ÉTUDE SUR LA SOUVERAINETÉ NUMÉRIQUE DE LA RDC

Une étude faite par **CYBERASTRE**



crédit photo LeonardJospin1

[redacted]

crédit photo LeonardJospin1

Copyright Août 2025 office@cyberastre.com

 Copyright Août 2025 office@cyberastre.com

TABLE DES MATIERES

Étude sur la Souveraineté Numérique de la RDC – Rapport Cyberstratégique 3

1. Contexte et Problématique de la Souveraineté Numérique en RDC 4

2. Public Concerné par le Manque de Souveraineté Numérique 7

3. Plan d'Action Réaliste – Rapatrier les Données Nationales via un Partenariat Public-Privé (PPP) 11

3.1 Architecture Technique Proposée pour un Cloud Souverain (Data Center Tier III/IV) 11

3.2 Estimation des Coûts d'Infrastructure (Construction, Équipements, Connectivité, Maintenance) 14

3.3 Localisation Stratégique du Data Center – Choix du Site (Kinshasa, Lubumbashi, Goma ?) 17

3.4 Modèle Économique et Retour sur Investissement (ROI) pour le PPP 19

4. Livrable – Vers un Cahier des Charges pour une Infrastructure Stratégique 25

 Copyright Août 2025 office@cyberastre.com

ÉTUDE SUR LA SOUVERAINETÉ NUMÉRIQUE DE LA RDC – RAPPORT CYBERSTRATÉGIQUE

 Copyright Août 2025 office@cyberastre.com

1. CONTEXTE ET PROBLÉMATIQUE DE LA SOUVERAINETÉ NUMÉRIQUE EN RDC

La **République Démocratique du Congo (RDC)** fait face à une perte de souveraineté numérique alarmante. En l'absence d'infrastructures locales robustes, la quasi-totalité des données et du trafic Internet congolais transite par l'étranger. En 2019 encore, **aucun centre de données national de niveau international (Tier III ou IV)** n'existait sur le territoire DROITNUMERIQUE.CD. Cela signifie que les services numériques du pays s'appuyaient essentiellement sur des serveurs hébergés hors des frontières. On estime que **plus de 95 % des flux numériques congolais empruntent des infrastructures étrangères**, faute de centres de données locaux et de points d'échange Internet suffisants INTERNETSOCIETY.ORG. Concrètement, un simple email entre deux Congolais pouvait, jusqu'à récemment, transiter par l'Europe ou l'Asie avant d'arriver, augmentant latence et coûts.

Plusieurs **services critiques sont hébergés à l'étranger**, exposant le pays à des risques majeurs. Par exemple, de nombreuses institutions et entreprises en RDC utilisent les services de géants du numérique (*Big Tech*) tels que **Google, Meta (Facebook)** ou **TikTok**, ce qui signifie que les données des utilisateurs congolais (courriels, données sur les réseaux sociaux, vidéos, etc.) résident dans des centres de données hors RDC. Jusqu'en 2024, le pays ne disposait pas d'un cloud national capable d'héberger ces services critiques. Les banques congolaises, les compagnies de télécommunications et même certaines agences gouvernementales ont souvent dû louer des serveurs à l'étranger ou utiliser des plateformes cloud internationales pour leurs applications internes, ce qui pose des problèmes de **sécurité des données** et de **dépendance technologique**.

La **dépendance vis-à-vis des Big Tech** est ainsi très élevée. Par exemple, les réseaux sociaux étrangers dominent : on comptait **6,45 millions d'utilisateurs de médias sociaux** (Facebook, WhatsApp, Instagram, etc.) en RDC début 2024 DATAREPORTAL.COM, soit environ 6 % de la population totale. Toute cette activité repose sur des plateformes dont les centres de données se trouvent hors du pays (États-Unis, Europe, Asie). De même, le trafic Internet local est fortement orienté vers des contenus externes (YouTube, Google Search, TikTok…), hébergés sur des serveurs étrangers. Faute d'infrastructure nationale, **les caches locaux de contenu** (qui stockent en RDC les données fréquemment accédées) sont quasi inexistants, obligeant les fournisseurs d'accès à Internet à échanger le trafic à l'international.

Cette situation engendre des **coûts élevés** et une **vulnérabilité stratégique**. Le coût de la bande passante internationale pèse lourdement sur les FAI congolais et donc sur les prix payés par les usagers INTERNETSOCIETY.ORG. En outre, la moindre coupure des câbles sous-marins reliant le pays

(par exemple le câble WACS, seule liaison océanique disponible jusqu'en 2021) provoque d'énormes perturbations. Une analyse de la Banque mondiale souligne d'ailleurs que la RDC a longtemps souffert d'un *point de défaillance unique* : le câble WACS, dont les coupures fréquentes ont isolé le pays à plusieurs reprises THEDOCS.WORLDBANK.ORG THEDOCS.WORLDBANK.ORG. Cela illustre à quel point **l'absence de souveraineté numérique** – c'est-à-dire la capacité à gérer et stocker localement ses données et son trafic – peut paralyser l'économie numérique congolaise.

