement 5G (les antennes et le cœur de réseau sont en 5G). La latence estimée de la 5G SA est comprise entre 5 et 20 millisecondes (ms), alors que la vitesse de transmission (débit) est comprise entre 500 Mb/s et 5 Gb/s ;
- **la 5G A (Advanced)** qui est une évolution de la 5G SA. Elle apporte des optimisations en termes de capacité, d'efficacité énergétique, de fiabilité et de couverture, tout en intégrant des fonctionnalités avancées telles que l'intelligence artificielle (IA) native au réseau, la communication étendue vers l'Internet des Objets (IoT) et la préparation progressive aux cas d'usage de la 6G. La latence est comprise entre 2 et 10 millisecondes (ms), alors que la vitesse de transmission (débit) est comprise entre 2 et 10 Gb/s.

La figure ci-après résume les évolutions de la 5G, de la moins performante à la plus avancée, avec la latence comme critère de sélection incrémentale. *Toutefois, certaines des caractéristiques fournies demeurent globalement théoriques.*

42 https://www.carnot-tsn.fr/focus-5g-6g-de-la-5g-vers-la-6g-linexorable-avancee-des-generations/, site consulté le 25/04/2025.

Figure 15 : Évolutions des technologies 5G



(a) optimisée – (b) Sub-6 – (c) mmWave

Sources : MDPI[43] - Journal of Artificial Intelligence & Cloud Computing[44] - Private LTE & 5G[45] - TeleGraphic[46] - GSMA[47] - Nokia[48]

6.2. Les technologies 6G

La 6G est encore en phase de recherche et de développement. Son déploiement favorisera une intégration plus avancée des technologies immersives comme l'intelligence artificielle (IA), l'Internet des objets (IoT) et le métavers. Les caractéristiques ci-après sont, pour la plupart, théoriques. Toutefois, on distingue les évolutions suivantes :

- **La 6G NTN (satellites/HAPS)** qui utilisera des satellites et autres systèmes non terrestres pour compléter la couverture des réseaux mobiles afin d'offrir une connectivité ubiquitaire (notamment dans les zones rurales, maritimes, etc.). Les débits devraient être compris entre 10 et 280 Mb/s, tandis que la latence serait comprise entre 10 – 60 millisecondes (ms) ;
- **La 6G IA** qui intègrera l'intelligence artificielle pour optimiser automatiquement le fonctionnement d'un réseau de communication électronique. Il s'agira d'un réseau ultra-efficace, donc à même de s'adapter automatiquement aux besoins des utilisateurs et aux évolutions technologiques. La latence devrait varier entre 1 et 5 millisecondes (ms). Quant aux débits escomptés, ils devraient être supérieurs à 10 Gb/s ;
- **La 6G Advanced (ou Avancée)** qui correspondra à l'évolution des versions antérieures ou de base (NTN, IA). Grâce à une latence plus faible, des débits plus élevés, la 6G Avancée permettra d'introduire les communications immersives (réalité étendue, holographie, etc.) On pourrait retenir que la 6G Avancée regroupera la 6G holographique ou tactile (communications immersives et en

43 https://www.mdpi.com/2079-9292/11/11/1736, site consulté le 23/05/2025.

44 https://onlinescientificresearch.com/articles/a-comparative-study-of-mmwave-vs-sub6-ghz-5g-networks-for-urban-environments.pdf, site consulté le 23/05/2025.

45 https://www.privatelteand5g.com/the-rise-of-5g-standalone-networks-and-their-game-changing-capabilities/, site consulté le 23/05/2025.

46 https://www.telegraphic.jp/en/2023/12/246/, site consulté le 23/05/2025.

47 https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/gsma-5GmmWave-guide-a-resource-for-operators.pdf, site consulté le 23/05/2025.

48 https://www.nokia.com/mobile-networks/monetization/5g-advanced/5g-advanced-explained/, site consulté le 23/05/2025.

temps réel) et la 6G quantique (sécurité et traitements des données basés sur les technologies quantiques). C'est pour cette raison que les débits devraient varier entre 10 et 100 Gb/s, avec une latence comprise entre 1 et 2 millisecondes (et possiblement inférieure à 1 ms).

La figure ci-après résume les évolutions envisagées de la 6G, de la moins performante à la plus avancée, notamment en termes de latence.

Figure 16 : Évolutions des technologies 6G

	6G (NTN)	6G (IA)	6G (Avancée)
Latence	▪ 20 – 60 ms (1) ▪ 10 – 20 ms (2)	▪ 1 – 5 ms	▪ ≤1 – 2 ms
Débit (DL)	▪ 45 – 280 Mb/s (1) ▪ 10 – 100 Mb/s (2)	▪ >10 Gb/s	▪ 10 – 100 Gb/s

(1) LEO -- (2) HAPS

Sources : 3GPP[49] - Nokia[50] - Arxiv[51] - Ericsson[52] - Huawei[53]

6.3. Les réseaux non terrestres (NTN)[54]

Les Non-Terrestrial Networks (NTN) ou réseaux non terrestres intègrent des infrastructures spatiales (satellites en orbite LEO[55], MEO[56], GEO[57]) et stratosphériques, notamment les HAPS[58] (drones, ballons, dirigeables). Ces réseaux ont pour vocation d'offrir une connectivité globale.

L'adoption des NTN permet déjà de surmonter plusieurs obstacles en réponse aux défis de connectivité dans de nombreux pays. Pour rappel, le développement d'une économie ou d'une société numérique passe par une *connectivité optimale*. C'est la raison pour laquelle toutes les technologies ou réseaux de communication électronique ont pour but d'améliorer la connectivité.

49 https://www.3gpp.org/technologies/ntn-overview, site consulté le 23/05/2025.

50 https://www.nokia.com/6g/spectrum-for-6G-explained/, site consulté le 23/05/2025.

51 https://arxiv.org/pdf/2310.06425, site consulté le 23/05/2025.

52 https://www.ericsson.com/en/6g/spectrum/sub-thz, site consulté le 23/05/2025.

53 https://www.huawei.com/en/huaweitech/future-technologies/performance-requirements-evaluation-methodology-ai-6g, site consulté le 23/05/2025.

54 https://www.keysight.com/us/en/cmp/topics/non-terrestrial-network-basics-advantages-and-challenges.html, site consulté le 15/05/2025.

55 Low Earth Orbit pour Orbite Basse.

56 Medium Earth Orbit pour Orbite Moyenne.

57 Geostationary Earth Orbit pour Orbite Géostationnaire.

58 High-Altitude Platform Station ou Station de Plateforme à Haute Altitude.

Malgré certaines résistances liées aux coûts d'investissement et aux défis réglementaires, il semble difficile d'imaginer un écosystème numérique pleinement fonctionnel à l'échelle planétaire sans NTN dans un futur très proche. Leur *intégration progressive* aux réseaux terrestres devrait d'ailleurs constituer la clé d'une transformation numérique inclusive et durable.

Aussi, la République du Congo, à l'instar de la République Démocratique du Congo, devrait bientôt tirer profit des NTN pour accélérer son développement numérique avec des autorisations encadrées d'acteurs comme Starlink, OneWeb, etc. En effet, les réseaux non terrestres offrent les avantages suivants :

- **une connectivité étendue (accès universel)**

Les NTN permettent d'apporter l'Internet haut débit et des services de télécommunications dans des zones reculées où les infrastructures terrestres ou classiques sont limitées ;

- **un développement économique et numérique**

En intégrant les NTN, le Congo pourrait stimuler l'innovation technologique, attirer des investissements et développer des services numériques adaptés, notamment le commerce et les services en ligne ;

- **une amélioration des services publics**

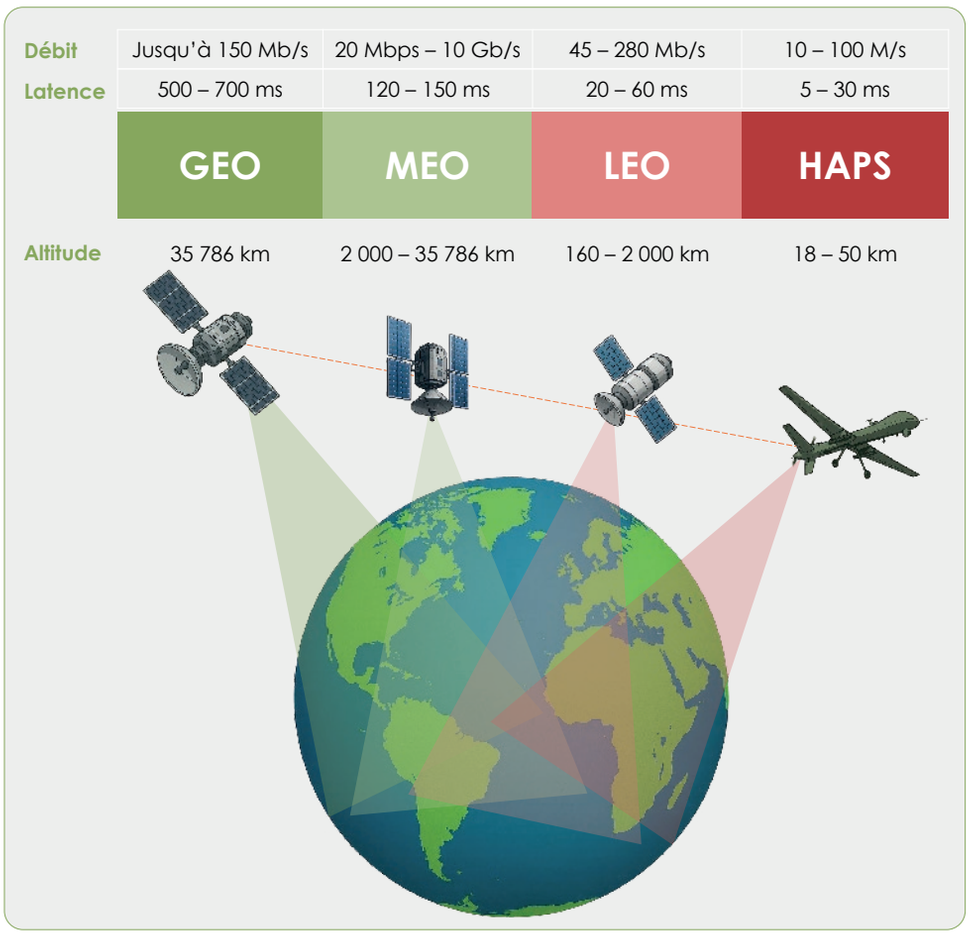
Les NTN pourraient, par exemple, jouer un rôle important dans la télémédecine. Ainsi, les populations localisées dans des zones mal ou peu desservies en infrastructures sanitaires pourraient accéder aux soins médicaux grâce aux consultations à distance. En cas de catastrophe naturelle également, comme le Congo en a connu, notamment dans le Septentrion, les NTN pourraient contribuer à renforcer leur gestion.

Lors de pannes réseau ou de coupures de services terrestres ou maritimes (câbles à fibre optique), les NTN devraient augmenter la capacité de résilience des réseaux et garantir une continuité de service indispensable au bon fonctionnement d'une économie numérique ;

- **un support aux nouvelles technologies**

L'essor du métavers, de l'IoT, de l'IA ainsi que de la réalité virtuelle (RV) et augmentée (RA) repose sur le traitement de données massives et une latence minimale. Les NTN, notamment les satellites LEO et les plateformes stratosphériques HAPS, offrent une alternative efficace aux infrastructures terrestres en garantissant une connectivité haut débit sans nécessiter l'installation coûteuse et lente d'infrastructures réseau à fibre optique.

Figure 17 : Description générale des NTN



Sources : UIT[59] – HAPS Alliance[60] – Starlink[61] – BusinessCom[62] – Hughes[63]

En somme, les NTN, via les réseaux LEO et HAPS, complètent les réseaux terrestres qui contribueront au soutien des technologies émergentes. Leur intégration dans l'architecture 6G NTN permettra de maximiser leur potentiel en assurant une qualité de service homogène et une interopérabilité efficace.

6.4. Quelles bandes de fréquences au Congo pour chaque technologie

La planification des bandes de fréquences radioélectriques est une des clés qui permet le déploiement des technologies de télécommunications. En République du Congo, les technologies déployées pour la **téléphonie mobile** sont la 2G, 3G, 4G et 5G (notamment la 5G NSA, à date). Le tableau suivant présente les bandes de fréquences assignées pour chaque technologie de téléphonie mobile. Afin de ne pas être en marge des évolutions technologiques, certaines bandes de fréquences ont été réservées pour le déploiement futur des technologies comme la 6G.

59 https://www.itu.int/hub/2023/01/satellite-regulation-leo-geo-wrs/, site consulté le 19/05/2025.

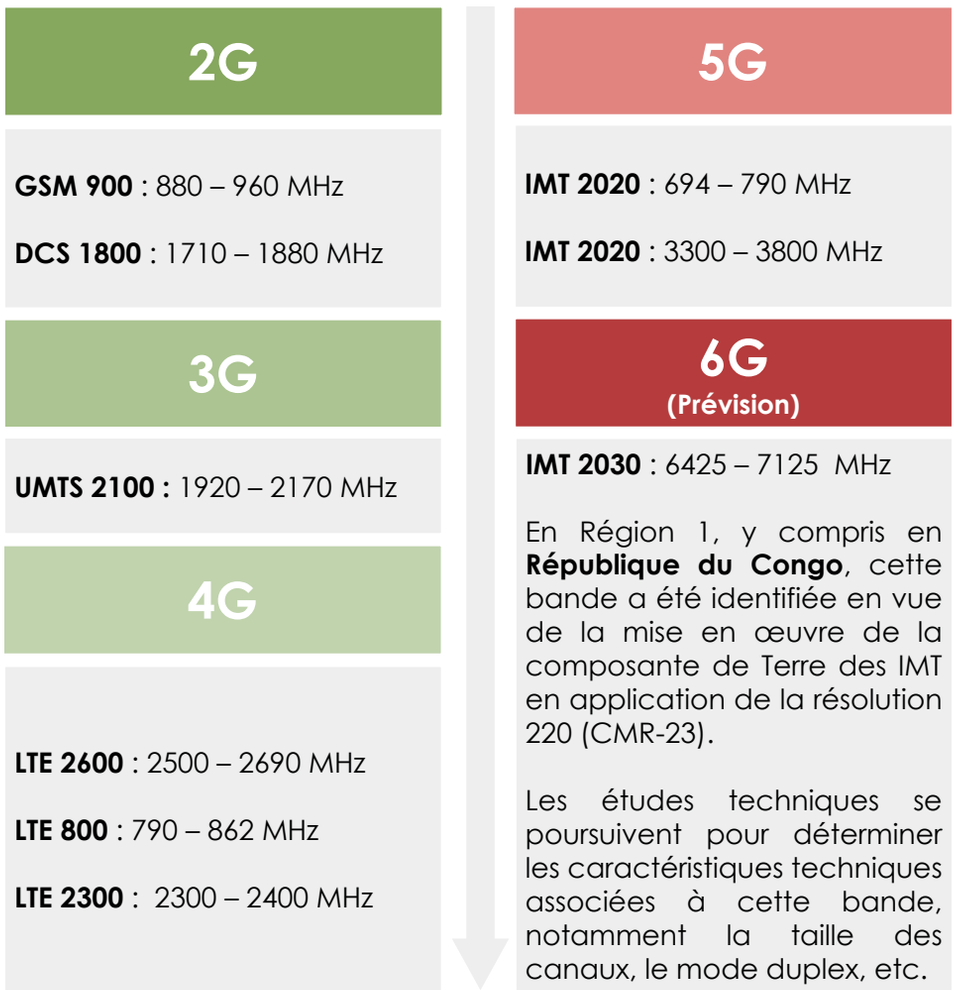
60 https://hapsalliance.org/blog/the-importance-of-haps-in-connecting-the-world-from-the-skies/, site consulté le 19/05/2025.

61 https://www.starlink.com/legal/documents/DOC-1470-99699-90, site consulté le 24/08/2025.

62 https://www.bcsatellite.net/blog/o3b-mpower-advances-with-successful-end-to-end-rf-testing/, site consulté le 24/08/2025.

63 https://www.hughes.com/what-we-offer/satellite-internet, site consulté le 24/08/2025.

Figure 18 : Ressources spectrales pour les réseaux d'accès des opérateurs de téléphonie mobile et autres services innovants



Sources : ARPCE - UIT

Les communications satellitaires ont toujours joué un rôle important dans les télécommunications mondiales. Avec l'amélioration et la baisse des coûts de déploiement des câbles à fibre optique, la majorité des communications électroniques transitent aujourd'hui par ces réseaux terrestres et sous-marins. Toutefois, le déploiement de nouvelles constellations de satellites, plus rapides et à moindre latence, repositionne cette technologie comme un complément stratégique, notamment pour les zones non desservies par la fibre.

La République du Congo a enregistré et réservé des ressources satellitaires afin qu'elle tire avantage des avancées technologiques en cours de développement. C'est ce que résume le tableau ci-dessous.

Figure 19 : Ressources satellitaires (orbite/spectre) enregistrées et réservées pour la République du Congo

GEO	
AP30/30A **(Radiodiffusion par satellite)** **Position orbitale : 37.3°W** 11,7 - 12,5 GHz 17,3 - 18,1 GHz	**AP30B** **(Fixe par satellite)** : **Position orbitale : 16.35°W** **Bande C** 4500 - 4800 MHz 6725 - 7025 MHz **Bande Ku** 10,70 - 10,95 GHz 11,20 - 11,45 GHz 12,75 - 13,25 GHz

MEO	LEO	HAPS
A la demande	**A la demande**	31 - 31,3 GHz 38 - 39,5 GHz 47,2 - 47,5 GHz 47,9 - 48,2 GHz

Source : ARPCE

6.5. Déploiements et usages futurs des technologies émergentes

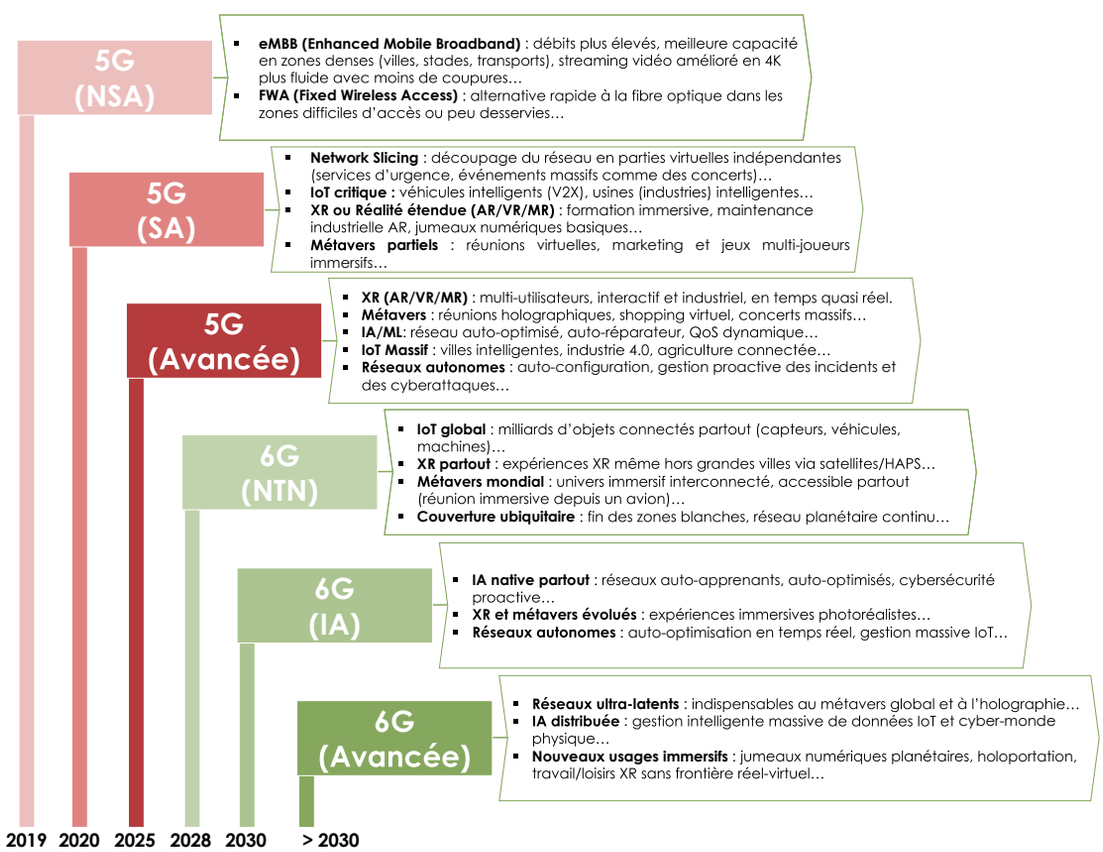
Pour anticiper les besoins futurs du Congo en relation avec les technologies émergentes et leurs usages, il est nécessaire de commencer par comprendre l'évolution de ces technologies dans le temps, et les usages qui sont prévus de la part des équipementiers. La période utilisée à cet effet dans la figure ci-dessous commence en 2019 et s'étend au-delà de 2030.