Depuis 2019, les autorités congolaises ont pris conscience de ce retard. Le **Plan National du Numérique Horizon 2025** identifiait la création de centres de données souverains comme une priorité absolue 7SUR7.CD. En 2020, la RDC a promulgué un *Code du Numérique* qui impose que les **données produites sur le territoire national** soient stockées en RDC même (exigence de souveraineté des données) 7SUR7.CD. Toutefois, faute d'infrastructures adéquates, cette loi était difficile à appliquer jusqu'à récemment. Ce n'est qu'en **2024** que le pays a vu l'inauguration de ses premiers data centers de classe mondiale, marquant un tournant dans la reprise de contrôle de son patrimoine numérique.

En août 2024, un consortium privé a ouvert à Kinshasa le **premier centre de données Tier III** du pays, OADC Texaf Digital, d'une capacité initiale de 2 MW 7SUR7.CD. Quelques jours plus tard, la société Raxio a inauguré un autre data center Tier III à Kinshasa (Raxio DRC1). Ces infrastructures, certifiées par l'Uptime Institute, offrent enfin la possibilité d'héberger localement des services jusqu'ici externalisés. OADC-Texaf, par exemple, est un centre *Open Access* neutre vis-à-vis des opérateurs, conçu pour accueillir aussi bien les banques et opérateurs télécom locaux que les **fournisseurs cloud internationaux (Google, Microsoft, Meta, ByteDance)** qui souhaiteraient y déployer des serveurs 7SUR7.CD. Ces avancées répondent à l'exigence légale et stratégique de souveraineté : *« le code du numérique impose la souveraineté nationale sur les données [...]. Pour que cela soit possible, il faut une infrastructure pour accueillir ces données »* rappelle Christophe Evers, dirigeant du data center OADC Texaf 7SUR7.CD.

En résumé, l'état des lieux en 2025 montre une **prise de conscience aiguë** du déficit de souveraineté numérique en RDC. Plus de *95 % du trafic Internet congolais* sort toujours du territoire, exposant données et communications nationales à des juridictions étrangères. Cette dépendance concerne l'ensemble des secteurs – de la vie quotidienne des citoyens à la finance, l'éducation et l'administration – et nécessite une réponse stratégique urgente. Les premières pierres (juridiques et infrastructurelles) ont été posées pour rapatrier les données et développer un **cloud souverain congolais**, mais le chemin à parcourir reste important pour inverser la tendance et garantir que l'économie numérique congolaise repose sur des bases nationales sécurisées.



crédit photo LeonardJospin1
Copyright Août 2025 office@cyberastre.com

 Copyright Août 2025 office@cyberastre.com

2. PUBLIC CONCERNÉ PAR LE MANQUE DE SOUVERAINETÉ NUMÉRIQUE

La perte de souveraineté numérique en RDC touche **un large pan de la population et des acteurs socio-économiques**, dont voici les principaux segments concernés :

- **Citoyens et usagers des services numériques :** Avec l'essor de la téléphonie mobile et d'Internet, des dizaines de millions de Congolais sont désormais connectés. En janvier 2024, on dénombrait **28,31 millions d'internautes** en RDC, soit un taux de pénétration d'environ 27,2 % de la population DATAREPORTAL.COM. Ce chiffre, en forte progression (le taux n'était que de **1,9 % en 2013**, et 30,4 % en 2023 AFRICA24TV.COM), illustre la dépendance grandissante de la population aux services en ligne : réseaux sociaux, messagerie, actualités, divertissement, etc. Or, l'essentiel de ces services (Facebook, YouTube, WhatsApp, TikTok…) sont fournis par des plateformes étrangères. Chaque utilisateur congolais de Facebook – ils sont plus de **6,4 millions d'utilisateurs actifs sur les réseaux sociaux** début 2024 DATAREPORTAL.COM– voit ses données personnelles (profil, photos, messages) hébergées dans des centres de données hors RDC. La même réalité vaut pour les emails (souvent gérés via Gmail, Outlook), les contenus vidéo (YouTube, TikTok) ou même les applications de messagerie. Les citoyens sont donc directement concernés : leur **vie privée numérique** et la **qualité de service** (temps de réponse, disponibilité) dépendent de cette infrastructure extérieure. En cas de panne des liaisons internationales ou de décision unilatérale d'une Big Tech, c'est l'utilisateur lambda en RDC qui se retrouve coupé de ses services essentiels.

- **Clients des services financiers et bancaires :** La **banque en ligne, le paiement mobile et les fintech** ont connu un essor notable. La RDC a enregistré une forte progression des services de **mobile money**, passant d'environ 6,7 millions d'abonnés mobile money en 2017 à plus de 9 millions en 2018 DROITNUMERIQUE.CD(et ce chiffre a continué d'augmenter dans les années suivantes). Des millions de citoyens utilisent quotidiennement **M-Pesa, Airtel Money, Orange Money** ou des applications de transfert de fonds pour payer des biens, envoyer de l'argent à la famille ou régler des factures. Or, ces plateformes s'appuient sur des infrastructures techniques souvent hébergées hors du pays ou centralisées par région. Par exemple, le cœur de la plateforme M-Pesa n'est pas nécessairement hébergé en RDC même, ce qui pose des questions de disponibilité en cas de coupure internationale et de contrôle sur les données financières des utilisateurs. De plus, les banques commerciales congolaises commencent à proposer des applications mobiles et de l'e-banking : si ces applications utilisent des services cloud (pour l'hébergement des serveurs bancaires, des bases de données clients, etc.), elles recourent souvent à des data centers en Europe ou en Afrique du Sud, faute d'alternative

locale. Les **clients bancaires** (entreprises et particuliers) sont donc exposés – par exemple, des informations sensibles comme les soldes de compte ou historiques de transactions peuvent transiter par des réseaux étrangers. Un manque de souveraineté numérique fragilise aussi la **résilience du système financier** : une cyberattaque outre-frontière ou un litige géopolitique pourrait entraver l'accès aux données bancaires congolaises si elles résident en dehors du pays.

- **Étudiants, élèves et enseignants – Éducation à distance :** La pandémie de COVID-19 a montré l'importance de l'**enseignement à distance** et de l'**e-learning** en RDC, mais aussi ses limites. Durant les confinements de 2020, des initiatives comme la "classe télévisée" ou les cours par radio ont tenté de pallier la fermeture des écoles CD.AMBAFRANCE.ORG UNICEF.ORG. Néanmoins, pour de nombreux élèves du supérieur et du secondaire en zones urbaines, Internet a été le relais indispensable : cours en visioconférence sur Zoom ou Google Meet, partages de documents sur Google Classroom, MOOC en libre accès, etc. Tous ces outils éducatifs en ligne reposent sur des serveurs à l'extérieur (les serveurs Zoom/Google étant à l'étranger). Les **étudiants congolais** qui suivent des formations en ligne (par exemple des certifications IT, des cours universitaires ouverts) dépendent ainsi de plateformes globales. Le **ministère de l'Enseignement** lui-même a mis en ligne des contenus pédagogiques et examiné la possibilité de cours en ligne, mais faute d'un hébergement national fiable, ces contenus sont dispersés sur YouTube, Facebook ou des sites web hébergés en Europe. L'absence d'un cloud éducatif national pénalise aussi la **protection des données scolaires** : les listes d'élèves, notes, travaux en ligne peuvent se trouver sur des serveurs non soumis aux lois congolaises. Enfin, cette situation creuse la **fracture numérique** : seuls les étudiants urbains connectés bénéficient de l'enseignement en ligne de qualité, tandis que ceux des zones rurales – où 52% de la population vit DATAREPORTAL.COM – restent en marge, dépendant de supports moins interactifs (radio, papier). Un hébergement local couplé à un bon réseau national aurait pu permettre de diffuser plus largement et à moindre coût ces contenus éducatifs numériques (par exemple via des CDN locaux), ce qui n'est pas encore le cas.

- **Administration publique et e-gouvernement :** La **digitalisation de l'État congolais** est en marche, avec des projets d'e-gouvernement, d'identification numérique des citoyens, de télé-procédures administratives, etc. Toutefois, le manque de souveraineté numérique complique grandement ces initiatives. Un exemple frappant est le projet d'**identification nationale (ONIP)** : il s'agit de créer un registre national de la population (cartes d'identité biométriques, état-civil digitalisé). Ce projet stratégique manipule des **données personnelles ultrasensibles** (noms, empreintes, etc.) de plus de 100 millions de Congolais. Faute d'expertise locale suffisante, la RDC a envisagé de s'appuyer sur des sociétés externes, avec le risque que le cœur de la base de données soit opéré depuis l'étranger. Récemment, des inquiétudes ont émergé sur l'implication d'intérêts étrangers dans la gestion des données de l'ONIP – par exemple l'entreprise *Jongoro* basée au Rwanda dans le domaine du BPO numérique 7SUR7.CD 7SUR7.CD. Une telle situation pourrait mettre la souveraineté nationale en péril, en exposant les données identitaires de la

 Copyright Août 2025 office@cyberastre.com

population à un pays voisin. Plus globalement, les **services d'e-gouvernement** (dématérialisation des démarches de passeport, visas en ligne, télé-déclaration fiscale, etc.) requièrent des plateformes numériques souvent développées avec l'aide de bailleurs internationaux. Sans infrastructure locale, ces plateformes sont fréquemment hébergées chez des prestataires cloud étrangers. Par exemple, le portail e-visa de la DGM ou la plateforme de gestion des impôts (DGI) pourraient transiter par des serveurs non localisés en RDC si l'on n'y prend garde. Cela pose des problèmes de **confidentialité** (les données des contribuables, des demandeurs de visa, etc., pourraient être stockées hors du territoire) et de **continuité de service** (en cas de rupture d'Internet international, l'administration en ligne devient inopérante). Les fonctionnaires et les citoyens utilisant ces services sont donc directement concernés par le rapatriement des données.

En somme, **toutes les couches de la société congolaise** – du citoyen utilisant WhatsApp à l'étudiant suivant un cours en ligne, du commerçant mobile money au fonctionnaire exploitant une application e-gouv – subissent aujourd'hui les conséquences d'une infrastructure numérique largement externalisée. Chaque interruption de la connectivité internationale ou chaque changement de politique d'une entreprise Big Tech peut impacter des millions de personnes en RDC. C'est pourquoi le **recentrage des données et services critiques en RDC** n'est pas un luxe, mais une nécessité pour protéger les usagers, assurer la continuité des activités économiques et gouvernementales, et garantir la confidentialité des informations nationales.



crédit photo LeonardJospin1
Copyright Août 2025 office@cyberastre.com

 Copyright Août 2025 office@cyberastre.com

3. PLAN D'ACTION RÉALISTE – RAPATRIER LES DONNÉES NATIONALES VIA UN PARTENARIAT PUBLIC-PRIVÉ (PPP)

Face à ce diagnostic, nous proposons un **plan d'action structuré** pour rapatrier les données nationales en RDC et construire une véritable **souveraineté numérique**, s'appuyant sur un **Partenariat Public-Privé (PPP)**. Ce plan détaille : **(3.1)** l'architecture technique d'un cloud souverain / data center national, **(3.2)** les coûts d'infrastructure estimatifs, **(3.3)** la localisation stratégique de l'infrastructure, et **(3.4)** un modèle économique prévisionnel avec retour sur investissement (ROI).