- Dès **2019**, la technologie **5G NSA** s'est répandue à travers le monde, notamment dans les pays avancés ou « développés ». Cette technologie a montré, par exemple, qu'elle pouvait, grâce au Fixed Wireless Access (FWA), devenir une alternative à la fibre optique dans les zones mal desservies.
- En **2020**, dans certains pays du monde, la **5G SA** avait déjà été lancée. Les caractéristiques de cette technologie permettent déjà de tenir ou participer à des réunions virtuelles ou aux jeux multi-joueurs immersifs. Il s'agit de Métavers partiels.
- En **2025**, la **5G Avancée** a déjà fait ses débuts. Pour rappel, la latence théorique qu'elle promet est comprise entre 5 et 10 ms. L'IA et le Machine Learning (ML) permettent d'avoir un réseau auto-optimisé, auto-réparateur, avec une QoS dynamique. Des réunions holographiques deviennent possibles, y compris les concerts massifs au sein du Métavers.

- La **6G NTN** devrait être opérationnelle et commercialisée entre **2028** et **2030**. Elle nous promet, par exemple, un IoT global avec des milliards d'objets connectés (capteurs, véhicules, machines). Quant au Métavers, il devient mondial. Enfin, cet univers immersif est interconnecté et accessible partout. On pourrait même tenir des réunions immersives depuis un avion !
- **Vers 2030**, la **6G IA** pourrait être opérationnelle. L'IA native serait présente partout et les réseaux de téléphonie seraient auto-apprenants, auto-optimisés avec une cybersécurité proactive. La réalité étendue (XR) et le Métavers évolueront et offriront des expériences immersives photoréalistes.
- Enfin, **au-delà de 2030**, la **6G Avancée** pourrait être lancée avec des possibilités incroyables. Les usages immersifs devraient contribuer à l'holoportation (téléportation des hologrammes), faisant aussi disparaitre la frontière entre le réel et le virtuel grâce à une XR encore plus évoluée que favorisera, entre autres, la très faible latence qui devrait en découler.

Nous sommes en 2025, et d'ici au plus tard 2035, ces évolutions deviendront sans doute une réalité pour une certaine partie des habitants de la planète. Des pays comme le Congo pourront-ils bénéficier des évolutions technologiques à venir ?

Figure 20 : Evolutions et usages des technologies émergentes



Sources : UIT – 3GPP – Thales – Ericsson

6.6. Déploiement des technologies futures : quelles contraintes pour le Congo ?

En République du Congo, le déploiement des technologies de communication avancées telles que la 5G Standalone (SA), la 5G Avancée (A) et la 6G, à plus long terme, se heurtera probablement à un ensemble de contraintes qui pourraient ralentir l'alignement du pays sur le calendrier international de la 3GPP et de l'UIT.

▶ Contraintes économiques

La taille du marché congolais, estimée à environ 5,8 millions d'abonnés, dont le revenu moyen par utilisateur (ARPU) est faible (autour de 1 600 F CFA ou environ 2,5 euros), risquerait de limiter la rentabilité des investissements requis pour la mise en place d'un réseau **5G SA complet**. En effet, les déploiements de type Standalone (SA), avec cœur de réseau dédié, densification urbaine et virtualisation du réseau, nécessitent des capitaux considérables. Les opérateurs locaux prendraient-ils le risque d'investir des sommes importantes dans un marché qui pèse environ 192 milliards[64] de F CFA (à peine moins de 300 millions d'euros) ?

Le coût moyen d'une station de base 5G varierait entre 100 000 $ (environ 93 000 €) et 200 000 $ (environ 186 000 €), selon l'emplacement et le fournisseur. Le coût d'une petite cellule 5G varierait entre 10 000 $ (environ 9 300 €) et 50 000 $ (environ 46 500 €) par site. Par contre, la mise à niveau des sites 4G existants vers la 5G coûterait entre 20 000 $ (environ 18 600 €) et 50 000 $ (environ 46 500 €) par site[65]. En extrapolant, il faudrait compter entre 100 et 170 millions d'euros pour un réseau complet compatible avec la taille du marché congolais, en fonction des scénarios. Le niveau de maturité actuel de l'économie congolaise et du marché des communications électroniques incite à privilégier des solutions de niche, mieux adaptées aux besoins spécifiques des secteurs pétrolier, minier et industriel.

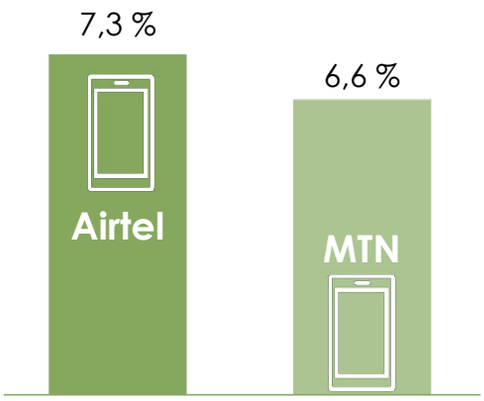
En outre, le coût élevé des terminaux 5G représente un autre frein bloquant non négligeable. Actuellement le nombre de terminaux compatibles 5G disponibles sur les réseaux des opérateurs reste faible. Or, sans terminaux compatibles et accessibles à des prix raisonnables, l'adoption de masse risque d'être ralentie ; et donc avoir un impact mitigé sur les perspectives de rentabilité pour les opérateurs. En valeur absolue, MTN et Airtel ont respectivement 148 723 et 85 261 terminaux[66] compatibles 5G. Par rapport à l'ensemble des terminaux disponibles, toutes technologies confondues, seuls 7,3 % des terminaux 5G sont disponibles sur le réseau Airtel, contre 6,6 % sur celui de MTN. C'est cette proximité des chiffres qui permet d'affirmer que l'accès au réseau 5G est un enjeu important pour la rentabilité des investissements des opérateurs de téléphonie mobile.

64 Il s'agit des données du marché de la téléphonie mobile et de l'Internet mobile, hors données de l'opérateur Congo Télécom.

65 https://patentpc.com/blog/5g-infrastructure-costs-what-telcos-are-paying, site consulté le 12/10/2025.

66 Statistiques fournies par les opérateurs MTN et Airtel en début septembre 2025 qui ne tiennent compte que des réseaux 3G-4G-5G.

Figure 21 : Part des terminaux 5G au Congo sur les réseaux de téléphonie mobile d'Airtel et MTN



Sources : Airtel et MTN

Contraintes énergétiques

La partie de cet ouvrage consacrée aux infrastructures énergétiques prend tout son sens ici. En effet, les différents scénarios développés avaient pour objectif de montrer l'aspect crucial de l'énergie dans le développement d'une économie numérique, et notamment des technologies émergentes. Il sera difficile de demander aux opérateurs de faire plus d'efforts si l'Etat ne prend pas la ferme résolution de combler ces lacunes énergétiques persistantes, même si certains progrès sont visibles.

Dans les télécommunications, et pas seulement, l'instabilité du réseau électrique national, la **dépendance au diesel** – clairement démontrée – pour l'alimentation des stations de base, ainsi que la lente progression des projets d'électrification, pèsent sur la continuité du service[67] et la planification des extensions de couverture.

Or, les infrastructures 5G et 6G, plus denses et énergivores, nécessitent un approvisionnement électrique fiable et durable. En dehors des stations de base, prenons le cas des data centers. Ils sont tout aussi énergivores, mais on ne peut s'en passer dans une économie numérique pour diverses raisons, dont celle en lien avec une partie de sa souveraineté numérique.

Contraintes liées au capital humain

Les défis liés au capital humain et à la maîtrise technologique accentuent certaines limites. Le Congo, comme d'autres pays, souffre d'un déficit de compétences locales dans des domaines clés comme l'intelligence artificielle, la cybersécurité, l'analyse des données, la gestion de réseaux virtualisés, etc. Cette pénurie technique accroît la **dépendance** envers les équipementiers étrangers et retarde la montée en autonomie des acteurs nationaux.

La question de la dépendance aux équipementiers renvoie à celle de l'industrialisation du Congo, et de l'Afrique de façon plus générale. Peut-on penser à la souveraineté numérique si les équipements et les applications utilisés ne sont pas conçus et fabriqués par les Africains eux-mêmes ? C'est une question stratégique fondamentale qui accentuera ou non l'écart technologique entre l'Afrique et le reste du monde en fonction de l'approche politique qui en découlera.

67 C'est ce qui explique en général l'existence de zones blanches que le Fonds pour l'Accès et le Service Universels des Communications Electroniques (FASUCE) couvre de son mieux.

Contraintes technologiques

L'écart temporel entre les cycles technologiques mondiaux (IMT-2020 et IMT-2030), d'une part, et la réalité économique congolaise et du capital humain, d'autre part, pourrait retarder de plusieurs années le déploiement des technologies 5G Standalone, Avancée et 6G. Les infrastructures de transport de données, notamment la fibre optique et les centres de calcul en périphérie (Edge Computing)[68], semblent encore insuffisamment développées au Congo pour soutenir les **exigences de latence** et de **bande passante** des applications émergentes telles que la réalité étendue (XR), les réseaux industriels intelligents ou l'Internet des objets massifs.

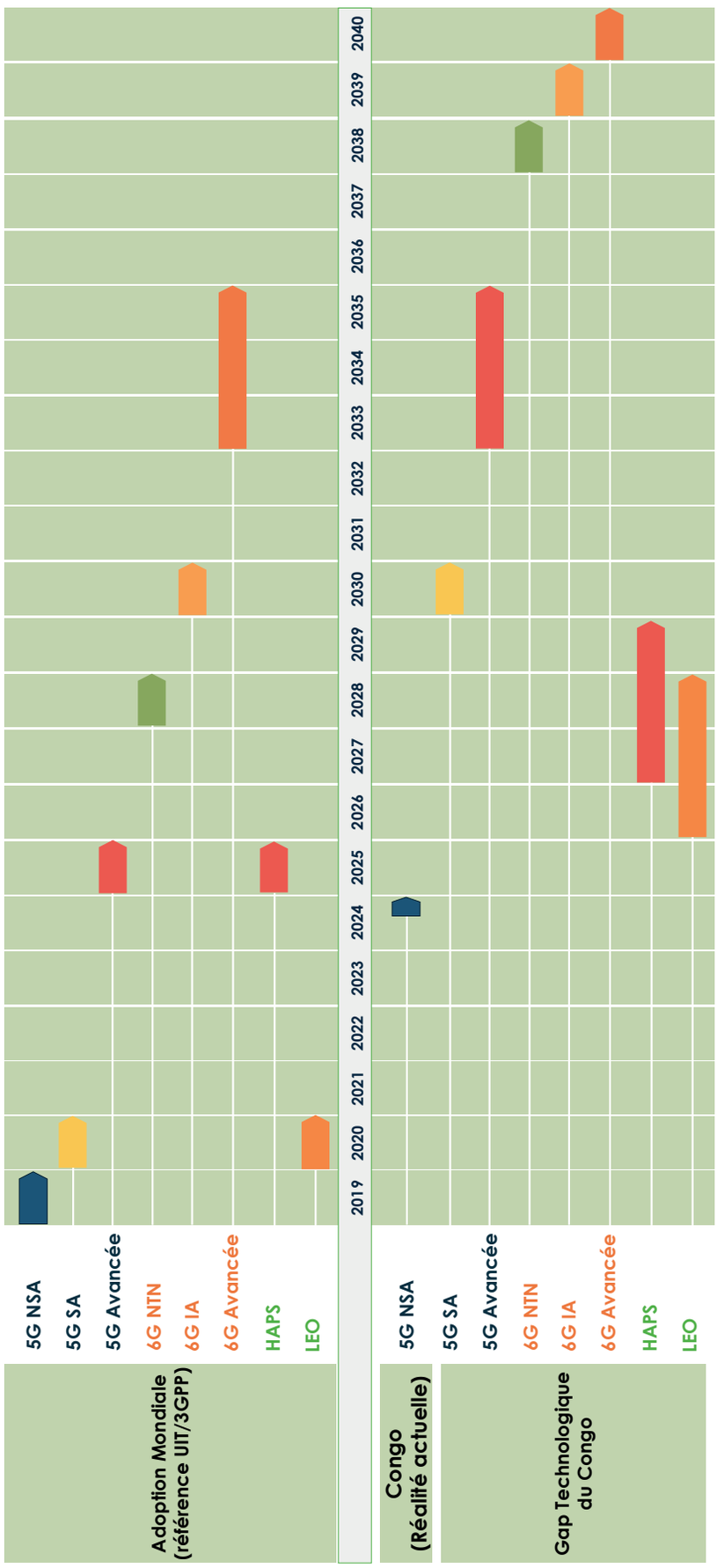
Ainsi, malgré les initiatives pionnières d'opérateurs comme MTN dans la 5G NSA (la plus basique) et les réseaux privés industriels qui sont amenés à se construire, le Congo devra d'abord lever ces différentes contraintes pour espérer converger, à moyen terme, vers les standards internationaux de la connectivité 5G et 6G.

6.7. Gap technologique du Congo dans le déploiement des technologies émergentes

Il existe un décalage temporel dans le déploiement des technologies émergentes au Congo, en comparaison des cycles proposés par l'UIT (IMT-2020 - IMT-2030) et le 3GPP. Dans cet ouvrage, ce décalage ou retard est assimilé à un gap technologique ; ce que montre la figure ci-après. Toutefois, aucune projection n'étant parfaite, celles qui suivent sont d'abord conceptuelles. Elles peuvent néanmoins servir de référentiel dans le déploiement futur des technologies émergentes. **Ces hypothèses supposent que les technologies seraient accessibles par la masse critique.**

68 Le Edge Computing consiste à amener le cloud au plus près du terrain pour que les applications 5G, IA, Métavers, IoT, santé connectée, industrie intelligente, etc. fonctionnent en temps réel, et sans dépendre de l'Internet mondial. C'est donc toujours du « cloud », mais rapproché physiquement des utilisateurs dans des mini data centers locaux afin de réduire encore plus la latence.

Figure 22 : Déploiement actuel et futur des technologies dans le monde vs au Congo



Congo : situation actuelle avec la 5G NSA

Les premiers déploiements mondiaux de cette technologie ont eu lieu en 2019. Au Congo, c'est en fin 2024 que MTN a lancé cette technologie. Le Congo a donc accusé un retard d'environ **5 ans** avant son lancement effectif, probablement à cause du niveau de maturité tardive du marché congolais.

Gap technologique du Congo

C'est en 2020 que les premiers lancements de la **5G SA** ont eu lieu. Compte tenu du retard déjà accumulé pour la 5G NSA, et parce que le déploiement de la 5G SA est conditionné par un cœur 5G dédié, une dorsale fibre étendue et l'émergence de cas d'usages B2B rentables, il est possible que son déploiement au Congo ait lieu en **2030**, si elle doit profiter au plus grand nombre, et pas seulement à certaines entreprises.

Pour la **5G Avancée**, alors que les premiers déploiements ont eu lieu en 2025 dans certains pays, on projette son déploiement au Congo entre **2033** et **2035.** Cette technologie déprendra en grande partie de la disponibilité du cloud local, de l'Edge Computing et d'une forte augmentation du trafic.

La **6G NTN** devrait être commercialisée à partir de 2028. Au Congo, serait-ce réaliste, compte tenu du retard que nous aurions déjà accumulé avec la 5G Avancée ? Elle pourrait l'être vers **2038,** et cette adoption tardive pourrait être liée à la nécessité d'une couverture fibre nationale plus robuste, et aussi d'interconnexions régionales plus fiables.

La **6G IA** devrait suivre vers 2031. Au Congo, il est probable que son déploiement commercial commence en **2039.** Cette technologie est conditionnée par la maturité de l'écosystème IA et de la capacité de calcul locale (data centers, serveurs, Edge Computing) pour traiter les données en temps réel.

La **6G Avancée** a un déploiement mondial prévu entre 2033 et 2035, contre une projection au Congo vers **2040**. Est-ce que le Congo n'aura pas connu de retard dans la construction des infrastructures, dans le développement de compétences locales et le transfert technologique ?

Le déploiement des **HAPS (High Altitude Platform Systems)** a déjà commencé en 2025. Ces plateformes seront probablement utilisées pour la couverture des zones rurales isolées. Ce sont des technologies plus faciles d'accès qui pourraient être disponibles au Congo à partir de **2027**.

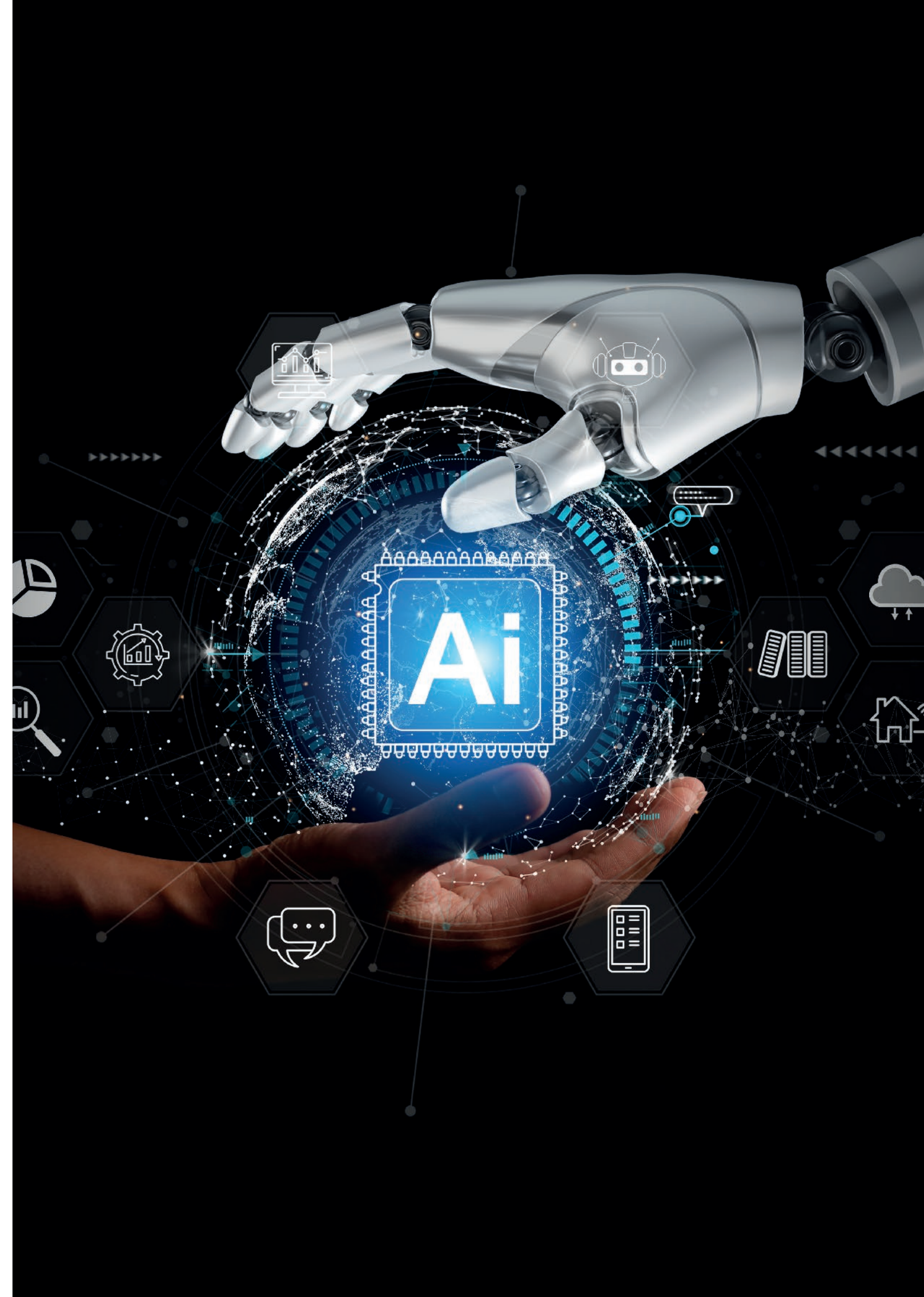
Enfin, la commercialisation des services via des Satellites en orbite basse **(LEO),** déployés depuis 2019, pourrait être effective dès **2026** au Congo. Ces services seront disponibles et fonctionneront en partenariat avec les opérateurs qui ont déjà des licences (MTN, Airtel ou Congo Télécom).

En somme, on peut retenir que les déploiements des **technologies terrestres (5G/6G)** risqueraient de prendre un retard moyen de 7 à 10 ans par rapport **à** ceux envisagés par l'UIT et 3GPP.

Les **technologies satellitaires (LEO / HAPS)**, en revanche, permettraient un rattrapage partiel du gap technologique dès **2026–2028**, grâce aux partenariats hybrides entre les opérateurs satellitaires (Starlink, OneWeb, etc.) et ceux ayant déjà des licences d'exploitation au Congo. Le Congo pourrait ainsi accélérer la couverture nationale avant même la généralisation de la 5G SA **;** ce qui est stratégique pour la connectivité rurale et la transformation numérique.

Figure 23 : Alternatives aux technologies terrestres et couverture nationale accélérée




Ai





VII. SOUVERAINETÉ NUMÉRIQUE ET INFRASTRUCTURES DE STOCKAGE

La souveraineté numérique repose sur la maîtrise des données, des infrastructures de stockage et des règles qui les encadrent. Cette section analyse les politiques et modèles de régulation applicables, évalue la capacité du Congo à affirmer sa souveraineté face aux grandes plateformes mondiales et identifie les leviers nécessaires pour un *possible* contrôle effectif des données nationales.