3.1 ARCHITECTURE TECHNIQUE PROPOSÉE POUR UN CLOUD SOUVERAIN (DATA CENTER TIER III/IV)

Nous préconisons la mise en place d'un **Data Center National** de niveau **Tier III** (au minimum) ou **Tier IV** (idéalement), capable d'héberger les données et applications critiques du pays.

- **Norme de construction (Tier III vs Tier IV) :** Un data center **Tier III** offre déjà un haut niveau de redondance et de disponibilité (environ 99,982 % de disponibilité garantie). Concrètement, cela signifie que toutes les infrastructures essentielles – alimentation électrique, climatisation, connexions réseau – sont **redondées**. Par exemple, un site Tier III dispose de plusieurs circuits d'alimentation électrique et de systèmes de refroidissement duplicatifs, de sorte qu'en cas de panne d'un équipement, un second prend automatiquement le relais 7SUR7.CD. Ce niveau permet des maintenances sans arrêt global (maintenance *concurrentielle*). Un **Tier IV** va encore plus loin avec une tolérance aux pannes totale (aucun point de défaillance unique, redondance *2N* ou *2N+1*), assurant 99,995 % de disponibilité. Cependant, Tier IV engendre un surcoût important (+~30% de coût par rapport à Tier III) et une complexité accrue. **Notre recommandation** est d'adopter un design Tier III (certifiable Uptime Institute), modulable et évolutif, avec la possibilité d'atteindre certains standards Tier IV pour les composants les plus critiques.

- **Capacité et modularité :** L'architecture proposée est un campus de data center d'une capacité initiale d'environ **1,5 à 2 mégawatts (MW)** de charge informatique, extensible en phases. Cela correspond à environ **300 à 500 racks** de serveurs à pleine charge (en tenant compte d'une densité moyenne de 3–5 kW par rack, extensible à des racks haute densité de 10–15 kW pour des usages intensifs). Cette taille initiale s'alignerait sur les projets existants : par exemple, le data center Raxio DRC1 à Kinshasa fournit 1,5 MW pour

400 racks BUSINESSWIRE.COM. L'infrastructure serait modulaire, avec des salles IT ajoutées au fur et à mesure de l'augmentation de la demande. Chaque module/salle serait équipé de systèmes redondants séparés, permettant d'isoler les extensions sans impacter les salles existantes.

- **Alimentation électrique et énergie :** Le data center sera alimenté par le réseau électrique national (**SNEL**), couplé à des solutions de secours robustes. Nous prévoyons au moins **deux lignes électriques indépendantes** en provenance de postes distincts de la SNEL, afin de réduire le risque de coupure totale en cas de panne sur le réseau. En soutien, l'installation comportera plusieurs **groupes électrogènes diesel** de forte puissance (par ex. 3 x 1 MW chacun, configurés en N+1 pour Tier III, ou 2N pour Tier IV). D'après le retour d'expérience de OADC Texaf, celui-ci utilise deux générateurs de 1 MW en redondance pour assurer 24h/24 d'électricité, chaque générateur consommant ~20 000 litres de diesel par semaine 7SUR7.CD. Notre centre devra anticiper une consommation similaire tant que la fiabilité électrique nationale n'est pas optimale. À moyen terme, un investissement dans des **sources d'énergie renouvelable** (solaire photovoltaïque sur site, par exemple) est recommandé pour réduire la dépendance au diesel et les coûts opérationnels. Des onduleurs/UPS en quantité suffisante (redondance N+1) garantiront une alimentation sans coupure lors des basculements réseau <-> générateurs.

- **Refroidissement et climatisation :** Les serveurs seront maintenus dans une fourchette de température et d'humidité stable via un système de climatisation de précision. L'architecture adoptera des **systèmes de refroidissement redondants** (CRAC/CRAH units en double, chillers à double circuit, etc.). Pour le Tier III, chaque salle serveur disposera d'au moins deux circuits de refroidissement indépendants (redondance N+1). Pour viser Tier IV, on pourrait aller vers une redondance 2N (doublement complet des chillers, tours de refroidissement, etc.). Étant donné le climat de la RDC, on privilégiera un système combinant refroidissement mécanique et **free cooling** (refroidissement par air extérieur filtré) pendant les périodes plus fraîches, afin d'améliorer l'efficacité énergétique (PUE cible autour de 1.6 ou moins). Des allées chaudes/froides confinées seront mises en place pour optimiser la dissipation thermique. Chaque composant de refroidissement critique aura un backup immédiat prêt à prendre le relais 7SUR7.CD.

- **Connectivité réseau et sécurité des flux :** Le data center souverain sera un **nœud de connectivité majeur**. Il devra se connecter à **plusieurs dorsales fibre optique** redondantes. Techniquement, on prévoit au moins deux chemins fibre distincts vers les principaux opérateurs (par exemple, une liaison vers le point d'échange Internet national DRC-IX à Kinshasa, et une autre vers un point d'atterrissement de câble international ou vers un pays voisin pour backup). L'objectif est de faire du data center un point de peering incontournable : il accueillera un **Internet Exchange Point (IXP)** local pour échanger le trafic entre opérateurs congolais, afin de garder le maximum de flux *en local*. Idéalement, KINIX (l'IXP de Kinshasa) pourrait être redéployé ou dupliqué au sein du data center pour faciliter ces échanges. Les opérateurs (Vodacom, Airtel, Orange, Africell, etc.)

y seront invités pour interconnecter leurs réseaux. De même, des liaisons spécialisées pourront relier le data center aux agences gouvernementales clés (via le réseau de la SCPT par exemple) pour assurer une connexion directe des administrations au cloud souverain sans passer par Internet. En termes de sécurité réseau, l'infrastructure intègrera des pare-feux de nouvelle génération, des systèmes de détection/prévention d'intrusion (IDS/IPS) et la possibilité d'isoler certains tenants (par exemple le cloud gouvernemental) sur des segments ou des clouds privés virtuels séparés, garantissant la confidentialité.

- **Stockage des données et services cloud :** Outre l'aspect *colocation* (mettre des serveurs tiers), le data center national visera à opérer un **Cloud Souverain** congolais. Techniquement, cela implique de déployer des plateformes de virtualisation et de stockage mutualisé au sein de l'infrastructure. Par exemple, on pourrait bâtir une offre de **cloud public national** (type IaaS/PaaS) en partenariat avec un acteur existant (par ex. une solution OpenStack ou VMware hébergée localement, possiblement soutenue par un grand fournisseur sous licence *white label*). Ce cloud souverain permettrait aux ministères, banques et entreprises de stocker leurs données et d'exécuter leurs applications sur des serveurs en RDC, tout en bénéficiant de la flexibilité du cloud (création de machines virtuelles à la demande, etc.). L'architecture devrait donc intégrer des **baies de stockage haute capacité** (plusieurs pétaoctets de capacité initiale) en redondance, pour héberger bases de données et fichiers. Une attention particulière sera portée à la **sécurité physique et logique** de ces données : chiffrement au repos, contrôle d'accès strict, et plan de reprise après sinistre (avec sauvegardes redondantes dans un site secondaire).

- **Sécurité physique et exploitation :** Le site sera conçu selon les meilleures pratiques de sécurité physique pour un site stratégique. Clôture périmétrique, vidéosurveillance 24/7, contrôle d'accès multi-niveaux (badges, biométrie) aux salles serveurs, présence de gardes formés – tout cela est indispensable. Le bâtiment lui-même sera construit dans une zone stable, hors risques majeurs d'inondation ou de tremblement de terre, avec un niveau de durcissement physique (portes blindées, absence de fenêtres dans les salles sensibles, etc.). Un **Centre d'Exploitation du Réseau/Système (NOC/SOC)** surveillera en permanence les infrastructures, avec des alertes en temps réel sur la température, l'alimentation, la détection incendie (système anti-incendie au gaz neutre pour ne pas endommager les équipements en cas de feu). Le personnel d'exploitation sera composé de techniciens et d'ingénieurs congolais formés (avec l'appui initial éventuel du partenaire privé étranger en PPP pour le transfert de compétences).

En résumé, l'architecture proposée est celle d'un **data center de classe mondiale** sur sol congolais, alliant **haute disponibilité, redondance, sécurité et évolutivité**. Il servira de socle à un cloud souverain national, pouvant héberger aussi bien les applications gouvernementales (e-gov, finances, identification) que les données des entreprises locales et même des services de cache/

 Copyright Août 2025 office@cyberastre.com

content des Big Tech (CDN de Google, Meta, etc.), afin de rapatrier progressivement l'ensemble des flux numériques à l'intérieur du pays. Cette infrastructure sera construite selon un **modèle PPP**, détaillé plus loin, ce qui signifie que le secteur privé apportera expertise et capitaux tout en travaillant de concert avec l'État pour répondre aux impératifs stratégiques (lois sur les données, continuité des services publics, etc.).

3.2 ESTIMATION DES COÛTS D'INFRASTRUCTURE (CONSTRUCTION, ÉQUIPEMENTS, CONNECTIVITÉ, MAINTENANCE)

La réalisation d'un data center Tier III/IV de cette envergure en RDC implique des investissements significatifs. Nous présentons ci-dessous une estimation chiffrée des coûts par poste, sur la base des références de projets similaires en Afrique et des conditions locales congolaises. Ces chiffres seront à affiner lors d'études techniques détaillées, mais donnent un ordre de grandeur du financement nécessaire.