7.1. Politique de gestion des données : un enjeu de souveraineté numérique

La politique de gestion des données est un ensemble de principes, de directives et de procédures qu'un État ou une organisation met en place pour collecter, stocker, protéger, utiliser et supprimer des données. Cette politique a pour but de garantir leur qualité, intégrité et confidentialité afin de faciliter l'accès et l'utilisation d'un service, entre autres.

Des entreprises comme Google, Meta (Facebook, Instagram, WhatsApp), TikTok, Netflix, Amazon Prime Video, Youtube, Disney+, etc., traitent des volumes considérables de données (mégadonnées ou Big Data). A cet effet, elles ont mis en place des politiques de gestion des données auxquelles doivent consentir tous les usagers qui souhaitent utiliser leurs services. Le tableau suivant compare les politiques de gestion des données de certaines de ces entreprises.

Tableau 4 : Politique comparée de gestion des données des utilisateurs

Meta (Facebook, Instagram, WhatsApp)	▶ **Collecte :** infos comptes (identifiants, activités, terminaux, contenus créés, géolocalisation). ▶ **Traitement et analyse :** fonctionnalités, contenus créés, amis, followers, relations, services connectés. ▶ **Partage et stockage :** données stockées et partagées mondialement (interne Meta et externe avec partenaires et prestataires).
TikTok	▶ **Collecte :** similaire à Meta (compte, activité, appareil, contenus, localisation). ▶ **Traitement et analyse :** personnalisation des contenus et services. ▶ **Partage et stockage** : données partagées avec utilisateurs, prestataires, plateformes tierces (Meta, Google) et partenaires.
Netflix **Prime Video**	▶ **Collecte :** infos compte (paiement inclus), données de visionnage (titres, durée, recherches). ▶ **Traitement et analyse** : données de visionnage pour recommandations. ▶ **Partage et stockage :** données partagées pour les deux entités (Netflix et Prime Video) en interne et en externe (prestataires, partenaires, etc.)
Google	▶ **Collecte :** données de compte (nom, email), activités (recherche, YouTube, Maps), appareils, localisation … ▶ **Traitement et analyse :** personnalisation, sécurité, publicité ciblée. ▶ **Partage et stockage :** données traitées mondialement, partagées en interne (Google/Alphabet) et avec prestataires, encadrées par des règles.

Sources : Politique de gestion de données de Meta - Politique de confidentialité de Tiktok - Conditions d'utilisation et énoncé de confidentialité Netflix - Conditions générales d'utilisation d'Amazon Prime Video - Politique de gestion des données de Google.

Ces politiques ont en commun :

- la collecte,
- le profilage,
- le partage des données avec des prestataires et,
- le stockage et le transfert des données à l'international.

Le stockage et le transfert des données à l'international préoccupent notamment de nombreux pays. En effet, ces géants du numérique hébergent et dupliquent hors du pays d'origine (de l'utilisateur) les données qu'ils collectent. A moins d'appartenir à une communauté puissante comme l'Union Européenne, la plupart des pays subissent plutôt les politiques de ces entreprises mondiales.

Le Congo, par exemple, a adopté une loi sur la protection des données à caractère personnel inspirée du RGPD (Règlement Général sur la Protection des Données) européen. Le Congo dispose-t-il de la même puissance que l'Union Européenne ou la Chine, par exemple, pour faire appliquer cette loi ?

7.2. Localisation des centres de données

Qu'est-ce que la localisation des données ? Elle désigne l'ensemble des lois, politiques ou pratiques qui imposent que certaines données – généralement personnelles, sensibles ou stratégiques – soient stockées et traitées dans une juridiction déterminée (souvent à l'intérieur des frontières d'un État ou d'une communauté régionale). Elle peut prendre deux formes :

- localisation stricte : interdiction de transfert transfrontalier, les données doivent rester sur le territoire ;
- localisation souple : possibilité de transfert hors du territoire à condition que les flux soient tracés, encadrés juridiquement et protégés (par exemple via clauses contractuelles, accords internationaux ou garanties techniques).

Qu'est-ce que la localisation des centres de données ? Cette localisation désigne l'implantation géographique/physique des infrastructures de stockage (data centers) où les serveurs et équipements sont hébergés.

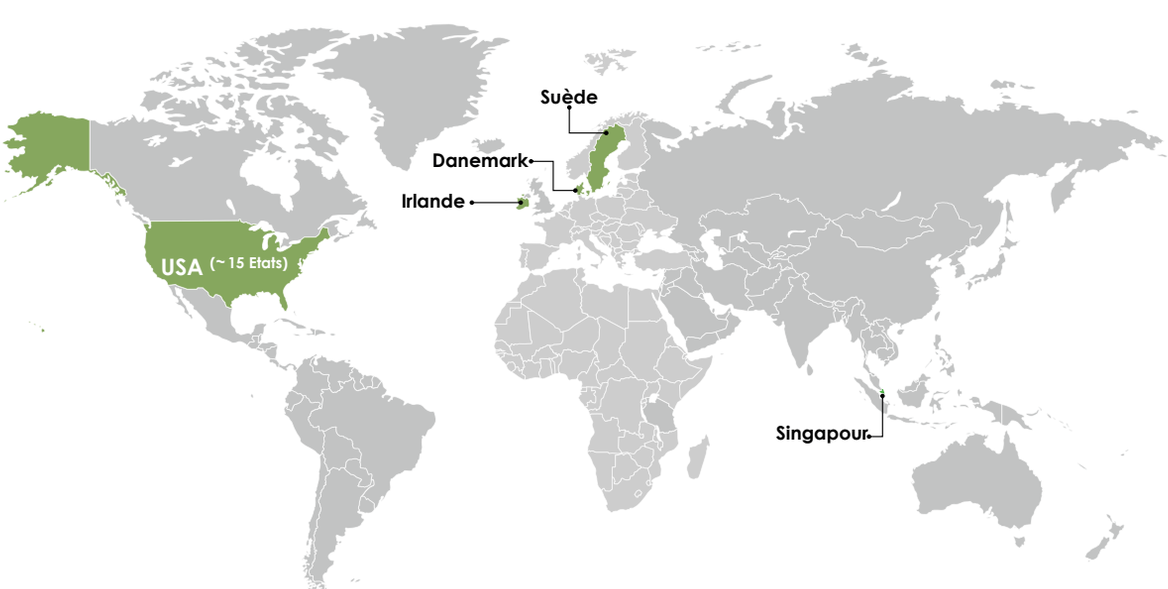
Les figures suivantes sur la localisation de certains centres de données des géants du numérique retenus dans cette analyse permettent de visualiser leur présence mondiale. On a ainsi une idée plus précise des lieux (pays) où les données des utilisateurs du monde, y compris celles des Congolaises et des Congolais, sont potentiellement hébergées.

C'est pourquoi la question du cadre juridique du traitement et de l'hébergement des données, évoquée supra, ne peut faire l'économie d'une réflexion quant à son application effective, notamment par les pays africains comme le Congo.

7.2.1. Localisation des centres de données de Meta

Facebook, **Instagram** et **WhatsApp** partagent les infrastructures de **Meta** pour héberger leurs services. Ces centres de données sont essentiellement situés aux Etats-Unis (dans environ 15 Etats américains). Meta a également implanté des centres de données en Suède, au Danemark, en Irlande et à Singapour.

Figure 24 : Localisation des centres de données de Meta (Facebook, WhatsApp et Instagram)



Source : Politique de confidentialité de Meta

7.2.2. Localisation des centres de données de TikTok

TikTok n'aurait implanté ces centres de données que dans deux (2) Etats américains **(USA)**. En **Europe**, ils ont des centres de données en Norvège et en Irlande, tandis qu'en **Asie**, ses data centers sont localisés en Malaisie et à Singapour.

D'origine chinoise, il est surprenant que cette entreprise n'ait pas déclaré de centres de données implantés sur le territoire chinois ! Officiellement, TikTok précise ne pas en avoir en Chine. Et pourtant, elle a été condamnée à 530 millions d'euros d'amende par l'Union Européenne[69] pour avoir transféré des données d'utilisateurs européens vers des serveurs en Chine ; données que l'entreprise affirme avoir « effacées ». Ceci tend à prouver que les données sont facilement transférables d'une localisation à une autre.

Dans le cas du Congo, pourtant doté d'une loi contraignante, quelle pourrait être sa marge de manœuvre dans une situation identique ?

Figure 25 : Localisation des centres de données de TikTok



Source : Politique de confidentialité de Tiktok

7.2.3. Localisation des centres de données de Netflix et Prime Video

Netflix et **Prime Vidéo** utilisent les infrastructures d'AWS (Amazon Web Services[70]) pour le stockage et la gestion des données[71]. Ainsi, des données bancaires ou sur les habitudes et préférences des utilisateurs sont stockées, analysées, échangées, voire vendues, pour une monétisation qui ne profite pas aux usagers. Pour cause, l'accès au service est conditionné par des politiques d'utilisation que personne ou presque … ne lit.

69 https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following, site consulté le 13/09/2025.

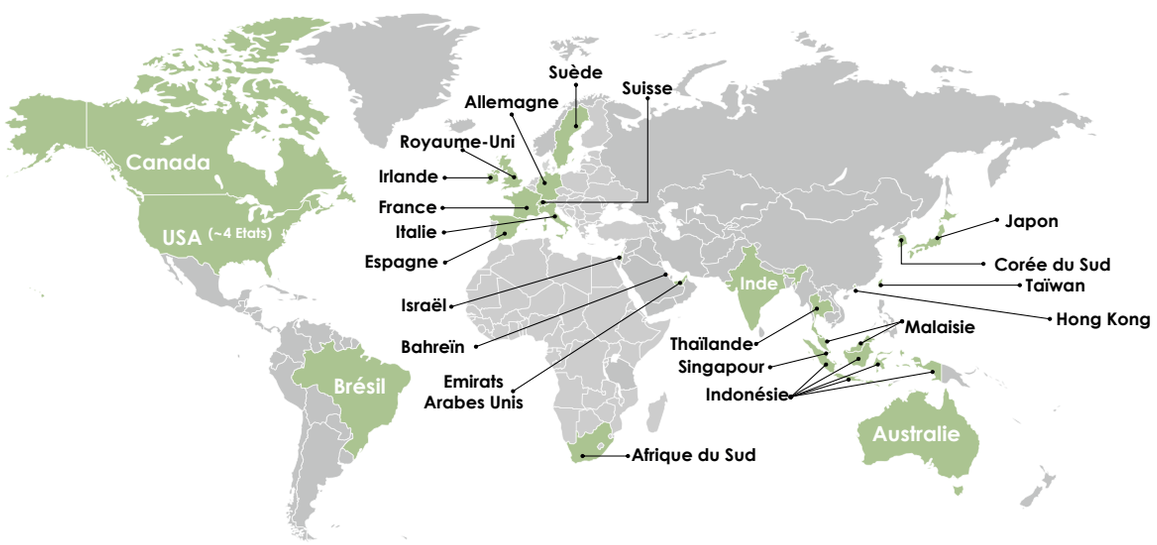
70 Sans doute la plateforme cloud la plus complète et largement adoptée au monde. Elle propose plus de 200 services entièrement fonctionnels à partir de centres de données répartis dans le monde entier.

71 https://aws.amazon.com/fr/solutions/case-studies/netflix-case-study, site consulté le 04/06/2024.

Aux **USA**, AWS aurait des centres de données dans quatre (4) Etats. En **Europe**, les centres de données sont localisés en Suisse, en Suède, en Allemagne, au Royaume-Uni, en Irlande, en France, en Italie et en Espagne. Au **Moyen-Orient**, c'est au Bahreïn, en Israël et aux Emirats Arabes Unis qu'AWS a installé des data centers (centres de données). En **Afrique**, seule l'Afrique du Sud en héberge, idem en **Amérique du Sud** avec le Brésil. Enfin, en **Asie**, AWS a des centres de données en Inde, en Australie, en Indonésie, en Thaïlande, à Singapour, en Malaisie, à Hong Kong, à Taïwan, en Corée du Sud et au Japon.

Comment le droit congolais peut-il protéger les abonnés de Netflix et/ou Prime Vidéo compte tenu de la dispersion mondiale des serveurs de ces mastodontes du numérique ? Les mécanismes de contrôle des flux sont-ils réellement effectifs au Congo ?

Figure 26 : Localisation des centres de données de Netflix et Amazon Prime Video

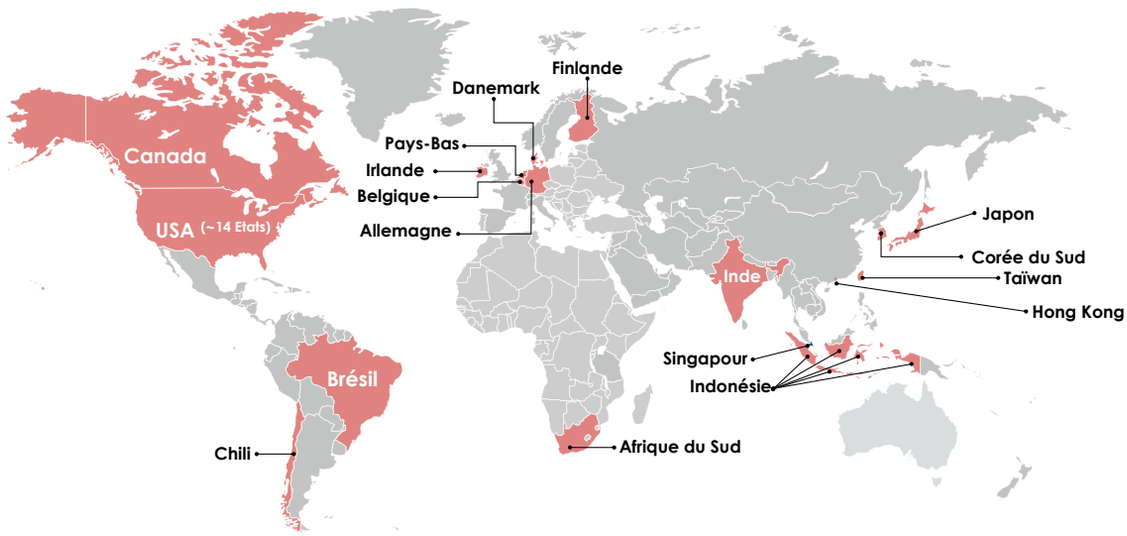


Sources : Conditions d'utilisation et énoncé de confidentialité de Netflix | Centre d'aide de Netflix - Prime Video : Help | Conditions générales d'utilisation d'Amazon Prime Video | Infrastructure mondiale - AWS

7.2.4. Localisation des centres de données de Google

Google est une des sociétés les plus influentes, avec des centres de données à travers le monde, et notamment aux **USA** (dans environ 14 Etats). En **Europe**, elle a des centres de données en Finlande, au Danemark, aux Pays-Bas, en Irlande, en Belgique et en Allemagne. En **Amérique du Sud**, le Brésil et le Chili font office d'hébergeurs, tandis qu'en **Afrique**, seule l'Afrique du Sud en héberge également. Enfin, en **Asie**, les centres de données sont localisés en Inde, à Singapour, en Indonésie, à Hong Kong, à Taïwan, en Corée du Sud et au Japon.

Figure 27 : Localisation des centres de données de Google



Sources : Règles de confidentialité et conditions d'utilisation de Google | Emplacements des centres de données de Google

7.3. Comparaison de quelques modèles de régulation des données

Le développement des technologies émergentes contraint tous les pays du monde à prendre des dispositions réglementaires en matière de collecte, utilisation, transfert et protection des données. Les réglementations suivantes vont être étudiées, sommairement, afin d'en tirer des leçons utiles pour la République du Congo : la CCPA (California Consumer Privacy Act) appliquée en Californie aux Etats-Unis, le RGPD (Règlement Général de la Protection des Données) en vigueur au sein de l'Union Européenne, et la PIPL (Personal Information Protection Law) en République populaire de Chine.

Ces textes visent à garantir, au propriétaire des données, un niveau de protection nationale, régionale et transfrontalière, le cas échéant, dans le cadre de la collecte et de l'exploitation desdites données.

7.3.1. Approche réglementaire

Le **RGPD**[72], le règlement européen sur la protection des données personnelles, repose sur une approche fondée sur les droits fondamentaux des citoyens européens. Il vise à garantir une protection élevée des données personnelles, dans le respect de la vie privée, de la transparence et de la responsabilité des entreprises. Ce cadre juridique s'inscrit dans une tradition européenne de respect de l'État de droit, avec une économie sociale de marché et une volonté de coopération réglementaire entre les Etats membres.

Le **PIPL**[73], la loi chinoise sur la protection des données personnelles, met l'accent sur la souveraineté numérique et le contrôle étatique. Elle impose aux entreprises des obligations strictes en matière de transparence, de sécurité et de consentement, tout en permettant à l'État de conserver un rôle central dans la régulation. Ce cadre reflète une culture du collectif, une priorité donnée à la stabilité nationale, et une économie dirigée, où la cybersécurité est un enjeu stratégique majeur.

72 https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/principles-gdpr_fr, site consulté le 21/09/2025.

73 https://personalinformationprotectionlaw.com/, site consulté le 21/09/2025.

Le **CCPA**[74], la loi californienne sur la protection des données personnelles, adopte une approche pragmatique et commerciale de la protection des données, centrée sur les droits des consommateurs. Il laisse une marge de manœuvre aux entreprises, dans un cadre juridique influencé par les lobbies technologiques. Cette loi reflète une culture individualiste, une forte valorisation du libre marché, et une régulation fragmentée au niveau des États. L'économie américaine, de type capitaliste libérale, accorde une place prépondérante aux acteurs privés dans la gouvernance des données.

7.3.2. Champ d'application

Les régimes de protection des données comme le RGPD, le PIPL et le CCPA ont tous une portée extraterritoriale : ils s'appliquent aux entreprises situées hors de leur territoire dès lors qu'elles traitent les données de leurs résidents.

Le **RGPD** vise les entités qui ciblent ou surveillent des personnes dans l'UE, tandis que le **PIPL** impose des obligations similaires pour les données des citoyens chinois, avec un accent sur la souveraineté numérique.

Le **CCPA**, bien que d'inspiration plus commerciale, s'applique aussi aux entreprises étrangères dès lors qu'elles collectent des données de résidents californiens et atteignent certains seuils économiques.

7.3.3. Consentement et droits des individus

Le **RGPD** impose un consentement explicite et accorde aux personnes des droits étendus (accès, rectification, effacement, portabilité, opposition).

Le **PIPL** adopte une approche similaire, mais prévoit davantage d'exceptions au consentement, notamment pour des motifs contractuels, légaux ou d'intérêt public.

Le **CCPA**, quant à lui, ne repose pas sur un consentement préalable strict, mais sur le droit de refus de la vente ou du partage des données, avec des droits d'accès, de suppression et de correction plus limités.

7.3.4. Sanctions

La souveraineté numérique est une vaste préoccupation mondiale. La plupart des Etats, surtout industriels, souhaitent avoir un maximum de contrôle sur le vaste écosystème de l'économie numérique. La mise en application des sanctions de justice prononcées par certains pays contre des géants du numérique peuvent-elles constituer des arguments de souveraineté numérique ?

Le **RGPD** prévoit des sanctions particulièrement dissuasives, pouvant atteindre 4 % du chiffre d'affaires mondial annuel d'une entreprise ou 20 millions d'euros, selon le montant le plus élevé[75].

Le **PIPL**, de son côté, impose également des sanctions sévères, dans une logique centrée sur la cybersécurité et la souveraineté numérique, avec des amendes pouvant aller jusqu'à 5 % du chiffre d'affaires. Les sanctions peuvent également inclure des mesures administratives telles que la suspension d'activités ou le retrait de licences.

74 https://www.oag.ca.gov/privacy/ccpa, site consulté le 21/09/2025.

75 Ces sanctions sont modulées en fonction de la gravité de la violation, du nombre de personnes concernées, du degré de coopération avec l'autorité de contrôle, et des mesures correctives mises en place.

Le **CCPA**, quant à lui, applique des amendes plus limitées, principalement à l'échelle des entreprises opérant en Californie. Ces sanctions peuvent aller jusqu'à 2 500 $ par violation non intentionnelle et 7 500 $ par violation intentionnelle, notamment en cas de non-respect du droit de refus de la vente des données personnelles. Dans l'Etat de Californie, où sont basées de nombreuses grandes entreprises technologiques (Google, Meta, Apple, etc.), l'influence des lobbies technologiques a sans conteste contribué à limiter la portée des sanctions du CCPA. Les entreprises mises en cause disposent de 30 jours pour corriger les manquements avant sanction effective.

Le tableau suivant montre les raisons et la valeur des sanctions auxquelles font face certains opérateurs du numérique. Le Nigéria et le Kenya ont infligé des sanctions relativement modestes qui se situent dans la fourchette de celles prononcées par la Russie. Quant à l'Union Européenne, elle est de loin la communauté économique qui sanctionne le plus, et notamment les géants du numérique.