Tableau 1. Estimation des coûts de construction et d'équipement du Data Center Souverain (Capacité ~2 MW)

Poste de dépense	Détails	Coût estimé (USD)
Construction du bâtiment (génie civil)	Terrain, fondations, structure anti-feu, aménagement salles blanches (≈ 1 500 m² utiles, deux niveaux)	~5–7 millions $
Systèmes électriques (HT/BT)	Transformateurs, tableaux électriques redondants, onduleurs (UPS) N+1, générateurs diesel (2 × 1 MW) 7SUR7.CD, réservoirs carburant, câblage électrique double alimentation	~4–6 millions $
Systèmes de refroidissement	Groupes froid/redresseurs, unités de climatisation de précision redondantes (N+1), allées confinées, tours de refroidissement/condenseurs, supervision HVAC	~3–5 millions $
Équipements IT mutualisés	Baies de stockage, serveurs pour le cloud souverain (clusters de virtualisation), équipements de sauvegarde, racks (400 racks dont racks gouvernementaux), câblage structuré, etc.	~4–8 millions $ (selon l'ampleur du cloud public installé)

Infrastructure réseau & connectivité	Routeurs et switchs cœur réseau redondants, pare-feux, équipements IXP (switch peering), liaisons fibre optique métropolitaines (divers opérateurs), accès aux câbles sous-marins (WACS, 2Africa via Moanda)	~2–4 millions $
Sécurité physique & incendie	Systèmes de vidéosurveillance, contrôle d'accès, détecteurs incendie VESDA, système d'extinction au gaz (FM200 ou équivalent) redondant, poste de garde, anti-intrusion	~1 million $
Frais de conception, ingénierie et certifications	Études techniques, honoraires d'ingénierie, obtention certification Tier III (et potentiellement Tier IV), tests de mise en service (commissioning)	~1 million $
Imprévus et contingences (10%)	Marge pour variation des coûts, change (importation équipements), etc.	~2–3 millions $
Total Investissement initial	*(ordre de grandeur)*	**~22 à 34 millions USD**

Justification des coûts et références : Le coût de construction d'un data center varie typiquement entre **7 et 12 millions USD par MW** de capacité IT en Afrique REDDIT.COM GLOBENEWSWIRE.COM, pouvant monter jusqu'à ~15 M$/MW dans des pays aux conditions difficiles (pénurie d'expertise, importation coûteuse) GLOBENEWSWIRE.COM. Notre estimation (~11–12 M$/MW) est cohérente avec ces valeurs, compte tenu qu'en RDC le climat d'affaires est complexe mais que la main-d'œuvre locale est moins chère. À titre de comparaison, la société **Raxio Group a investi 30 millions USD** pour bâtir à Kinshasa un data center Tier III de 1,5 MW BUSINESSWIRE.COM BUSINESSWIRE.COM, ce qui correspond à ~20 M$/MW – chiffre incluant probablement des coûts de démarrage et l'inefficience d'un premier projet du genre. Grâce à un modèle PPP bénéficiant d'exonérations fiscales potentielles et de facilitation par l'État (terrain mis à disposition, allègement douanier pour l'importation des équipements stratégiques), on peut espérer rester dans la fourchette basse à médiane des coûts.

Coûts de connectivité : À noter que l'un des avantages clés du PPP sera de **négocier des capacités fibres à coût maîtrisé**. La RDC a récemment vu l'atterrissage du câble sous-marin **2Africa à Moanda** (septembre 2023), opéré par Orange et Airtel THEAFRICAREPORT.COM. Ce câble gigantesque offre des Tb/s de bande passante internationale. Un investissement sera nécessaire pour relier efficacement le data center à l'atterrage de Moanda (en complétant la dorsale fibre

Moanda–Kinshasa inaugurée en 2023 AGENCEECOFIN.COM) et au câble **WACS** existant (via la station de Muanda également). Le coût d'une fibre dédiée de ~600 km peut atteindre plusieurs millions, mais on privilégiera l'utilisation de fibres optiques déjà posées (par exemple la fibre de la SNEL le long du fleuve, ou le réseau dorsal de la SCPT en cours de déploiement) pour relier Kinshasa au littoral. Des **accords de peering** seront à établir : leur coût n'est pas direct en CAPEX mais en négociation (le data center devrait idéalement héberger un nœud du réseau WACS/2Africa pour minimiser les coûts de transit). Nous avons budgété ~3 M$ pour les équipements réseau actifs et l'interconnexion aux backbones, ce qui inclut la création d'un IXP local modernisé. On rappelle que *garder le trafic local en local* réduira drastiquement les dépenses de transit IP à long terme, ce qui est un bénéfice indirect du projet INTERNETSOCIETY.ORG.

Coûts d'exploitation annuels (OPEX) : En plus des investissements initiaux, il faut prévoir le budget de fonctionnement. Un data center de 2 MW en RDC engendrera des coûts opérationnels significatifs, notamment : l'énergie (électricité de la SNEL + diesel de secours), la maintenance des équipements (contrats de maintenance sur groupes électrogènes, chillers, UPS), le personnel 24/7 (techniciens, ingénieurs, sécurité), l'assurance, etc. Une estimation approximative place ces coûts OPEX autour de **2 à 3 millions USD par an** initialement. L'énergie sera une part majeure : par exemple, 1 MW de charge IT consommé en continu nécessite ~8,76 GWh par an, et si l'électricité coûte (hypothèse) 0,15 $/kWh en moyenne (en combinant SNEL et diesel), cela représente ~1,3 M$ par an pour 1 MW effectif de charge. À 50% de charge moyenne la première année, on serait autour de 0,65 M$. Ajoutons salaires, maintenance et divers, on atteint ~2 M$ annuel.

Ces dépenses seront en partie compensées par les revenus générés (voir modèle économique), mais il est important que le PPP planifie une **trésorerie suffisante** pour supporter les OPEX durant les premières années avant l'atteinte du plein taux d'occupation.