Tableau 5 : Sanctions contre les géants mondiaux du numérique

Montants	Entreprise	Motif principal	Pays	Année
2,4 Mds €	Google	Abus de position dominante	Union Européenne	2017
4,3 Mds €				2018
1,5 Mds €				2019
1,2 Mds €	Meta (Facebook)	Transfert de données vers USA sans garanties	Union Européenne	2023
1,2 Mds $	Didi (Chine)	Collecte illégale & transferts non conformes	Chine	2022
746 M €	Amazon	Publicité ciblée sans consentement	Luxembourg	2021
530 M €	TikTok	Absence base légale & transferts hors UE	Union Européenne	2025
345 M €	TikTok	Paramètres par défaut, mineurs, transparence	Union Européenne	2023
225 M €	WhatsApp (Meta)	Manque d'information aux utilisateurs	Union Européenne	2021
220 M $	Meta / WhatsApp	Usage abusif des données utilisateurs	Nigeria	2024–25
78 M €	Google	Non-respect des pénalités antérieures	Russie	2025
500 k $	MultiChoice Nigeria	Atteintes à la vie privée	Nigeria	2025
260 k $	Google	Non-localisation des données	Russie	2022
240 k $	WhatsApp, Snap, Tinder…	Non-localisation des données	Russie	2022–23

Sources : European Data Protection Bureau (EDPB) – Reuters – Voice of America (VOA) – International Association of Privacy Professionals (IAPP)

7.3.5. Rapport de force et souveraineté numérique

Les sanctions que peuvent infliger les régulateurs sont-elles des signes de souveraineté numérique ? Tous les pays disposent-ils des mêmes arguments pour contraindre, notamment les géants du numérique, à respecter la législation en vigueur dans les pays où ils exercent ?

- **Sanctions : signes de souveraineté numérique d'un pays ?**

Lorsqu'un Etat ou une communauté économique, à travers ses différentes autorités de régulation, parvient à imposer l'application de sanctions aux géants du numérique, cela démontre sa puissance, surtout juridique et économique. En plus, les sanctions ont l'avantage de créer un précédent qui contraint les entreprises à anticiper et se conformer aux pratiques locales.

Dans le tableau précédent, on note que Google, pour n'avoir pas respecté le cadre légal en vigueur dans l'Union Européenne, a dû s'acquitter de sommes importantes d'un montant total d'environ 10,2 milliards d'euros.

L'Union Européenne représente un grand marché domestique « sans frontières » qui permet de réguler avec force les plateformes numériques. Cette régulation est notamment possible du fait de l'existence d'un cadre réglementaire clair et prévisible. Soit les géants du numérique s'adaptent et peuvent continuer à commercer au sein de cet espace économique, soit ils subissent les conséquences d'un refus de se conformer à la réglementation en vigueur.

- **Absence de sanctions : faible souveraineté numérique d'un pays ?**

Comparé à l'Union Européenne, un pays avec un poids économique moindre comme le Nigeria peut, conformément à sa législation, sanctionner des géants du numérique. C'est ce qu'il a fait en infligeant une amende de 220 millions de dollars à Meta (WhatsApp). Meta avait fait appel de cette décision. Cet appel a été rejeté le 25 avril 2025, et le jugement exigeait le paiement de l'amende dans un délais de 60 jours[76].

C'est bien la question fondamentale face à ces géants du numérique : les amendes seront-elles payées ? Le rapport de force joue-t-il en la faveur d'un pays comme le Nigéria face à ces géants du numérique qui pourraient menacer de suspendre certaines activités ou contester les amendes à payer ? Le retrait de certaines activités de Meta du Nigeria pourrait-il impacter négativement la santé financière de ce géant ou toute autre grande pointure mondiale du numérique ?

A date, il semblerait que Meta n'ait pas payé ladite somme, mais continue malgré tout d'opérer au Nigeria. Or, à l'image de l'Union Européenne, la souveraineté d'un Etat est plus forte s'il peut contraindre à l'exécution du paiement.

7.3.6. Principes qui gouvernent la souveraineté numérique

Il semble établi que les sanctions contre les géants du numérique constituent un des éléments d'affirmation d'un *certain degré* de souveraineté numérique. Cependant, elles ne suffisent pas car une souveraineté numérique plus ou moins globale suppose l'existence :

76 https://techpoint.africa/insight/meta-and-fccpc-continue-tussle, site consulté le 23/09/2025.

- **De lois efficaces**

Il est primordial de disposer de textes clairs, mais surtout *applicables et cohérents* avec les standards internationaux. Sans base légale solide, les sanctions risquent d'être annulées ou contournées.

- **D'une capacité de régulation efficace**

Les autorités de régulation doivent disposer de moyens humains, financiers et techniques pour garantir leur *efficacité et indépendance* afin de surveiller les pratiques des géants du numérique et instruire les dossiers en bonne et due forme.

- **D'une capacité de sanction avérée**

Imposer de lourdes amendes aux acteurs du numérique, dont les géants, est une étape, certes ; cependant, il faut surtout qu'elles soient confirmées en justice et qu'il y ait un suivi rigoureux sur les recours, les délais et leur *exécution*.

- **Un pouvoir de contrainte économique**

Un *faible poids économique* et un *faible pouvoir d'achat* dans un pays ou une zone communautaire rendent difficile l'application des sanctions. C'est pourquoi l'Union Européenne, qui a un poids économique important, rend des sanctions que ne peuvent ignorer les géants du numérique.

- **Un pouvoir de contrainte technique**

La capacité d'imposer des blocages, de suspendre des services ou de restreindre l'accès au pays est un levier stratégique pour **imposer** l'application des règles, donc de la législation locale ou communautaire.

Les contraintes techniques, plus généralement, intègrent également la **capacité industrielle** d'un Etat à concevoir et à fabriquer ses propres équipements (hardware et software), comme le font les Chinois ou les Américains.

Figure 28 : Princes de souveraineté numérique



7.4. Le Congo peut-il prétendre à la souveraineté face aux géants mondiaux de l'économie numérique ?

Le Congo est confronté au défi de la souveraineté numérique, comme le reste des pays du monde. On pourrait définir la souveraineté numérique comme la capacité d'un État à concevoir, fabriquer, puis contrôler les équipements, les infrastructures, les données et les flux numériques qui circulent, sont hébergés ou exploités sur son territoire, afin de préserver son autonomie stratégique, notamment face aux puissances technologiques. La *souveraineté numérique* constitue donc un maillon important, voire vital, de la *souveraineté économique* et *nationale* d'un Etat.

Le Congo n'échappe pas aux problématiques liées à la gestion des données imposées par les activités et la structure même des géants mondiaux de l'économie numérique, entre autres. Dès 2014, il a fait partie des pays qui ont signé la Convention de Malabo sur la protection des données personnelles. Depuis 2019, son arsenal juridique s'est étoffé avec l'adoption des lois suivantes :

- Loi n°29-2019 sur la protection des données à caractère personnel ;
- Loi n°37-2019 sur les transactions électroniques ;
- Loi n°26-2020 sur la cybersécurité ;
- Loi n°27-2020 sur la cybercriminalité ;
- Loi n°5-2025 créant la Commission nationale de protection des données.

De façon plus précise, la loi n°29-2019 portant protection des données à caractère personnel dispose :

Article 23 : Le transfert transfrontalier de données à caractère personnel ne peut avoir lieu que *si le pays tiers assure un niveau de protection suffisant de la vie privée, des libertés et droits fondamentaux* des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet.

Article 24 : Le responsable d'un traitement peut transférer des données à caractère personnel vers un pays tiers ne répondant pas aux conditions prévues à l'article 22 de la présente loi si le transfert est ponctuel, non massif et que la personne à laquelle se rapportent les données *a consenti expressément* à leur transfert ou si le transfert est nécessaire à la protection de la vie de cette personne, à la sauvegarde de l'intérêt public, au respect des obligations permettant d'assurer la contestation, l'exercice ou la défense d'un droit en justice et à l'exécution d'un contrat entre le responsable du traitement et l'intéressé.

Article 25 : Un transfert ou un ensemble de transferts de données vers un pays tiers *n'assurant pas un niveau de protection suffisant peut être autorisé par la commission lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée, des libertés et droits fondamentaux des personnes concernées* ainsi qu'à l'exercice des droits correspondants. L'autorisation est délivrée sur la base d'une demande dûment motivée émanant du responsable du traitement.

Tableau 6 : Synthèse comparative des législations (Congo - UE - Chine)

	Congo	Union Européenne	Chine
Lois	**Plusieurs lois**	**Plusieurs lois**	**Plusieurs lois**
	▶ Cybersécurité ▶ Cybercriminalité ▶ Transactions électroniques, ▶ Protection des données personnelles	▶ **RGPD**[77] (Données) ▶ **DSA**[78] (Contenus) ▶ **DMA**[79] (Concurrence)	▶ **PIPL**[80] (Données personnelles) ▶ **DSL**[81] (Tous types de données) ▶ **CSL**[82] (Cybersécurité)
Droits	Accès, rectification, opposition, effacement dans certains cas	Accès, rectification, effacement, limitation, opposition, portabilité, droit de ne pas faire l'objet d'une décision prise par un algorithme	Accès, copie, correction, suppression, retrait du consentement, droit de limiter/refuser certains traitements, portabilité sous conditions
Transferts	Transferts vers l'étranger soumis à autorisation préalable de l'autorité nationale, au consentement de la personne ; nécessité de garanties adéquates	Interdiction de transférer des données hors de l'Union Européenne, sauf si des garanties existent	Transferts transfrontaliers soumis à des évaluations de sécurité
Sanctions	Sanctions pénales et administratives prévues, niveau d'application encore à éprouver	Jusqu'à 4 % CA mondial des acteurs du numérique (Sanctions largement éprouvées)	Jusqu'à 50 millions RMB[83] ou 5 % du chiffre d'affaires annuel précédent de l'entreprise concernée

Ce tableau montre que le Congo dispose d'un ***arsenal législatif*** relativement complet, mais fragmenté (cybersécurité, cybercriminalité, transactions électroniques, données personnelles). Sa structure réglementaire se rapproche davantage de celle de la Chine, qui combine aussi plusieurs lois spécialisées, tandis que l'Union Européenne a choisi une approche plus intégrée, avec un cadre normatif unique et complémentaire : le RGPD (protection des données), le DSA (responsabilité et contenus en ligne) et le DMA (concurrence et régulation des grandes plateformes).

Sur les **droits des personnes**, le Congo s'inspire du RGPD, mais dans une portée plus restreinte. En matière de transferts de données, il impose des conditions strictes (autorisation préalable + garanties). Enfin, si des **sanctions** sont bien prévues par le droit congolais, elles restent moins dissuasives que celles de l'UE (jusqu'à 4 % du chiffre d'affaires mondial, avec un régime éprouvé) ou de la Chine (jusqu'à 5 % du chiffre d'affaires annuel).

77 Règlement Général sur la Protection des Données
78 Digital Services Act
79 Digital Markets Act
80 Personal Information Protection Law
81 Data Security Law
82 Cybersecurity Law
83 Renminbi (Monnaie de la Chine)

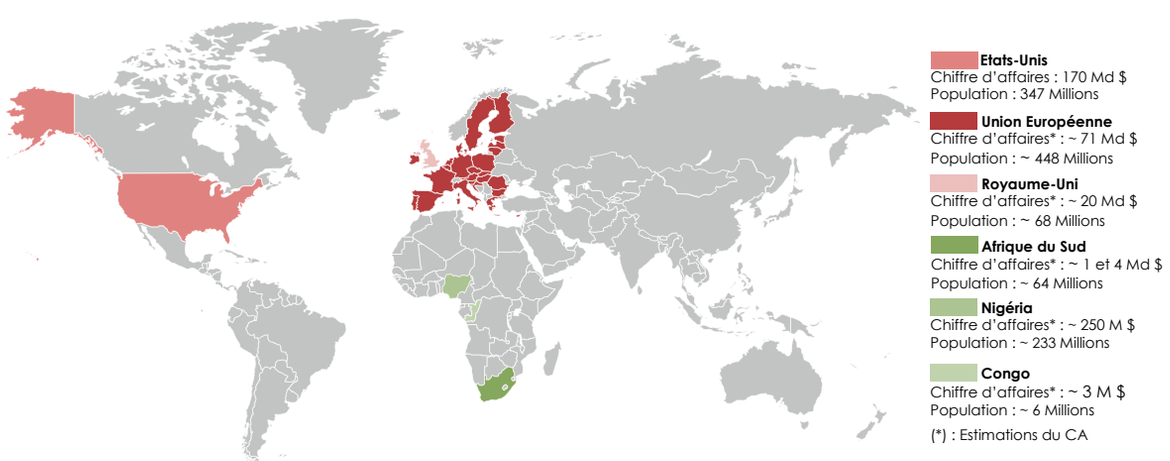
Quels sont la **capacité d'application et les pouvoirs de contrainte économique et technique** dont dispose finalement le Congo ? Cette question est fondamentale car des lois non appliquées affaiblissent la régulation, et donc la réputation d'un pays en la matière. Au regard de la taille et/ou du poids économique du Congo, pourra-t-il appliquer son cadre légal dans son entièreté, notamment face aux géants mondiaux du numérique ?

Dans son rapport annuel, Alphabet (Google) ne publie pas de chiffres par pays, mais uniquement par zones géographiques, à l'exception des Etats-Unis. Ainsi, en 2024, Alphabet a généré les chiffres d'affaires suivants à travers le monde :

- États-Unis : **170,4 Mds $;**
- EMEA (Europe, Moyen Orient & Afrique) : **102,1 Mds $;**
- APAC (Asie-Pacifique) : **70,9 Mds $** ;
- Autres Amériques (Canada + Amérique latine) : **6,1 Mds $**.

En l'absence de chiffres par pays, on ne peut que les estimer. Or, l'Afrique se trouve dans le groupe EMEA, lequel représente le deuxième marché d'Alphabet. Toutefois, dans ce groupe, il y a les Européens qui sont censés avoir un pouvoir d'achat plus important, par exemple, que celui des Africains. C'est donc à partir de la taille des marchés, notamment publicitaires (source principale des revenus d'Alphabet) et du pouvoir d'achat, qu'on peut estimer les revenus approximatifs de Google par bloc régional ou par pays.

Figure 29 : Ventilations d'une partie du chiffre d'affaires de Google par pays



Sources : Securities and Exchange Commission (SEC)[84] – Statista[85] – DataReportal 2025 (Nigeria, Congo, South Africa)[86].

Cette carte montre que l'Union Européenne aurait contribué d'environ 71 milliards de dollars au chiffre d'affaires global d'Alphabet (Google) grâce, entre autres, à ses 448 millions d'habitants, le Royaume-Uni 20 milliards de dollars avec 68 millions d'habitants, l'Afrique du Sud entre 1 et 4 milliards de dollars avec 64 millions d'habitants, le Nigéria

84 https://www.sec.gov/ixviewer/ix.html?doc=/Archives/edgar/data/1652044/000165204424000019/goog-20231231.htm, site consulté le 26/09/2025.

85 https://www.statista.com/statistics/272016/uk-digital-advertising-spending/, site consulté le 26/09/2025.

86 https://datareportal.com/reports, site consulté le 26/09/2025.

environ 250 millions de dollars avec 233 millions d'habitants et le Congo environ 3 millions de dollars avec 6 millions d'habitants.

Mais plus que le nombre d'habitants, c'est surtout le nombre d'internautes par pays qu'il faut prendre en considération ; ce que montre la figure ci-dessous qui permet également de calculer le revenu moyen généré par internaute (ARPU) dans la formation du chiffre d'affaires de Google. On observe que l'Union Européenne a plus d'internautes que les Etats-Unis, mais avec un ARPU 3 fois moins important (546 $ USA vs 179 $ UE). Quant au Congo, sont ARPU serait 546 fois inférieur à celui généré par les Américains. Cela veut donc dire que Google pourrait se passer des revenus des Congolais sans que cela n'impacte significativement son résultat et ses profits. En revanche, pourrait-il se passer des revenus qu'il génère au sein de l'Union Européenne ? Il semblerait que non ; ce qui justifie que Google préfère négocier avec les Européens et payer les sanctions infligées par elle.

En revanche, le Congo pourrait-il infliger des sanctions à Google ?

Figure 30 : Revenus Google par internaute et impact économique 2023

Région Pays	Internautes (Millions et %)		Revenu par internaute	Impact économique
Etats-Unis	~ 312 M	94%	~ 546 $	739 Mds $
UE (27)	~ 400 M	90%	~ 179 $	~ 196 Mds $
Royaume-Uni	~ 65 M	96%	~ 300 $	~ 148 Mds $
Afrique du Sud	~ 51 M	79%	~ 30-70 $	~ 6,3 Mds $
Nigéria	~ 122 M	54%	~ 3-5 $	~ 1,8 Mds $
Congo	~ 2,5 M	38%	~ < 1 $	* 80 M $

Sources : Google & Public First

Cette figure présente aussi des estimations de l'impact des services de Google dans les pays ou blocs économiques retenus. En Europe, les produits, plateformes et outils de Google - notamment Search, Ads, Maps, Workspace, YouTube, Cloud, Play et Android - auraient contribué pour environ 196 milliards de dollars à l'activité économique au sein de l'Union Européenne en 2023. De fait, les entreprises européennes auraient employé un peu plus de 3 millions de personnes grâce à Google.

Au Congo, l'impact économique attribué à Google reste très limité. Il est estimé à environ 80 millions de dollars (≈ 48 milliards de F CFA). Ce seraient les outils proposés par Google (Search, YouTube, Maps, publicité en ligne, etc.) qui auraient permis à l'économie congolaise de produire une telle valeur en 2023 grâce aux activités des entreprises et des particuliers. Il s'agit, toutefois, de l'estimation de l'impact économique, et non d'une contribution directe de Google au produit intérieur brut (PIB) du Congo. Cette valeur ne correspond donc pas aux revenus ou aux impôts de Google au Congo, mais à la valeur ajoutée que ses services ont pu générer dans l'économie nationale.

Le Congo est un **marché de faible importance** pour Google. Aussi, ce dernier ne céderait probablement pas aux sanctions possibles que le Congo pourrait lui infliger. Le Congo, par contre, **utilise** les services de Google qui contribuent à une valeur économique qui n'est pas négligeable.

En conséquence, la capacité de l'État congolais à exercer un **contre-pouvoir** économique sur Google est extrêmement **faible**. Le rapport de force est, en effet, largement asymétrique. Le Congo ne représente qu'un marché marginal pour l'entreprise, tandis que l'économie congolaise reste fortement dépendante des services numériques de Google. Cette **asymétrie** réduit les marges de manœuvre de l'État congolais en matière de régulation ou de négociation, contrairement à des blocs économiques plus puissants comme l'Union Européenne ou les États-Unis.

Les enjeux de sécurité et de lutte contre la cybercriminalité ne doivent pas être négligés en matière d'hébergement des données par les géants du numérique. Le Congo est plus vulnérable aux cyberattaques, moins en raison de ses infrastructures numériques ou de sa législation, que pour ses capacités limitées à gérer de telles menaces. C'est un argument que les géants mondiaux du numérique pourraient utiliser afin de ne pas héberger leurs données dans les data centers présents au Congo[87].

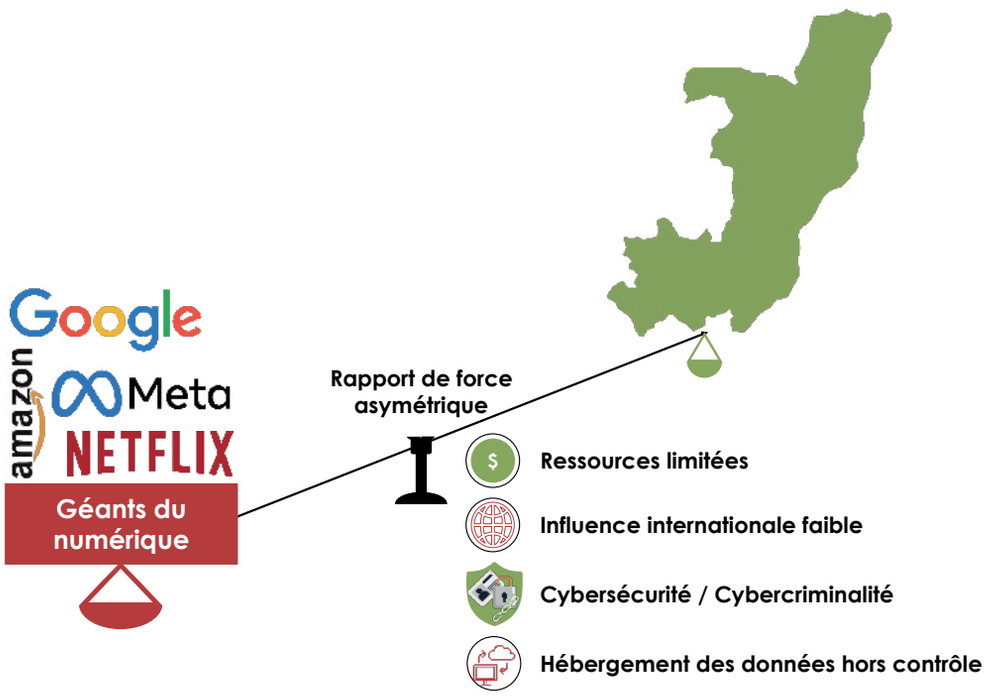
Supposons qu'ils acceptent de se soumettre à la législation congolaise en hébergeant leurs données dans des data centers locaux, quelle garantie la Commission en charge de la protection des données à caractère personnel aura-t-elle que ces données ne seront pas répliquées en dehors des frontières nationales, dans des data centers gérés et contrôlés par ces géants du numérique ?

La principale leçon que le Congo peut tirer de cette situation — et qui vaut pour de nombreux pays, particulièrement en Afrique — est qu'il ne dispose d'aucun réel contre-pouvoir face aux géants du numérique. En raison du faible poids économique que représente son marché dans le portefeuille mondial de ces entreprises, sa capacité à imposer des règles ou à défendre pleinement sa souveraineté numérique reste limitée.

Cette réalité souligne que **la souveraineté numérique ne peut être garantie que dans un cadre collectif par la coopération régionale** (Union Africaine, CEMAC, CEEAC, etc.). À défaut, le rapport de force restera largement asymétrique, au détriment des États pris individuellement.

87 Google dispose de nombreux serveurs caches (GGC) en Afrique. Leur rôle est de stocker localement les contenus les plus demandés afin de réduire la latence et d'économiser de la bande passante internationale. Mais contrairement aux data centers, ces caches ne traitent pas, ni n'hébergent des données utilisateurs.

Figure 31 : Rapport de force asymétrique entre le Congo et les géants du numérique



7.5. Données de souveraineté nationale pour le Congo

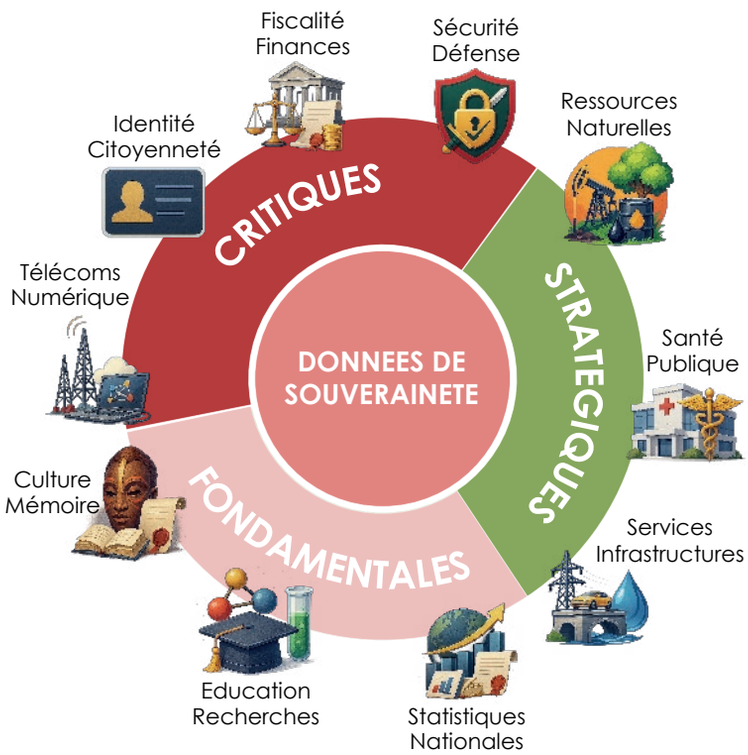
Malgré un rapport de force asymétrique entre le Congo et les géants du numérique, il existe des données dont l'identification et la protection permettraient de constituer un levier de contrôle stratégique. Ces données peuvent être catégorisées de la manière suivante : critiques, stratégiques et fondamentales.

Toute donnée ayant un impact sur la souveraineté - qu'elle soit critique, stratégique ou fondamentale - doit être hébergée localement. La hiérarchisation ci-dessus contribue d'abord à définir les niveaux de sensibilité et de priorité, mais pas à exclure certaines données du périmètre de souveraineté numérique. Cette hiérarchie gagnerait d'ailleurs à être investiguée plus en profondeur par les sachants de chacun des secteurs concernés.

- **Données critiques** : elles regroupent la sécurité et la défense, la fiscalité et les finances publiques, l'identité et la citoyenneté (personnes physiques et morales), ainsi que les télécoms et le numérique.
- **Données stratégiques** : elles concernent principalement les ressources naturelles (pétrole, mines, forêts), la santé publique (épidémiologie, dossiers médicaux, vaccinations), ainsi que les infrastructures et services essentiels (énergie, transport, eau).
- **Données fondamentales** : elles couvrent l'éducation et la recherche, la culture et la mémoire nationale (archives, patrimoine, médias publics), ainsi que l'open data socio-économique (statistiques publiques de types PIB).

En somme, ces données doivent être sous contrôle national (hébergement, traitement, accès) afin de garantir la souveraineté militaire, politique, économique, sociale et culturelle du Congo.

Figure 32 : Types de données de souveraineté



7.6. Limites et leviers de contrôle

▶ Limites

Il existe encore des limites à la maîtrise totale par le Congo du traitement local de toutes ces données numériques. En effet, de nombreux équipements, logiciels et normes sont imposés par les équipementiers (OEM[88]) tels que Cisco, Huawei, Microsoft, etc. Les serveurs peuvent être localisés au Congo, mais la **dépendance logicielle** (Azure Stack, Oracle, VMware, etc.) crée une **dépendance technologique**. Le Congo n'a pas encore les moyens de contourner cette réalité.

À cela s'ajoute une autre forme de dépendance : celle liée aux fabricants de smartphones (Apple, Samsung, Huawei…) et aux écosystèmes de comptes en ligne. Pour exploiter pleinement les capacités d'un smartphone ou accéder aux principales applications et services (Play Store, App Store, sauvegarde cloud, etc.), il est souvent obligatoire de disposer d'un compte Gmail, Apple ID ou équivalent.

Dans un data center, il est normal que les données soient répliquées de façon automatique sur plusieurs sites : c'est la redondance, et elle est indispensable. Au Congo, des opérateurs disposent de data centers privés. Si une copie des données locales part vers un autre pays, la **souveraineté** devient **partagée,** voire **compromise** en fonction du type de données. Dans ces conditions, la **réplicabilité**[89] des données serait un maillon que nous ne maîtriserions pas.

88 Original Equipment Manufacturer

89 Le cadre légal de la gestion des données existe, mais n'est pas pleinement opérationnel.

Le Congo, et c'est une problématique mondiale, ne dispose pas d'une masse critique de spécialistes en IA, cloud, cybersécurité, etc. Sans cette main d'œuvre spécialisée, il est difficile de maintenir une souveraineté numérique réelle. Il faudrait donc faire recours aux experts étrangers à cause de compétences locales limitées ; ce qui crée une **dépendance en capital humain stratégique**.

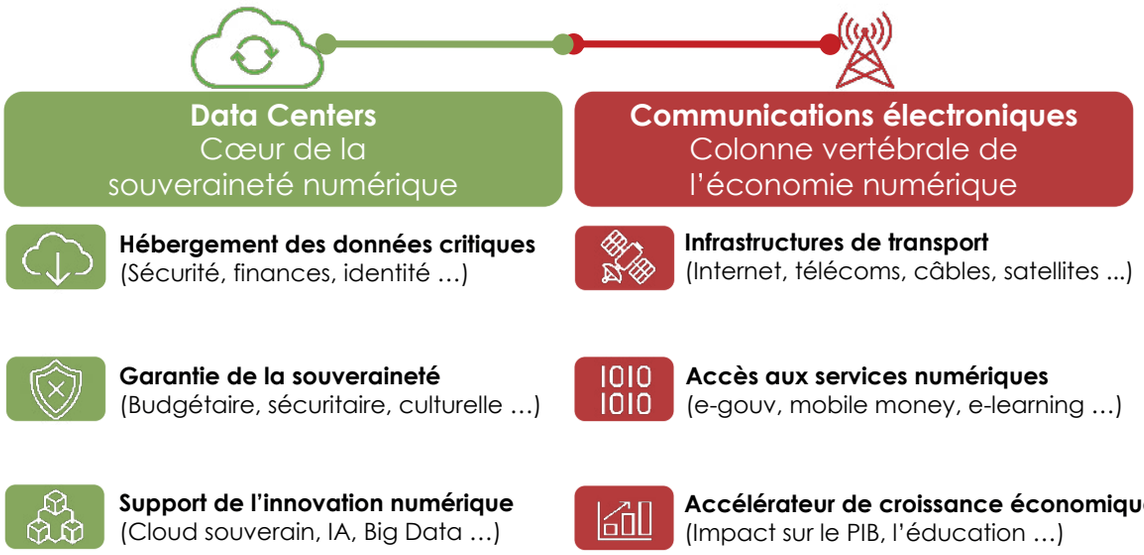
Figure 33 : Chaîne de souveraineté des données



La formule paraît simpliste. Mais si le Congo parvenait à contrôler l'infrastructure, les logiciels, l'hébergement, et disposait des compétences techniques, tout en contrôlant la réplication des données, on pourrait parler de souveraineté numérique **globale**. En revanche, si un ou plusieurs maillons échappent au contrôle national, alors la souveraineté du Congo sur les données qu'il produit devient **partielle, voire nulle**, surtout si en amont il ne maitrise pas la conception et la fabrication de ses propres équipements.

Le Congo pourra difficilement, à court ou moyen terme, contrôler l'ensemble de la chaîne de souveraineté des données. En tant qu'infrastructures des communications électroniques, les data centers sont au cœur de la **souveraineté numérique**. Cependant, la colonne vertébrale de l'écosystème de **l'économie numérique** demeure les réseaux de communications électroniques.

Figure 34 : Souveraineté numérique versus économie numérique



Leviers de contrôle possibles

L'Union Européenne, qui regroupe 27 Etats, montre qu'il est possible de faire face aux géants du numérique. Le Congo, pris isolément, ne le peut pas. Or, il appartient à une zone économique : la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC) dont le poids économique reste modeste à l'échelle mondiale. Selon le rapport annuel 2023 de la Banque des États de l'Afrique Centrale (BEAC), le PIB cumulé de la zone s'élevait à 64 444 milliards de FCFA, soit environ 106 milliards de dollars. A titre de comparaison, ce montant est inférieur au chiffre d'affaires annuel de certaines grandes entreprises technologiques.

En regroupant tous les pays de l'Afrique sub-saharienne, on obtient une population d'environ 1,3 milliard d'habitants en 2024[90]. La population de l'Allemagne, en comparaison, est d'environ 84 millions d'habitants. Elle est de 68 millions pour le Royaume-Uni et de 66 millions pour la France.

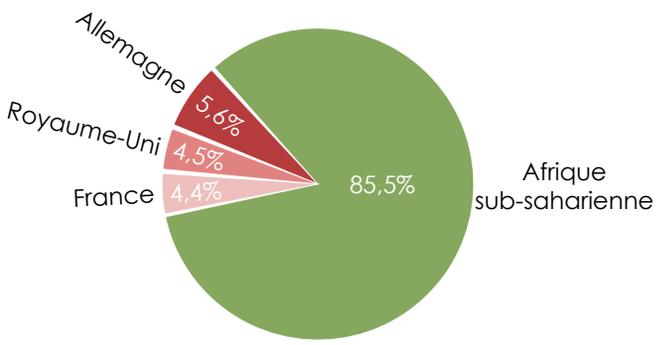
Malgré une population de plus d'un milliard de personnes, le PIB de l'Afrique sub-saharienne ne dépasse pas 2 000 milliards de dollars en 2024. En revanche, l'Allemagne, le Royaume-Uni et la France, avec des populations inférieures à cent millions d'habitants, ont respectivement généré les PIB suivants : 4 450 Mds, 3 644 Mds et 3 162 Mds de dollars.

Le PIB par habitant montre clairement l'écart de richesse produit entre l'Afrique sub-saharienne et le mini bloc européen constitué par l'Allemagne, le Royaume-Uni et la France. Par exemple, le PIB/habitant de l'Allemagne est 36,8 fois supérieur à la moyenne des pays de l'Afrique sub-saharienne.

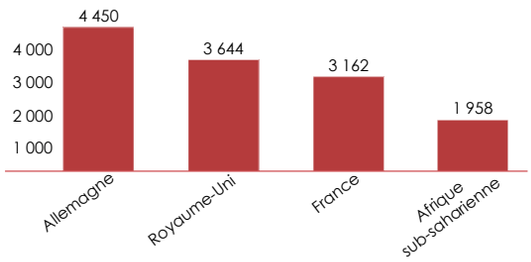
90 https://data.worldbank.org/indicator/NY.GDP.MKTP.CD, site consulté le 01/09/2025.

Graphique 1 : Indicateurs de comparaison entre l'Afrique sub-saharienne et 3 pays de l'Union Européenne

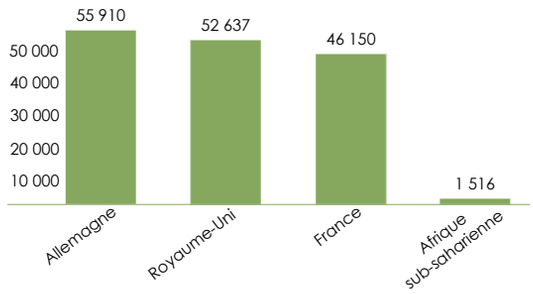
Répartition de la population (2024)



Produit Intérieur Brut (2024) en Mds $



PIB par habitant (2024) en $



Sources : Banque Mondiale – Fonds Monétaire International

Ces graphiques nous montrent que la richesse d'un Etat n'est pas fonction de sa population, et que l'Afrique sub-saharienne, même si elle venait à s'unir dans les circonstances actuelles, aurait un poids relatif face aux géants du numérique. C'est pourquoi le réel développement économique et industriel du continent africain est un véritable enjeu de puissance et de souveraineté.





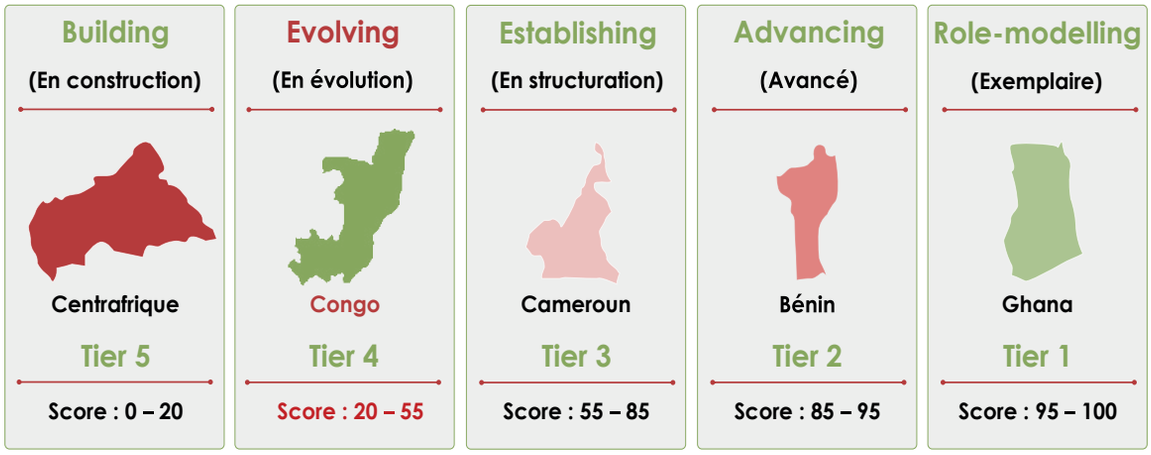
VIII ENJEUX DE CYBERSÉCURITÉ

La cybersécurité est un pilier essentiel de la confiance numérique et de la souveraineté technologique. Cette section met en évidence les priorités du Congo en matière de sensibilisation, d'équipements et de gouvernance technique, tout en évaluant son niveau actuel et les perspectives de maturité face aux menaces croissantes du cyberespace.

8.1. Importance de la sensibilisation

La cybersécurité n'est pas une option pour un Etat, une entreprise ou les citoyens : c'est une obligation. L'Union Internationale des Télécommunications (UIT) publie régulièrement le Global Cybersecurity Index (Indice Mondial de Cybersécurité). Il comporte cinq catégories (Tiers) qui permettent de montrer le niveau de maturité des pays membres. En 2024, le Congo se situait dans le Tier 4, conformément à la figure suivante.

Figure 35 : Niveau de maturité du Congo dans la cybersécurité



Sources : UIT

On peut constater que le Bénin, et surtout le Ghana, font mieux que le Congo en se situant respectivement en Tier 2 et Tier 1. Ce classement prend en compte différents aspects comme le cadre légal, les mesures techniques, etc. Dans le cas du Congo, seul le cadre légal justifie une note supérieure à 10. En effet, le Congo dispose de textes sur les transactions électroniques, la cybersécurité, la cybercriminalité, la protection des données, etc. Cependant, ils sont encore insuffisants.

Figure 36 : Détails de la note du Congo pour le Tier 4

Evolving **(En évolution)**  **Congo** **Tier 4** **Score : 20 – 55**	**Cadre légal**	14,12 / 20
	Mesures Techniques	0,00 / 20
	Mesures Organisationnelles	3,90 / 20
	Renforcement des compétences	0,72 / 20
	Coopération	8,87 / 20
	Score global	**45,63 / 100**

Sources : UIT

En 2024, sur le plan technique, le score du Congo est nul. Pour cause, le Congo ne dispose pas encore d'un CERT[91] national pour répondre aux attaques contre son cyberespace. L'ANSSI est en voie d'opérationnalisation, certes, mais elle n'est pas encore en mesure de pleinement faire face à ce type d'attaques. Ce qui fait qu'elle ne peut pas efficacement implémenter la ou les stratégies de défense et de protection qui s'imposeraient. Or, pour répondre aux attaques, notamment complexes, il faut disposer de compétences, c'est-à-dire de techniciens chevronnés capables d'y faire face.

Le renforcement des compétences devient donc une priorité absolue. Ce qui est certain, c'est que la note du Congo en dit long sur les efforts qui restent encore à fournir en la matière. Enfin, l'opérationnalisation de l'ANSSI montre des débuts encourageants en matière de coopération entre agences. On peut citer la coopération existante entre l'ARPCE et l'ANSSI qui devrait permettre, entre autres, de renforcer la sécurité des systèmes d'information et des réseaux de communications électroniques, d'assurer une gestion efficace des incidents de cybersécurité, ainsi que de favoriser le partage d'informations sur les incidents et menaces de cybersécurité.

Le Congo se situe dans une zone de vulnérabilité que montrent les indicateurs internationaux présentés supra. Davantage de sensibilisation aux problématiques de cybersécurité devient importante afin qu'une masse critique de personnes physiques et morales en prennent conscience.

La démarche de sensibilisation qui paraît la plus efficace devrait commencer par :

- **Les décideurs politiques**

Leur sensibilisation est cruciale car ce sont eux qui définissent la vision et allouent les ressources. Sans compréhension claire des enjeux, aucune stratégie nationale ne peut être soutenue, et encore moins pérennisée.

91 Computer Emergency Response Team (Équipe d'intervention en cas d'incident informatique).

- **Les administrations d'Etat**

Elles sont parfois ciblées par les hackers (services publics, finances, défense). D'où l'ultime nécessité de former les responsables des systèmes d'information des administrations à la gestion des risques numériques.

- **Les entreprises d'Etat et privées (y compris les TPE, TPI, etc.)**

Le tissu économique national repose sur les entreprises, et notamment les TPE, TPI, etc. Or, la plupart ne disposent pas de plans de sauvegarde, de reprise d'activité ou de sensibilisation interne parce qu'elles n'ont pas mis en place de système d'information.

- **Le grand public (utilisateurs lambda)**

Des campagnes pédagogiques, y compris en langues nationales (Lingala et Kituba), doivent être lancées dans les écoles, les médias, les réseaux sociaux, de sorte que chaque citoyen se sente concerné par la sécurité de son environnement numérique. C'est à cause de l'ignorance, parfois induite par l'illettrisme, que la fraude Mobile Money, le phishing ou les arnaques en ligne prospèrent.

- **Les acteurs de l'éducation et de la recherche**

Il faudrait généraliser la sensibilisation dès le plus jeune âge, et pas seulement dans les centres formant des ingénieurs ou des décideurs. Sans intégration de la cybersécurité dans les programmes scolaires, techniques et universitaires, le Congo prend un grand risque de dépendance aux compétences étrangères.

- **Les médias et influenceurs du numérique**

On ne saurait parler de sensibilisation de masse sans impliquer, à l'ère du numérique, les médias et les influenceurs des réseaux sociaux qui sont suivis par des centaines de milliers de personnes.

Des campagnes de formation des journalistes et des créateurs de contenu sur la cybersécurité (vérification, protection des sources, hygiène numérique) s'imposent sans doute. Ce seront eux les relais efficaces auprès de leur audience respective.