En conclusion, le **budget global de construction** du data center souverain est estimé entre **22 et 34 millions USD**, et il convient d'y adjoindre un **fonds de roulement** couvrant les premiers OPEX (2–3 M$/an). Ce niveau d'investissement est conséquent mais cohérent avec les enjeux : il s'agit d'implanter une infrastructure stratégique comparable aux standards internationaux. Des financements combinés public-privé, voire des partenaires au développement (Banque mondiale, BAD, etc.) pourraient contribuer, étant donné l'importance du numérique dans le développement économique.

3.3 LOCALISATION STRATÉGIQUE DU DATA CENTER – CHOIX DU SITE (KINSHASA, LUBUMBASHI, GOMA ?)

Le choix de la localisation du data center souverain est déterminant pour maximiser son impact et sa viabilité. Plusieurs options ont été envisagées (Kinshasa, Lubumbashi, Goma, ou ailleurs), chacune avec ses atouts. **Après analyse des critères clés** – connectivité, concentration de la demande, sécurité géopolitique, infrastructures existantes – **Kinshasa** apparaît comme le **site stratégique optimal** pour implanter ce premier grand data center national.

Pourquoi Kinshasa ?

- **Centre de gravité démographique et économique :** Kinshasa, avec plus de **17 millions d'habitants** dans son agglomération (en 2024) 7SUR7.CD, représente le plus grand bassin d'utilisateurs numériques du pays. C'est ici que se concentre la majorité des entreprises, des sièges d'institutions financières, des administrations centrales et des universités. Implanter le data center à Kinshasa, c'est le rapprocher **physiquement de ses principaux clients potentiels** (ministères, banques, opérateurs télécom, grandes entreprises), ce qui réduit la latence et facilite les connexions directes. Par exemple, relier un ministère ou une banque située à Gombe/Lingwala au data center kinshasa est trivial via fibre urbaine, tandis que si le DC était à 1500 km, la latence et la fiabilité des liaisons seraient moindres.

- **Connectivité internationale existante et à venir :** Kinshasa est déjà le nœud des télécommunications du pays. C'est près de Kinshasa (à **Muanda, Kongo-Central**) que les câbles sous-marins **WACS** et **2Africa** atterrissent ou vont atterrir 7SUR7.CD. Une dorsale fibre optique relie Muanda à Kinshasa (620 km inaugurés en 2023) AGENCEECOFIN.COM, offrant une capacité de transport élevée directement jusque la capitale. De plus, Kinshasa est connectée régionalement : des faisceaux fibre ou micro-ondes la relient aux pays voisins (Brazzaville à 5 km de distance, point d'échange possible vers l'Afrique de l'Ouest; et via le Katanga vers la Zambie/Afrique australe). La présence de **KINIX (point d'échange Internet de Kinshasa)** est un atout : il draine déjà l'échange de trafic local entre FAI couvrant plus de 85% des internautes du pays INTERNETSOCIETY.ORG. En localisant le data center à Kinshasa, on peut **interconnecter immédiatement l'IXP KINIX** et bénéficier de la mutualisation du trafic local existant. Au contraire, Goma ou Lubumbashi n'ont pas encore de trafic local à échanger à grande échelle (LUBIX existe à Lubumbashi mais le volume reste moindre). Enfin, **Kinshasa offre plusieurs chemins d'accès** : en plus de la route ouest via l'Atlantique (WACS/2Africa), une route **sud** via fibre Liquid Telecom par Lubumbashi-Zambie jusqu'à l'océan Indien est en développement THEDOCS.WORLDBANK.ORG, et une route **est** via Goma vers l'Ouganda/Rwanda est envisagée. En cas de coupure sur un câble, Kinshasa pourra basculer sur une autre route plus aisément qu'une ville isolée.

- **Infrastructures et énergie :** La capitale dispose des meilleures infrastructures d'accueil : disponibilité de terrains en zone technologique (par ex. **Silikin Village** à Kinshasa-Gombe,

où OADC Texaf s'est implanté 7SUR7.CD), présence du siège de la SNEL (pour des raccordements électriques prioritaires), et d'une concentration de sociétés pouvant fournir maintenance et services (ingénierie, sécurité, etc.). Certes, la fiabilité électrique de Kinshasa n'est pas parfaite, mais elle est meilleure qu'ailleurs en RDC (grâce au barrage d'Inga tout proche). Un projet à Kinshasa pourrait s'appuyer sur les efforts de la ville pour améliorer la distribution (postes de transformation renforcés). De plus, Kinshasa offre la possibilité d'une **synergie avec les data centers privés récents** : par exemple, Raxio et OADC Texaf. Placer notre centre souverain à Kinshasa permettrait éventuellement d'établir des **liens de redondance** entre ces sites (pour des backups mutuels ou de la reprise d'activité croisée en cas de sinistre), créant un écosystème local robuste.

- **Visibilité stratégique et confiance :** D'un point de vue politique, la présence du data center national dans la capitale revêt un caractère symbolique fort – c'est un projet de souveraineté, et sa proximité avec les instances dirigeantes assure un suivi étroit. Cela peut aussi faciliter la **confiance des administrations** : elles seront plus enclines à migrer leurs données vers un site qu'elles peuvent physiquement auditer et surveiller aisément. De même, pour les **investisseurs privés du PPP**, Kinshasa est plus rassurant : c'est la ville où la stabilité est la plus grande (en comparaison, l'Est du pays subit des troubles sécuritaires, et le Grand Katanga est stable mais éloigné de la supervision centrale).