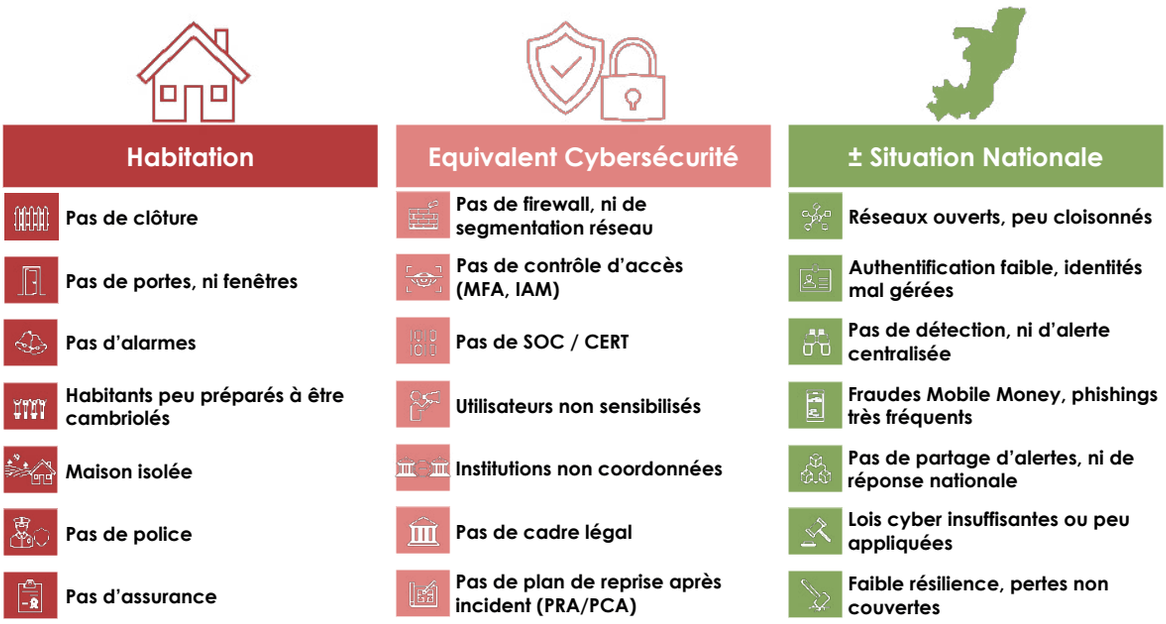
Il serait peut-être indiqué que des partenariats entre l'ANSSI et les médias voient aussi le jour afin de diffuser des messages de prévention qui soient cohérents. Il faudrait éviter que les médias ne diffusent des contre-sens qui apporteraient de la confusion, et donc pourraient entamer ou fragiliser la confiance numérique des Congolais.

8.2. Importance des équipements et plateformes techniques

Les hackers se gardent de savoir si des lois existent lorsqu'ils agissent contre les intérêts économiques, sécuritaires, industriels ou militaires d'un pays ou d'une organisation. La loi n'a pas d'emprise sur eux, à moins qu'ils ne soient *capturés* ; ce qui est souvent très difficile. Un hacker basé aux Philippines, qui veut attaquer le cyberespace congolais, ne cherche pas à en connaitre le cadre légal. Par contre, s'il est confronté à une réponse efficace à son attaque parce qu'une stratégie et des mesures pratiques de cybersécurité ont été mises en place, ceci peut contribuer à complexifier sa tentative au point, éventuellement, qu'il abandonne.

Si nous prenons l'exemple d'une maison, comme le montre la figure ci-après, on peut mieux percevoir la situation dans laquelle se trouve le Congo par rapport à la notation qui lui a été attribuée par l'UIT concernant son niveau de maturité en cybersécurité.

Figure 37 : Analogie « Maison » et Cybersécurité au Congo



Une maison qui n'a ni clôture, ni portes, ni fenêtres, etc. est forcément vulnérable. Des personnes mal intentionnées peuvent donc la cambrioler sans aucune difficulté, surtout si ses habitants sont peu attentifs ou distraits.

La situation actuelle peut donc être comparée à une ville où la plupart des maisons seraient sans protection. L'analogie est la suivante :

- **pas de clôture** équivaudrait à l'absence de firewall (pare-feu) et de segmentation réseau. On notera qu'un pare-feu contrôle et filtre le trafic réseau entrant et sortant afin de protéger un système contre les accès non autorisés ou les menaces extérieures ;
- **pas de portes**, ni fenêtres équivaudraient à des accès ouverts aux systèmes sans authentification forte tels que le Multifactor Authentication (MFA) et l'Identity and Access Management (IAM). Le MFA, par exemple, exige plusieurs types de vérification (un mot de passe, un code envoyé par SMS, etc.) pour confirmer l'identité d'un utilisateur ;
- **pas d'alarme** équivaudrait à l'absence de CERT ou de SOC qui sont des plateformes qui permettent de détecter des intrusions. SOC signifie Security Operations Center (*Centre des opérations de sécurité*) et CERT signifie Computer Emergency Response Team (*Équipe de réponse aux urgences informatiques*) ;
- **habitants peu préparés à être cambriolés** seraient des citoyens, des entreprises ou des institutions qui n'ont pas de culture en termes de sécurité numérique ; ce qui fait qu'ils ne sauraient avoir les bons réflexes face aux menaces ;
- **maisons isolées** équivaudrait aux administrations et aux opérateurs d'infrastructures critiques qui agiraient sans coordination, ni partage d'alertes ;
- **pas de police** marquerait l'absence d'un mécanisme de protection et d'intervention. Ce qui voudrait dire que des *forces de l'ordre* du cyberespace ne seraient pas formées et mobilisées en nombre suffisant ;

- **pas d'assurance** marquerait l'absence de mécanismes de résilience et de compensation (PRA/PCA, couverture financière après incident). Le PRA est le Plan de Reprise d'Activité qui permet de redémarrer les systèmes informatiques après un incident majeur, tandis que le PCA (Plan de Continuité d'Activité) maintient les services essentiels pendant la crise, y compris en mode dégradé.

En somme, la plupart des maisons (administrations, entreprises, citoyens) restent vulnérables isolément. C'est ce qui expliquerait que personne ne prévient ses voisins en cas de cambriolage. Et les cambrioleurs agissent en quasi-impunité. C'est pourquoi le Congo doit sortir de cette situation critique.

8.3. Projections sur la maturité du Congo en cybersécurité

La maturité du Congo en matière de cybersécurité demeure encore assez embryonnaire. Les efforts déjà fournis pour rattraper son retard, notamment sur le plan juridique, démontrent une volonté des autorités compétentes de ne pas laisser le cyberespace congolais sans protection. Combien de temps faudrait-il pour que le Congo entre dans la catégorie 1 (ou tier 1) de l'UIT ? Si le Ghana y est parvenu, cela suppose que le Congo pourrait s'en donner les moyens et la rigueur nécessaires.



Figure 38 : Maturité du Congo en cybersécurité à l'horizon 2035 !

	2026 – 2027 (Tier 4 → Tier 3)	2028 – 2030 (Tier 3 → Tier 2)	2030 – 2035 (Tier 2 → Tier 1)
Cadre Juridique	**Consolidation et mise en œuvre du cadre juridique**	**Application effective et harmonisation sectorielle**	**Alignement international et exemplarité juridique**
	▪ Textes d'application (notifications des incidents, infrastructures critiques) ; ▪ Rendre totalement opérationnelle la Commission de protection des données ; ▪ Créer un cadre légal pour les CERT/SOC.	Application effective : ▪ des contrôles ; ▪ des enquêtes ; ▪ des sanctions, et coordination judiciaire multisectorielle.	▪ Harmonisation continue des textes aux normes internationales ; ▪ Textes imposant l'évaluation périodique de la cybersécurité (audits, publication indicateurs …) ; ▪ Coopération judiciaire transfrontalière (entraide, extradition, preuves numériques).
Plan Technique	**Surveillance passive**	**Surveille proactive**	**Surveillance prédictive**
	▪ Mettre en place un CERT/SOC de niveau 1 et 2 (détection, réponse, partage, alertes) ; ▪ Inventaire national des actifs critiques par secteur ; ▪ Imposition des contrôles de base (pare-feu, MFA, sauvegardes, segmentation réseau) dans les administrations et entreprises privées.	▪ Élever le SOC au niveau 3 (traque des menaces, surveillance intelligente) ; ▪ Généraliser PRA/PCA, EDR/XDR, ISO 27001/ ISO 62443 aux secteurs critiques ; ▪ Créer un cloud souverain sécurisé ; ▪ Segmenter les réseaux OT/ICS ≥70%.	▪ Zero Trust national (réseaux …) ; ▪ Cyber assurance nationale et SOC niveau 3+ couvrant ≥ 90 % des entités ou infrastructures critiques ; ▪ Défense prédictive (notamment avec l'Intelligence artificielle) ▪ Coopération internationale automatisée (échanges d'indicateurs en temps réel …)
Plan Organisationnel	**Installation et gouvernance**	**Coordination et résilience**	**Intégration et pilotage durable**
	▪ ANSSI pleinement opérationnelle : directions techniques, gouvernance nationale, budget dédié ; ▪ Désignation de RSSI ministériels et points focaux sectoriels ; ▪ Mise en place d'un processus national de gestion des incidents et d'un comité interministériel de cybersécurité.	▪ Déploiement de PRA/PCA sectoriels et d'exercices inter-organisationnels ; ▪ Création d'un centre de coordination nationale de crise relié au CERT/SOC national ; ▪ Mise en place d'un tableau de bord national de maturité (indicateurs par secteur, etc.).	▪ Intégration de la cyber-résilience dans la planification nationale (défense, économie, éducation …) ; ▪ Exercices régionaux conjoints (sous région, Afrique) et coordination internationale ; ▪ Amélioration continue par les audits cycliques, retours d'expérience …).
Renforcement des Compétences	**Sensibilisation et formation des premiers experts**	**Professionnalisation de la formation**	**Pôle de compétences et centre régional d'excellence**
	▪ Lancement d'un programme national de formation initiale (Universités, écoles techniques, etc.) ; ▪ Création des premières filières certifiantes (CEH, ISO 27001, SOC Analyst, etc.). ▪ Sensibilisation à grande échelle : décideurs, administrations, entreprises, citoyens, etc.	▪ Mise en place de simulations d'attaques/défense ; ▪ Formation de plusieurs professionnels spécialisés (forensic, OT/ICS …) ; ▪ Intégration de la cybersécurité dans les curricula universitaires et techniques ; ▪ Partenariats régionaux (certification et recherche appliquée).	▪ Création d'un Institut national de cybersécurité (formation, R&D, innovation) de réputation régionale ; ▪ Développement de programmes de doctorat et de recherche locale (IA, cyberdéfense, cryptographie) ; ▪ Constitution d'une communauté professionnelle (des centaines d'experts actifs dans le public/privé).
Coopération Nationale et Internationale	**Coordination nationale et alignement international**	**Coopération opérationnelle et partage d'informations**	**Intégration internationale et leadership régional**
	▪ Mise en place de points focaux sectoriels (télécoms, banques, énergie, défense …) ; ▪ Participation aux plateformes régionales existantes ; ▪ Premiers accords d'échange d'alertes avec Interpol, etc.	▪ Participation aux simulations d'attaques avec d'autres CERT ; ▪ Partage opérationnel de Cyber Threat Intelligence (CTI) ; ▪ Contribution aux opérations conjointes de cybercriminalité financière, fraudes numériques, etc.	▪ Participation aux plateformes régionales et internationales d'assistance et d'échange automatique d'indicateurs ; ▪ Coordination sous-régionale et accueil d'un forum international annuel sur la cybersécurité.

Certains termes techniques utilisés dans le tableau ci-dessus se défissent comme suit :

- **EDR** (Endpoint Detection and Response ou Détection et Réponse sur les Terminaux) surveille et protège les ordinateurs contre les attaques ;
- **XDR** (Extended Detection and Response ou Détection et Réponse Étendues) protège carrément tout le réseau, et non seulement les ordinateurs ;
- **OT** (Operational Technology ou Technologie Opérationnelle) contrôle les machines industrielles, usines, électricité, transport, etc ;
- **ICS** (Industrial Control Systems ou Systèmes de Contrôle Industriel) surveille et contrôle les équipements et processus dans les environnements industriels ;
- **Segmenter les réseaux OT/ICS ≥70 %** : séparer les réseaux industriels critiques du reste du réseau informatique dans au moins 70 % des cas. Cela permet d'éviter qu'une attaque informatique ne bloque les infrastructures vitales (eau, électricité, pétrole, gaz, etc.) ;

- **Zero trust national** : on ne fait confiance en aucun utilisateur, ni système. Chaque accès est vérifié en permanence dans tous les réseaux du pays ;
- **CTI** (Cyber Threat Intelligence ou Renseignement sur les Menaces Cyber) consiste à collecter, analyser et partager des informations sur les cybermenaces (logiciels malveillants, techniques d'attaque, etc.) afin de les anticiper et les prévenir avant qu'elles ne se produisent ;
- **CEH** (Certified Ethical Hacker ou Hacker Ethique Certifié) est un pentester formé à tester la sécurité et résilience des systèmes informatiques de manière légale et responsable.

En se basant sur les cinq catégories de l'UIT, le Congo pourrait entrer dans le tier 1 en 2035, comme décrit dans les projections[92] de la figure ci-dessus. A condition, toutefois, que **la stratégie ou politique nationale** qui englobe tous les secteurs soit la plus cohérente possible. La formation des élites dans ce secteur est la clé pour que la souveraineté du cyberespace congolais ne soit pas totalement mise entre les mains d'experts étrangers.

92 Ces projections ne reflètent pas une trajectoire absolue pour le Congo. Les hypothèses retenues sont principalement conceptuelles et non quantitatives, et ne prétendent donc pas à la certitude.



IX. IDENTITÉ ET CULTURE NUMÉRIQUES DU CONGO ?

L'identité numérique constitue le socle de la participation citoyenne et institutionnelle dans l'espace digital. Cette section explore ses différentes dimensions - nationale, institutionnelle et individuelle - ainsi que la culture numérique qui les accompagne, afin d'évaluer le niveau d'appropriation et les défis liés à la confiance et aux usages. La culture numérique, de façon générale, fait référence à l'usage des terminaux numériques et aux comportements des personnes dans les espaces digitaux, dont les réseaux sociaux généralistes et professionnels.

9.1. Identité numérique nationale

9.1.1. Le .cg ou le symbole de la présence du Congo dans l'espace numérique mondial

L'identité numérique d'un pays est constituée d'éléments ou traces qui marquent sa présence sur Internet. Il peut s'agir de sites officiels, de services en ligne, etc.

L'identité numérique de la République du Congo est **.cg**. Il représente l'indicatif Internet (ou domaine national) du Congo à partir duquel on peut identifier un site ou une adresse numérique qui appartient à l'espace numérique de la République du Congo. Par analogie, le **.cg** est au numérique ce que le **+242** est à la téléphonie, c'est-à-dire l'indicatif téléphonique international de la République du Congo. Ou encore, on peut considérer le **.cg** comme l'équivalent du drapeau congolais dans l'espace numérique mondial.

Le **.cg** joue donc un rôle important dans l'écosystème de l'économie numérique du pays, à condition qu'il soit davantage pris en compte dans les différentes politiques et stratégies numériques nationales.

9.1.2. Le DNS ou la maîtrise de la sécurité du territoire numérique

Le DNS (Domain Name System ou Nom de Domaine) est un système qui traduit les noms de domaine (*comme www.gouv.cg*) en adresses IP (*comme 197.214.56.23*) compréhensibles par les ordinateurs. Il repose sur des serveurs DNS, c'est-à-dire des machines qui permettent d'enregistrer et de fournir ces informations.

Avoir un DNS, c'est avoir officiellement réservé une adresse sur Internet**.** Et par analogie, on peut dire que le DNS représente l'adresse d'une parcelle (plan cadastral). Par contre, avoir un **site Internet**, c'est construire quelque chose à cette adresse (un bâtiment sur une parcelle cadastrée). On peut donc avoir un DNS sans avoir de site Internet.

Une infrastructure DNS nationale est une clé d'entrée vers l'indépendance ou souveraineté numérique puisqu'elle permet de contrôler l'accès aux ressources Internet locales. Cependant, cette souveraineté n'est pas totale si elle ne s'appuie pas sur des :

- data centers locaux pour héberger les contenus et services ;
- dispositifs de cybersécurité nationaux comme un CERT (Computer Emergency Response Team) ou un SOC (Security Operations Center) pour surveiller, prévenir et réagir aux incidents ;
- politiques de gouvernance numérique claires et souveraines.

Le Congo dispose d'une souveraineté administrative sur le domaine .cg, mais pas d'une souveraineté technique complète. Et tant que les serveurs DNS de premier niveau sont opérés à l'étranger (par DNSAfrica), le pays reste dépendant d'infrastructures externes. En cas de rupture ou de litige, la résolution des noms de domaine en .cg pourrait être compromise, entraînant l'inaccessibilité des services et sites web utilisant cette extension.

En **conclusion**, le Congo gagnerait à héberger et administrer ses propres serveurs DNS sur le territoire national afin d'assurer la maîtrise complète de ses noms de domaine, de renforcer la sécurité de ses données et de garantir son indépendance numérique.

Figure 39 : Criticité des DNS pour la sécurité du cyberespace local

	Situation Actuelle	Conséquences	Axes de Réflexion
Contrôle du DNS National	Le domaine **.cg** est administré depuis l'étranger. Les sous-domaines comme **.gouv.cg** sont gérés localement.	Le Congo ne contrôle pas totalement son adresse Internet nationale.	Reprendre la gestion complète du **.cg** au niveau national (ou la re-délégation du **.cg**)
Sécurité et Souveraineté	Les serveurs principaux sont situés hors du territoire.	Risque de dépendance technique et de perte de maîtrise en cas de litige ou de coupure.	Héberger les serveurs DNS du **.cg** au Congo et créer un CERT national pour renforcer la souveraineté numérique.
Trafic et Données	Le trafic DNS transite à l'extérieur du pays.	Risque de fuite ou d'exploitation de données liées aux activités congolaises en ligne.	Conserver le trafic DNS à l'intérieur du pays via les points d'échange Internet (CGIX).
Résilience du Réseau	Aucune solution locale de secours pour le DNS national.	En cas de problème avec l'opérateur étranger, les sites en **.cg** peuvent devenir inaccessibles.	Héberger une réplique autoritaire du registre **.cg** dans un datacenter national relié au CGIX.

9.1.3. Les points d'échange Internet du Congo (CGIX)

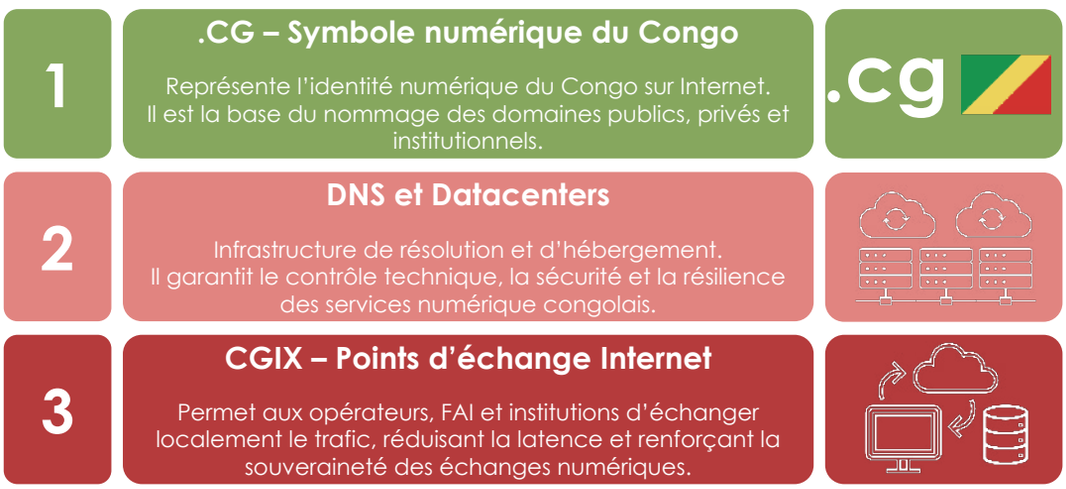
Les CGIX complètent le dispositif formé par le .cg et les serveurs DNS hébergés localement. Le Congo dispose de deux (2) points d'échange Internet localisés à Brazzaville et à Pointe-Noire. Tandis que le .cg représente l'identité numérique du Congo, et que les data centers sont censés assurer l'hébergement et la sécurité des données, les CGIX jouent un rôle essentiel en centralisant le trafic national.

Les CGIX permettent ainsi aux fournisseurs d'accès à Internet (FAI), aux opérateurs, aux administrations, entre autres, d'interconnecter directement leurs réseaux pour échanger du trafic localement, sans transiter par des routes internationales. Cela permet de réduire la latence et d'améliorer la qualité de service.

9.1.4. Synthèse sur l'identité numérique nationale

La figure ci-après résume la portée de chaque couche identifiée comme partie intégrante de l'identité numérique nationale.

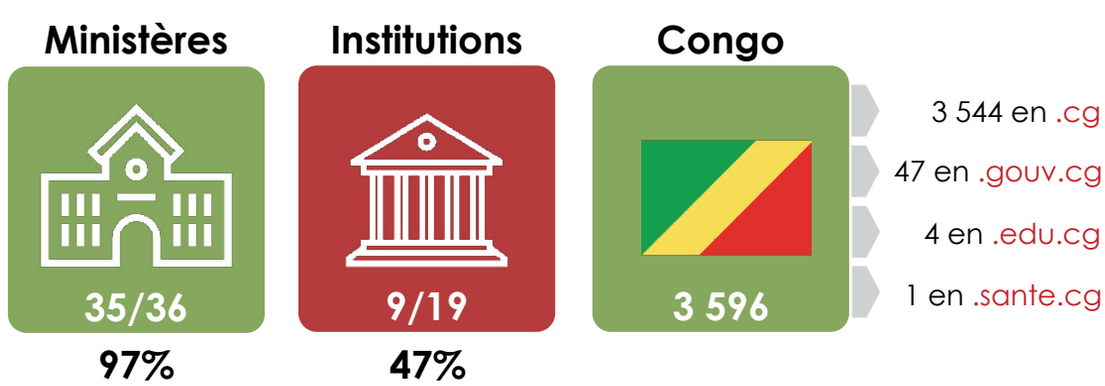
Figure 40 : Trio de l'identité numérique nationale



9.2. Identité institutionnelle

L'identité institutionnelle du Congo peut se mesurer par la proportion d'institutions officielles ayant un nom de domaine en .cg, qu'il soit actif ou non. On entend par institutions officielles celles qui sont présentées sur le site du gouvernement[93]. On peut aussi s'intéresser au nombre de ministères qui ont enregistré un nom de domaine[94] afin de dégager une tendance de l'encrage ou non de l'identité numérique au sein du gouvernement.

Figure 41 : Nombre de noms de domaine enregistrés



Source : ARPCE

On observe que 97% des « ministères » ont enregistré un nom de domaine, contre 47% des « institutions ». Au niveau national, 3 596 noms de domaine[95] ont été enregistrés à date en République du Congo.

93 https://gouvernement.cg/institutions/, site consulté le 10/10/2025.

94 Pour rappel, l'existence d'un nom de domaine ne signifie pas forcément qu'un site web a été activé.

95 Données disponibles au 30 septembre 2025.

Les institutions ont encore des efforts à fournir pour combler leur retard. En revanche, du côté du gouvernement, seul un (1) ministère sur 36 n'a pas encore de nom de domaine. Le gouvernement congolais montre ainsi l'exemple sur le plan administratif, ce qui est un signe encourageant compte tenu de l'importance des noms de domaine pour le cyberespace national.

Une des questions fondamentales est de savoir si tous les ministères et institutions hébergent leurs sites web, messageries et services de partage de fichiers sur des infrastructures nationales, ou bien à l'étranger via des prestataires comme OVHcloud ou LWS ?

Cependant, par rapport à d'autres pays, notamment de population comparable, le nombre total de noms de domaine enregistrés au Congo est insignifiant. Cela peut refléter une confiance limitée dans l'identité numérique nationale, entre autres facteurs. En effet, tous les pays de la figure suivante appartiennent au monde dit « développé », mais avec une population aussi faible que celle du Congo. Ce qui sous-entend qu'un développement économique soutenu peut se concrétiser avec une population de l'ordre de six (6) millions d'habitants.

L'indicateur de performance retenu ici est donc le ratio noms de domaine/population totale. Cet indicateur montre combien de sites Internet nationaux existent pour 1 000 habitants. Plus ce chiffre est élevé, plus cela veut dire que les entreprises, les institutions et les citoyens utilisent le domaine national pour exister sur Internet.

Le Danemark compte 1,3 million de noms de domaine enregistrés pour 5,98 millions d'habitants. Ainsi, on compte environ 216 domaines créés pour 1 000 habitants.

Figure 42 : Noms de domaine par pays de population comparable

Pays	Extension (ccTLD)	Domaines enregistrés	Population (Millions)	Domaines / 1000 hab
Danemark	.dk	1 300 721	5,98	217,6
Norvège	.no	829 132	5,57	148,8
Finlande	.fi	551 962	5,64	97,9
Slovaquie	.sk	464 754	5,42	85,7
Irlande	.ie	326 562	5,38	60,7
Singapour	.sg	203 000	6,11	33,2
Congo	**.cg**	**3 596**	**6,28**	**0,6**

Sources: Internet Society - Singapore Network Information Centre (SGNIC) – Singapore Department of Statistics (Singstat)

Un ratio faible, et c'est le cas du Congo, montre que très peu d'acteurs locaux ont créé une identité numérique nationale avec le **.cg**. Il n'y a que 0,6 domaine créé pour 1 000 habitants.

Cela montre aussi que le développement de l'économie numérique est loin d'être achevé, bien au contraire. C'est pourquoi il faut que l'écosystème d'une économie numérique soit bien maitrisé, et que le pouvoir d'achat des Congolais augmente pour le soutenir.

9.3. Identité numérique individuelle

Il s'agit d'informations qui permettent d'identifier une personne dans de multiples espaces numériques, tout comme la carte d'identité physique le permet dans le monde « réel ou physique ». Elle permet, sur le plan technique, de retracer en temps réel les interactions d'un utilisateur avec les services numériques (portails gouvernementaux ou plateformes privées), par exemple.

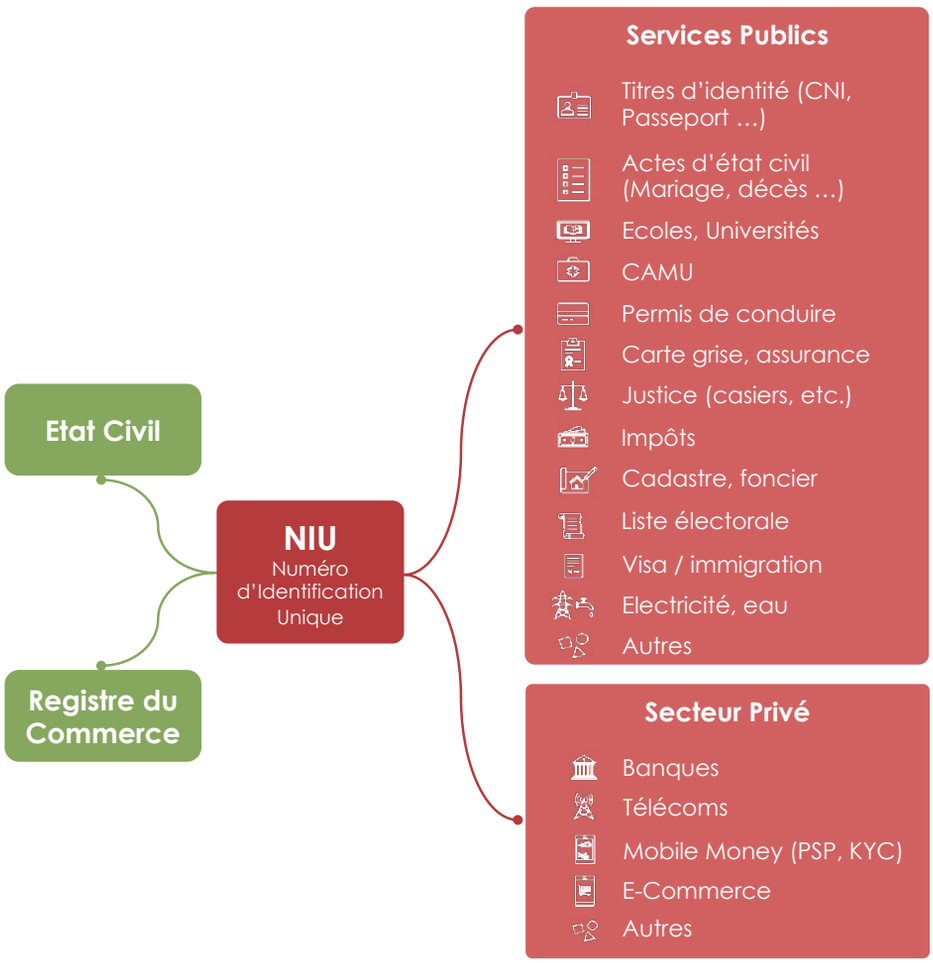
La protection des données étant importante et consacrée dans la réglementation congolaise, ce suivi doit être strictement encadré afin de garantir la transparence des usages et le respect de la vie privée des citoyens.

Au Congo, l'identité numérique individuelle est en cours de structuration. Elle devrait donc être consolidée, notamment par une mise en application plus fine du Numéro d'Identification Unique (NIU) déjà adopté, mais pas encore vraiment généralisé à toute la population et services.

Le NIU est censé être le cœur de l'identité numérique individuelle en République du Congo. Pourquoi ? Parce qu'il devrait relier chaque entité aux différents services numériques tels qu'administratifs, sociaux, de santé, économiques, scolaires, d'état civil, etc. Ce qui signifie que le NIU devrait constituer le socle technique et juridique de **l'e-gouvernement** (services pour une administration numérique), de **l'e-citoyen** (offres de services et contenus numériques pour le grand public) et de **l'e-business** (entreprises connectées favorisant le commerce et la croissance)[96]. Il est donc un maillon fondamental de la transformation numérique du Congo, aussi bien pour les personnes physiques, que pour les personnes morales.

96 Le NIU est un élément constitutif de la *Vision Congo Digitale 2030*, laquelle est la stratégie nationale du numérique mise en place par le gouvernement.

Figure 43 : Le NIU au cœur de la transformation numérique du Congo



On retiendra, néanmoins, que les maillons les plus sensibles du NIU ne sont pas les services connectés (santé, impôts, mobile money, etc.). Le NIU doit se nourrir d'informations capitales à partir des sources d'identité que sont les **mairies** pour les citoyens et les **chambres de commerce** pour les entreprises. Si donc les mairies et les chambres de commerce ne disposent pas d'un système d'information efficace, d'une gouvernance aux normes requises et d'un dispositif de cybersécurité renforcé par le CERT national à déployer, la transformation numérique du Congo pourrait être retardée, voire compromise.

9.4. Culture numérique et usages

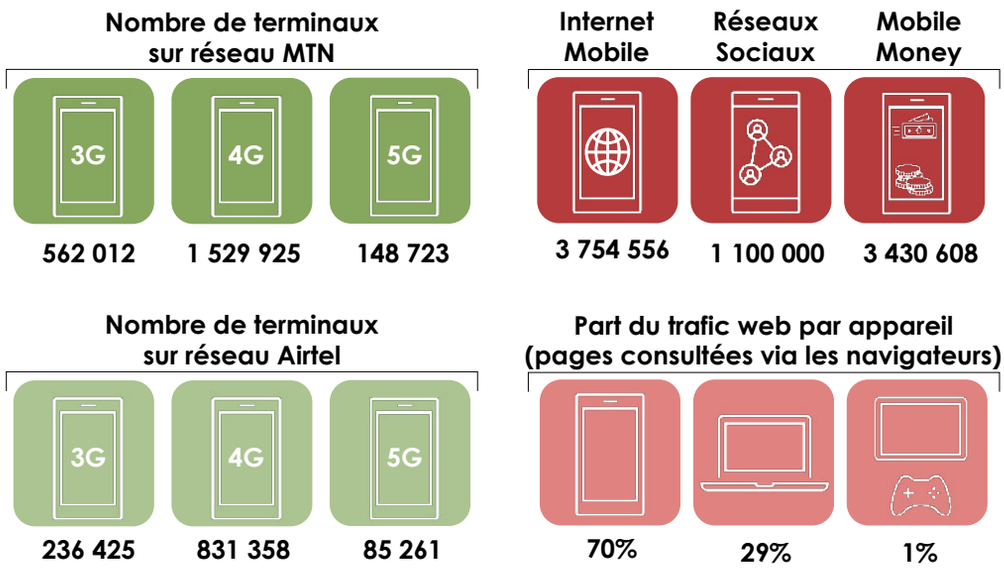
La culture numérique renvoie, comme énoncé supra, à l'utilisation des outils digitaux et aux habitudes et pratiques des individus dans les environnements en ligne ou interactifs comme les réseaux sociaux généralistes ou professionnels.

▶ Des réseaux à l'accès au numérique : les chiffres

Les réseaux des communications électroniques 3G, 4G et 5G permettent d'accéder à Internet et aux plateformes numériques. Les terminaux les plus nombreux sur les réseaux des opérateurs sont ceux de la 4G. Bien qu'il n'ait pas encore lancé officiellement son réseau 5G, l'opérateur Airtel compte environ 85 000 terminaux 5G actifs sur son réseau, contre près de 149 000 pour l'opérateur MTN.

On compte 3,7 millions de personnes qui accèdent à Internet via les smartphones, et environ 1,1 million qui sont actifs sur les réseaux sociaux. Le Mobile Money fait désormais partie des usages, et près de 3,5 millions de Congolais seraient actifs. Enfin, 70 % des internautes accèdent à Internet par leur smartphone, 29 % via des laptops et 1 % par les tablettes ou autres terminaux compatibles.

Figure 44 : Données sur l'usage des technologies au Congo



Sources : ARPCE – Opérateurs – DataReportal

Au Congo, la culture numérique se construit progressivement car portée par la généralisation de la technologie 4G, ainsi que le déploiement récent de la 5G qui favorisent un usage important des réseaux sociaux, du mobile money et des plateformes de divertissement.

▶ Les limites de cette culture numérique congolaise

Le Congo étant un pays jeune par sa population, ce sont donc les jeunes qui sont le plus souvent connectés, et qui participent aux nouveaux espaces numériques d'expression et d'interaction. Or, ces jeunes consomment presqu'essentiellement des services, outils et contenus étrangers. Il y a peu de production locale. C'est donc surtout une consommation ludique et monotone qui se crée. On peut d'ailleurs corréler cette assertion avec le faible taux d'enregistrement des noms de domaine qui montre que l'économie congolaise est encore embryonnaire sur le plan numérique, et qu'elle ne crée pas beaucoup de contenus et de richesses numériques.

Il existe aussi des limites sur le plan de la formation. Employons ici le mot illectronisme. Qu'est-ce que c'est ? Il s'agit de l'exclusion liée à la non-maîtrise des outils numériques d'une part, mais aussi, à l'absence de formation dans les métiers du numérique (pentesters, cyber analystes, intelligence artificielle, etc.). Il faudrait, quand des chiffres plus soutenus seront disponibles sur la question, corréler le taux d'illectronisme à celui de l'analphabétisation. Il ne serait pas surprenant que les deux données soient proches. On peut donc dire que le Congo est connecté, mais reste « illectronique » parce qu'il ne produit pas ses propres experts, développeurs et analystes.

Des limites … aux opportunités

Puisque les infrastructures existent (réseaux de communications électroniques, data centers, points d'échange Internet, etc.), et que le Congo a une identité numérique (le .cg), etc., ne pas développer une culture entrepreneuriale, donc une appropriation économique du numérique, constitue une faiblesse stratégique.

Le Congo, au final, ne serait-il qu'un pays connecté qui doit encore muer vers une économie réellement numérique ? C'est une vraie question qu'il faut se poser au regard des différents aspects évoqués tout au long de cet ouvrage.

Quoi qu'il en soit, il paraît urgent de prendre très au sérieux la formation du capital humain dans les métiers du numérique. Car c'est avec des esprits bien formés sur le plan local, mais avec une ouverture et une compréhension des problématiques mondiales, qu'il devrait être possible de créer une société numérique porteuse de sa propre identité et d'une partie, tout au moins, de sa souveraineté numérique.







X. INCLUSION NUMÉRIQUE DES FEMMES ?

L'inclusion numérique des femmes est un enjeu majeur de développement et d'équité dans la transformation numérique du Congo. Cette section analyse les facteurs qui favorisent ou freinent leur participation — couverture réseau, pouvoir d'achat, alphabétisation et accès aux métiers du numérique — afin d'identifier les leviers d'une inclusion réelle et durable.

10.1. Couverture réseau : inclusion ou exclusion des femmes ?

Les infrastructures ou technologies télécoms desservent les populations de manière uniforme, hommes et femmes confondus. En d'autres termes, la couverture des populations n'est pas genrée. Toutes les personnes couvertes peuvent donc prétendre accéder aux mêmes services fournis par les opérateurs ou fournisseurs de services de communications électroniques. On peut donc conclure qu'il n'y a pas de discrimination ou d'exclusion de genre en termes de couverture puisque les fréquences ou la fibre optique ne distingue pas les personnes couvertes en fonction de leur sexe.

En 2023, la population congolaise a été estimée à 6 142 180 habitants, dont 49,66 % d'hommes et 50,34 % de femmes[97]. Il y a donc presqu'autant d'hommes qu'il y a de femmes en République du Congo. De même, dans les zones couvertes, autant de femmes que d'hommes peuvent bénéficier des services de communications électroniques.

10.2. Pouvoir d'achat et alphabétisation

Lorsqu'une zone est couverte, l'accès au réseau dépend d'au moins deux facteurs que sont le pouvoir d'achat et le taux d'alphabétisation.

- **Pouvoir d'achat**

L'usager - homme ou femme - doit acquérir un terminal d'accès (portable, tablette, etc.) afin de se connecter au réseau. Il doit également disposer de moyens financiers suffisants pour s'offrir les services proposés par les opérateurs.

Dans son rapport sur le développement humain de 2025, le PNUD[98] présente le revenu national brut (RNB) en parité du pouvoir d'achat (PPA) en dollars entre les hommes et les femmes en République du Congo : 4 214 dollars pour les femmes et 7 591 dollars pour les hommes. Avec ces données, converties en F CFA au taux annuel moyen de 554,82 XAF pour 1 dollar[99] en 2021, on obtient 2 338 011 F CFA pour les femmes et 4 211 639 F CFA pour les hommes. En somme, les hommes gagnent environ 1,8 fois plus que les femmes au Congo.

97 Institut National de la Statistique (INS), *Cinquième Recensement Général de la Population et de l'Habitation (RGPH-5),* Résultats Préliminaires, Décembre 2023, p.15.

98 Selon le PNUD (Human Development Report 2025, données issues de la Banque mondiale 2024, converties en dollars PPA 2021 et estimées par genre par le PNUD), le revenu national brut par habitant du Congo est de 4 214 $ pour les femmes et de 7 591 $ pour les hommes.

99 https://www.exchangerates.org.uk/USD-XAF-spot-exchange-rates-history-2021.html, site consulté le 07/09/2025.

En 2023, on estime que 84 % des hommes disposent d'un téléphone portable, contre 80 % des femmes[100]. Cet écart de 4 points entre les hommes et les femmes s'explique en grande partie par les écarts de revenus entre hommes et femmes, certes ; mais aussi à cause du taux d'alphabétisation qui reste en faveur des hommes.

- **Taux d'alphabétisation et usages**

Si l'usager ne sait ni lire ni écrire, il aura du mal à utiliser le terminal qu'il a acquis. Le pouvoir d'achat ne suffit donc pas à accéder aux services de communications électroniques lorsque l'usager est illettré. En 2021, on estimait le taux d'alphabétisation chez les femmes de 15 ans et au-delà à 75,31 % contre 85,95 % chez les hommes[101]. Cet écart de 10,67 points entre les femmes et les hommes montre qu'il existe une forte inégalité en termes d'accès à l'éducation. Or, il y a quasiment autant de femmes que d'hommes au Congo. C'est pourquoi cet écart ne devrait pas se justifier, a priori.

Les personnes lettrées étant les plus susceptibles d'accéder aux services des opérateurs de téléphonie mobile et des fournisseurs d'accès à Internet, on compte 42,5 % de femmes qui utilisent les réseaux sociaux, contre 57,5 % d'hommes[102]. En termes d'usage, le gap dans l'utilisation des réseaux sociaux est de 15 points, encore plus élevé que l'écart entre les femmes et les hommes en rapport avec le taux d'alphabétisation.

On note également que 16,5 % des femmes ont un compte ouvert dans une banque classique, contre 19,8 % d'hommes. Cependant, 32,5 % des femmes ont un compte mobile money, contre 41,2 % d'hommes. Or, les comptes « mobile money » sont également associés à des comptes bancaires. Il s'agit en fait de transactions bancaires, mais qui passent par les réseaux des opérateurs de téléphonie mobile (MTN et Airtel).

Les paiements digitaux deviennent ainsi plus accessibles car le taux de bancarisation est désormais bien plus élevé que celui qui ne prenait en compte que la tenue d'un compte dans une banque classique. Toutefois, il existe toujours des écarts significatifs entre les hommes et les femmes dans les paiements digitaux. Les chiffres disponibles indiquent que 40 % des femmes font des paiements digitaux, contre 46,4 % des hommes. Et que 26,4 % des femmes ont utilisé un téléphone mobile ou bien Internet pour transférer (envoyer) de l'argent, contre 32,7 % des hommes.

10.3. Inclusion et promotion des femmes dans le numérique

Les écarts constatés ci-dessus reflètent une différence notable entre les hommes et les femmes dans l'accès et l'usage des outils et services numériques. Pour qu'elles soient autant présentes que les hommes, il faudrait réduire le gap entre les femmes et les hommes dans l'accès à l'éducation afin de réduire l'analphabétisme chez les femmes. Il est également essentiel que les femmes accèdent davantage aux filières à forte valeur ajoutée, notamment - mais pas exclusivement - dans les domaines STEM (sciences, technologies, ingénierie et mathématiques).

100 Dépêche No. 972 d'Afrobarometer, Margaret Eduonoo, *Les Congolais sont favorables à davantage d'efforts en matière d'égalité des sexes, notamment dans l'arène politique*, 2025, p.3.

101 https://donnees.banquemondiale.org/indicator/SE.ADT.LITR.MA.ZS?end=2021&locations=CG&name_desc=-false&start=2021&view=map, site consulté le 07/09/2025.

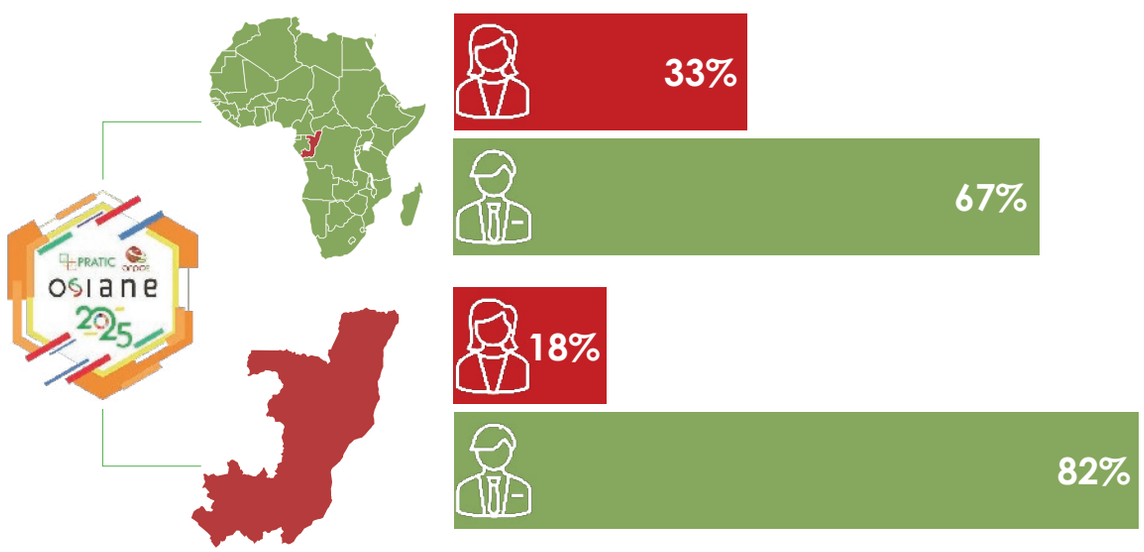
102 https://datareportal.com/reports/digital-2025-republic-of-the-congo, site consulté le 07/09/2025.

C'est peut-être à ce prix que les écarts en termes de revenus se resserreront entre les sexes. Toutefois, comme le montre le rapport du PNUD cité en référence, les écarts de revenus entre les hommes et les femmes ne sont pas l'apanage des pays Africains.

Le positionnement des femmes dans les espaces de conception et d'innovation doit, en revanche, être encouragé. Peu de femmes sont créatrices de start-ups numériques ou porteuses de projets technologiques à fort impact. En effet, à peine 33 % de femmes faisaient partie de la liste internationale[103] des tech-entrepreneurs retenus pour participer au Challenge Startup Bassin du Congo organisé au cours de l'édition 2025 du Salon International de la Tech et de l'Innovation de l'Afrique Centrale (Osiane).

En ramenant cette liste aux seuls représentants de la République du Congo, à peine deux (2) femmes ont présenté des projets, contre neuf (9) hommes ; soit 18 % des tech-entrepreneurs de la délégation du Congo au salon Osiane.

Graphique 2 : Représentativité genrée des start-uppeurs finalistes au Salon Osiane



Source : Osiane

Cette faible présence des femmes dans les métiers de la « tech » tend à prouver qu'elles sont déjà moins scolarisées que les hommes ! Mais est-ce l'unique raison ? Dans tous les cas, il revient aux pouvoirs publics de renforcer les efforts entrepris afin de réduire ce clivage entre hommes et femmes.

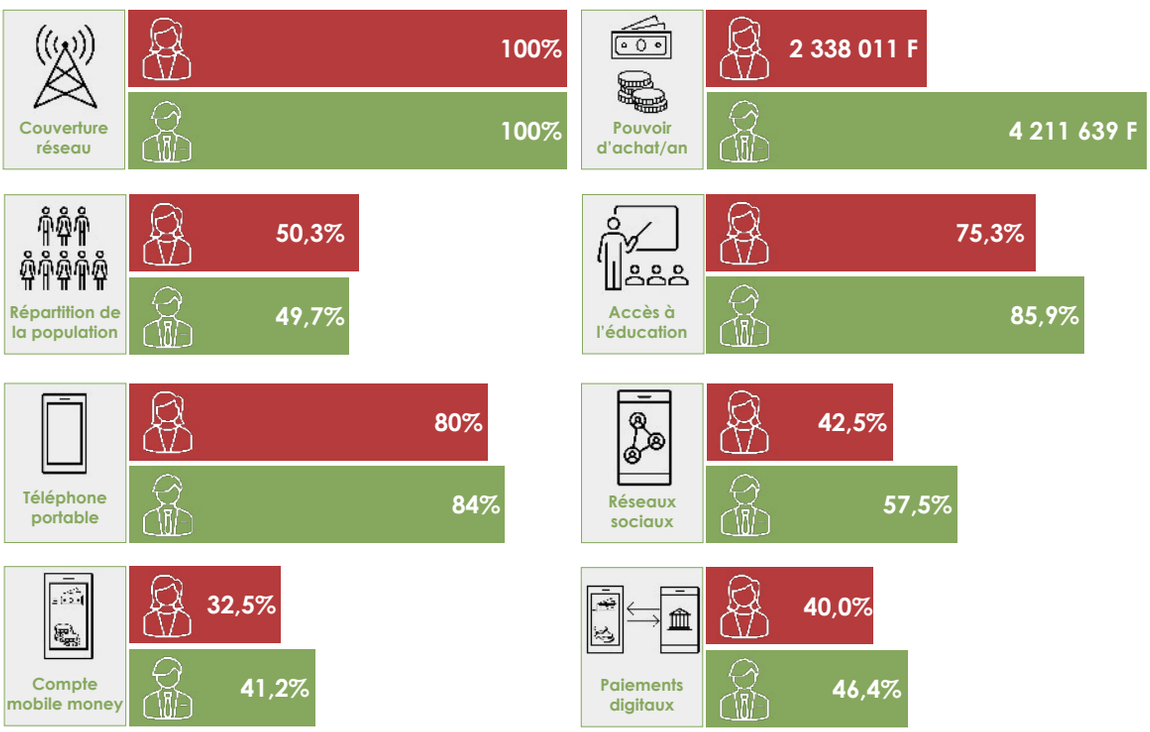
Une des solutions possibles pour combler ce déficit consisterait à identifier et à valoriser davantage de modèles féminins de réussite afin de les mettre en lumière de sorte que plus de femmes s'engagent dans les métiers du numérique ; ce qui suppose aussi qu'elles soient plus présentes dans les filières scientifiques et technologiques.

À compétences égales - voire parfois supérieures - les femmes devraient aussi pouvoir accéder aux instances stratégiques où se décident les grandes orientations du numérique, telles que les ministères, les comités de direction des opérateurs, ou encore les différentes agences ou organes de régulation de l'écosystème numérique.

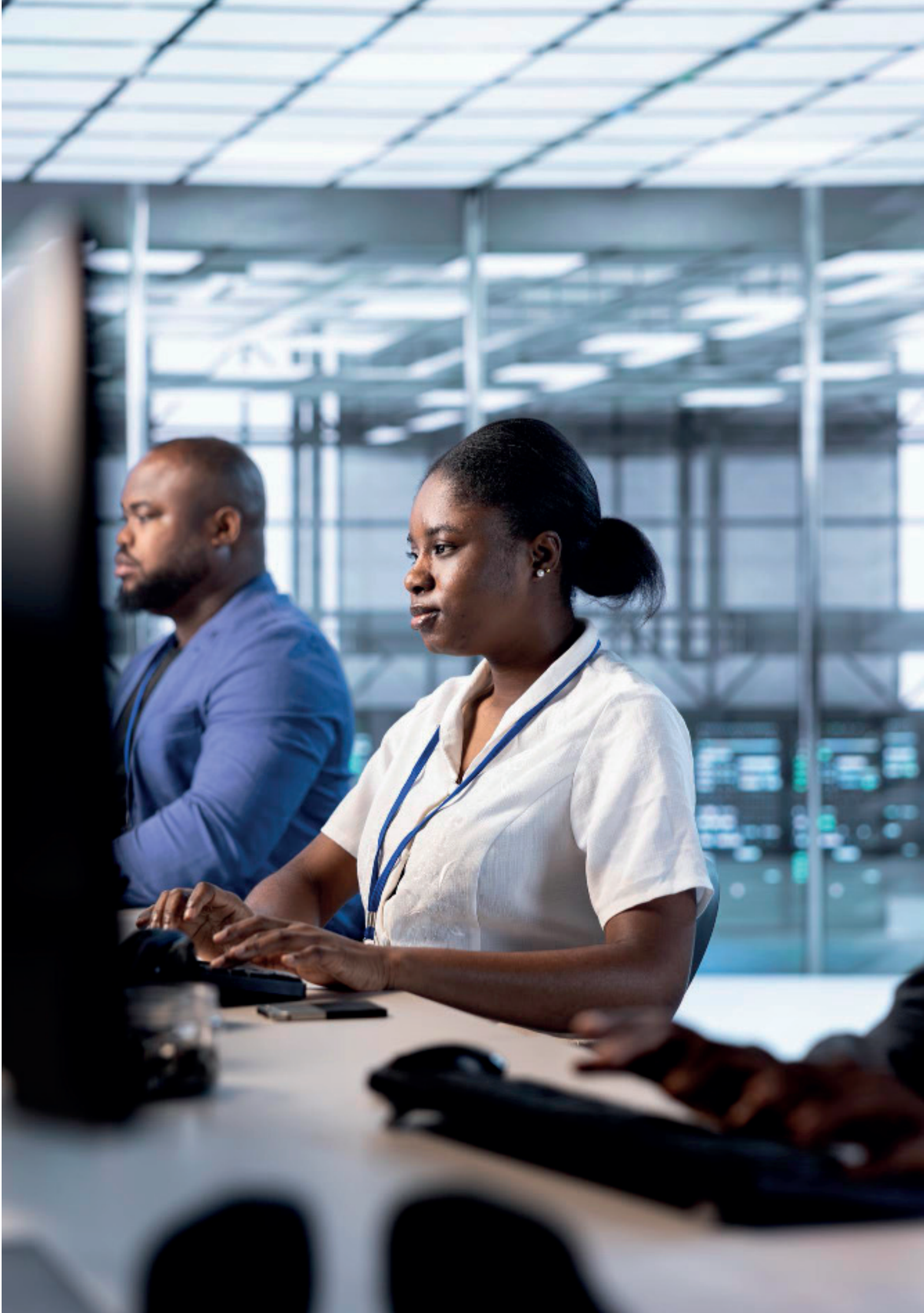
103 15 femmes sur 46 tech-entrepreneurs venus de plusieurs pays d'Afrique.

Cette inclusion est essentielle pour garantir une gouvernance numérique plus équitable et représentative. En effet, l'infographie ci-dessous résume assez bien certaines disparités qui existent entre les hommes et les femmes en République du Congo dans le secteur du numérique.

Graphique 3 : Niveau d'inclusion des femmes dans le numérique au Congo



Sources : Banque Mondiale – Datareportal – PNUD




ECURE
AYMENT



CONCLUSION

Le présent Livre Blanc met en lumière les fondements, les défis et les perspectives du développement numérique du Congo.

Il souligne la nécessité d'une approche intégrée où les dimensions technologique, réglementaire, énergétique, économique, sécuritaire et sociale sont pensées comme des composantes indissociables d'un même écosystème.

Sur le **plan institutionnel**, le Congo dispose désormais d'une base légale et réglementaire qui permet déjà d'encadrer les communications électroniques et l'économie numérique. Les progrès réalisés depuis 2009 témoignent d'une volonté constante de structurer le secteur afin qu'il soit crédible.

Cependant, la rapidité des innovations — 5G, 6G, intelligence artificielle, Internet des objets, métavers, crypto-actifs, réseaux non terrestres — impose d'accélérer l'adaptation du cadre juridique et des institutions. La cohérence des politiques publiques et la coordination interinstitutionnelle demeurent des leviers essentiels pour garantir une gouvernance efficace du numérique.

Sur **le plan analytique**, le diagnostic dressé par ce Livre Blanc fait ressortir plusieurs réalités qu'il faut considérer avec objectivité. Il s'agit, notamment :

- des infrastructures énergétiques qui sont peu résilientes, et ne répondent pas encore aux standards internationaux ;
- des disparités territoriales et sociales qui ne favorisent pas toujours un accès équitable aux services numériques ;
- du déficit de compétences techniques et de capacités locales d'innovation et d'industrialisation ;
- et du niveau encore modeste de préparation aux technologies émergentes.

Ces constats appellent des réponses structurées qui passent par la modernisation des infrastructures, le plein usage des sources d'énergie, le renforcement de la cybersécurité, le développement du capital humain et la concrétisation d'une inclusion numérique équitable.

Sur **le plan prospectif**, la transformation numérique du Congo ne doit pas se limiter à l'adoption d'outils technologiques. Elle doit s'inscrire dans une vision de souveraineté et de durabilité. Le numérique doit être un vecteur de diversification économique, de transparence administrative et d'intégration régionale. La souveraineté numérique, quant à elle, suppose la maîtrise des infrastructures critiques, la localisation des données sensibles et la protection du cyberespace national.

L'avenir du numérique congolais dépendra de la capacité collective de l'État, des opérateurs, du secteur privé, des chercheurs et de la société civile à conjuguer leurs efforts pour atteindre un but commun.

Ce Livre Blanc, loin d'être une fin en soi, constitue une des nombreuses étapes vers une planification continue, une gouvernance plus intégrée et une veille technologique active dans les secteurs des télécommunications et du numérique.

TABLE DES ILLUSTRATIONS

Figures

Figure 1 : Entités dans le secteur des postes, des télécommunications et de l'économie numérique 27

Figure 2 : Évolution prospective du cadre légal de l'économie numérique 28

Figure 3 : Enjeux des mutations technologiques 30

Figure 4 : Positionnement du Congo par rapport aux évolutions technologiques et réglementaires des télécommunications 33

Figure 5 : Niveau de préparation du Congo à la transformation numérique 35

Figure 6 : Enjeux de la régulation du futur 36

Figure 7 : Cartographie des centrales de production énergétique 40

Figure 8 : Évolution planifiée de certains indicateurs électriques 42

Figure 9 : Disponibilité moyenne quotidienne du réseau électrique (en heures) sur les sites et par pays 43

Figure 10 : Scénarios d'alimentation des sites télécoms 44

Figure 11 : Évolution du mix et des coûts énergétiques 44

Figure 12 : Cartographie des principales infrastructures télécoms de l'économie numérique 50

Figure 13 : Prérequis stratégiques pour le déploiement des technologies émergentes 51

Figure 14 : Quelques fondamentaux de la régulation numérique 54

Figure 15 : Évolutions des technologies 5G 58

Figure 16 : Évolutions des technologies 6G 59

Figure 17 : Description générale des NTN 61

Figure 18 : Ressources spectrales pour les réseaux d'accès des opérateurs de téléphonie mobile et autres services innovants 62

Figure 19 : Ressources satellitaires (orbite/spectre) enregistrées et réservées pour la République du Congo 63

Figure 20 : Evolutions et usages des technologies émergentes 64

Figure 21 : Part des terminaux 5G au Congo sur les réseaux de téléphonie mobile d'Airtel et MTN 66

Figure 22 : Déploiement actuel et futur des technologies dans le monde vs au Congo 68

Figure 23 : Alternatives aux technologies terrestres et couverture nationale accélérée 70

Figure 24 : Localisation des centres de données de Meta 75

Figure 25 : Localisation des centres de données de TikTok 76

Figure 26 : Localisation des centres de données de Netflix et Amazon Prime Video 77

Figure 27 : Localisation des centres de données de Google 78

Figure 28 : Princes de souveraineté numérique 82

Figure 29 : Ventilations d'une partie du chiffre d'affaires de Google par pays 85

Figure 30 : Revenus Google par internaute et impact économique 2023 86

Figure 31 : Rapport de force asymétrique entre le Congo et les géants du numérique 88
Figure 32 : Types de données de souveraineté 89
Figure 33 : Chaîne de souveraineté des données 90
Figure 34 : Souveraineté numérique versus économie numérique 91
Figure 35 : Niveau de maturité du Congo dans la cybersécurité 95
Figure 36 : Détails de la note du Congo pour le Tier 4 96
Figure 37 : Analogie « Maison » et Cybersécurité au Congo 98
Figure 38 : Maturité du Congo en cybersécurité à l'horizon 2035 ! 100
Figure 39 : Criticité des DNS pour la sécurité du cyberespace local 104
Figure 40 : Trio de l'identité numérique nationale 105
Figure 41 : Nombre de noms de domaine enregistrés..... 105
Figure 42 : Noms de domaine par pays de population comparable 106
Figure 43 : Le NIU au cœur de la transformation numérique du Congo..... 108
Figure 44 : Données sur l'usage des technologies au Congo 109

Graphiques

Graphique 1 : Indicateurs de comparaison entre l'Afrique sub-saharienne et 3 pays de l'Union Européenne 92
Graphique 2 : Représentativité genrée des start-uppeurs finalistes au Salon Osiane.....115
Graphique 3 : Niveau d'inclusion des femmes dans le numérique au Congo.....116

Tableaux

Tableau 1 : Télécommunications versus communications électroniques.....20
Tableau 2 : Cadre législatif du secteur des postes, des télécommunications et de l'économie numérique 25
Tableau 3 : Cadre réglementaire du secteur des postes, des télécommunications et de l'économie numérique 26
Tableau 4 : Politique comparée de gestion des données des utilisateurs 74
Tableau 5 : Sanctions contre les géants mondiaux du numérique 80
Tableau 6 : Synthèse comparative des législations (Congo - UE - Chine).....84

BIBLIOGRAPHIE

1. ARPCE, *Livre Blanc des Postes, des Télécommunications et de l'Economie Numérique*, 2021.
2. Banque des Etats de l'Afrique Centrale (BEAC), *Rapport Annuel 2023.*
3. Eduonoo, Margaret, *Les Congolais sont favorables à davantage d'efforts en matière d'égalité des sexes, notamment dans l'arène politique,* Dépêche No. 972, Afrobarometer, 15 avril 2025.
4. Ericsson White Paper, *5G Advanced: Evolution towards 6G*, BNEW-22:024836 Uen, June 2023.
5. Google, *Economic Impact, United States by the numbers*, 2023.
6. Google, *Economic Impact, United States by the numbers*, 2024.
7. GSMA, *5G mmWave, A resource for Operators*, February 2022.
8. GSMA, *L'économie du mobile en Afrique subsaharienne*, 2024.
9. Helios Towers, *Annual Report and Financial Statements*, 2023.
10. Helios Towers, *Annual Report and Financial Statements*, 2024.
11. Helios Towers, *Reporting Supplement to the Annual Report and Financial Statements*, 2023.
12. Huawei Technologies USA, *Internet 2030, Towards a New Internet for the Year 2030 and Beyond*, written by Future Networks Team for ITU-T, SG 13.
13. Institut National de la Statistique (INS), *Résultats Préliminaires du 5e Recensement Général de la Population et de l'Habitation*, Décembre 2023.
14. ITUPublications, *Etude de cas : La régulation collaborative au Sénégal*, 2022.
15. ITUPublications, *Global Cybersecurity Index 2024*, 5th Edition.
16. ITUPublications, *Manuel sur la Réglementation du Numérique*, 2020.
17. Ministère des Postes, des Télécommunications et de l'Economie Numérique, *Stratégie Nationale du Numérique, Vision Congo Digital 2030.*
18. Ministère des Postes, des Télécommunications et de l'Economie Numérique, *Stratégie Nationale de Cybersécurité.*
19. Plan National de Développement (PND) 2022-2026, Annexe n°2, Programme Pluriannuel des Actions Prioritaires.
20. PublicFirst, *Google's Economic Impact in the EU 2023*, September 2023.
21. Zhuangzhuang Cui, Peize Zhang, and Sofie Pollin, *6G Wireless Communications in 7-24 GHz Band : Opportunities, Techniques, and Challenges*, arXiv:2310.06425v2 [eess.SY] 2 June 2024.

AGENCE DE RÉGULATION DES POSTES ET DES COMMUNICATIONS ÉLECTRONIQUES

AUTEUR

Louis-Marc SAKALA
Directeur Général

RÉDACTION ET CHEF DE PROJET

Lenda Rudy MASSAMBA
Directeur des Projets et de la Prospective

ONT CONTRIBUÉ À L'ÉLABORATION DU LIVRE BLANC

Wilson Emery BOKATOLA
Directeur des Ressources en Fréquences

Jean Célestin ENDOKE
Directeur des Affaires Juridiques et Internationales

Jean Arnaud NGOUA
Directeur Service financier mobile

Love SARA AHOUI NDEKE
Conseillère en Communication et Relations Publiques du Directeur Général

Marga DEMBI
Cheffe de Bureau Prospective Économique

Christa NGOMA
Assistante du Directeur des Projets et de la Prospective

MISE EN PAGE

Dodo Albert NGOYI
Chef de Bureau Communication Digitale et Design

© 2025 ARPCE – Tous droits réservés



© 2025 ARPCE – Tous droits réservés



CONTACT

+242 05510 7272

91 Bis Avenue de l'Amitié

2490 Centre Ville, Brazzaville
République du Congo

www.arpce.cg

arpce Congo