Quid d'autres sites (Lubumbashi, Goma) :

- **Lubumbashi** (Haut-Katanga) est la deuxième ville économique, avec un fort secteur minier. Elle offre une proximité avec la Zambie et l'Afrique du Sud, ce qui est un atout pour la connectivité vers les clouds de Johannesburg. Un data center à Lubumbashi pourrait servir de **hub régional** pour le Sud-Est du pays. Cependant, pour une première infrastructure souveraine, Lubumbashi présente l'inconvénient d'être loin des centres de décision et de la majorité des utilisateurs finaux du pays (géographiquement très excentré à l'extrême sud-est). De plus, bien que Liquid Telecom et Airtel aient amené de la fibre à Lubumbashi THEDOCS.WORLDBANK.ORG, la ville ne dispose pas encore d'un IXP majeur ni d'atterrage de câble direct (elle dépend de routes terrestres via la Zambie). Lubumbashi pourrait être envisagée pour un **deuxième data center** de réplication (site de secours) à moyen terme, notamment pour assurer une redondance géographique (distance >1500 km de Kinshasa, ce qui est bon pour la résilience en cas de sinistre majeur). Mais en tant que site principal initial, elle est moins favorable que Kinshasa sur le plan de la concentration de trafic immédiate.

- **Goma** (Nord-Kivu) et la région Est en général disposent désormais d'un IXP récent (**GOMIX**, lancé en 2021) INTERNETSOCIETY.ORG. La ville dessert un hinterland important (Nord/Sud-Kivu, Rwanda, Ouganda). Cependant, Goma souffre de quelques handicaps : risques naturels (volcan Nyiragongo tout proche, sismicité), risque sécuritaire (conflits à l'Est), infrastructures plus limitées. La connectivité internationale y est possible via les pays

voisins (fibre vers Kampala/Nairobi potentiellement), mais aujourd'hui l'Est de la RDC reste souvent connecté via Kinshasa ou via des liaisons coûteuses par satellite THEDOCS.WORLDBANK.ORG. Un data center à Goma aurait du sens pour **servir l'Afrique de l'Est** et les organisations internationales nombreuses dans la région, mais ce serait plutôt en troisième phase d'un déploiement, une fois que Kinshasa (puis Lubumbashi) seraient établis.

En conclusion, **Kinshasa** est recommandée comme **localisation stratégique** du data center souverain pour le PPP. Concrètement, un terrain pourrait être identifié dans une zone à la fois centrale et sécurisée – par exemple dans le **périmètre du nouveau Pôle Technologique de Kinshasa (Kinshasa Digital City/Silikin Village)** qui héberge déjà un data center 7SUR7.CD, ou sur un terrain étatique à proximité d'infrastructures (pour minimiser les coûts de raccordement, comme près d'un poste haute tension et d'une artère fibre). La **commune de la Gombe** (cœur administratif) semble idéale pour la proximité avec les ministères, mais les contraintes d'espace peuvent orienter vers Mont Ngafula ou N'Djili où du foncier plus large est disponible, à condition d'y amener la connectivité adéquate.

Mesures complémentaires : Quel que soit le site exact à Kinshasa, des mesures seront prises pour renforcer la localisation choisie : améliorer les routes d'accès (pour acheminer les équipements lourds, et permettre la maintenance), s'assurer de la disponibilité du carburant (contrat avec une compagnie pétrolière pour alimenter en diesel en cas de délestage prolongé), et collaborer avec la police/armée pour sécuriser le périmètre (vu le caractère "infrastructure critique"). L'État congolais, dans le cadre du PPP, pourrait **apporter le terrain en apport** ou à un tarif symbolique, et faciliter les autorisations de construire, ce qui oriente encore plus le choix vers Kinshasa où ces démarches peuvent être centralement pilotées.

3.4 MODÈLE ÉCONOMIQUE ET RETOUR SUR INVESTISSEMENT (ROI) POUR LE PPP

La réussite du projet dépendra d'un modèle économique solide, alignant les intérêts du partenaire privé (rentabilité de l'investissement) et du secteur public (accès souverain aux infrastructures à un coût maîtrisé). Voici les **grandes lignes du modèle économique** proposé pour le data center souverain en PPP, ainsi qu'un **scénario de retour sur investissement** estimatif.

Structure du PPP : On envisage la création d'une **société de projet** mixte, détenue par l'État congolais (ou une agence publique numérique) et un ou plusieurs partenaires privés spécialisés (ex: un opérateur de data centers panafricain, ou un consortium constructeur-exploitant). Par exemple, un montage pourrait être : 30 % capital public (incluant apport du terrain, facilités fiscales) et 70 % capital privé (apport en numéraire, expertise technique). Ce PPP signerait avec l'État un **contrat de concession** ou de partenariat d'une durée de 10 à 20 ans, définissant les obligations (niveau de service, priorité nationale des données, etc.) et les mécanismes de partage des revenus.

Sources de revenus : Le data center/cloud souverain générera plusieurs flux de revenus :

- *a)* **Colocation et hébergement** : location d'espace rack, d'alimentation électrique et de connectivité aux clients. Tarification mensuelle par baie ou par U (unité de rack). Par exemple, un tarif moyen de **1 200 $ par mois par rack** standard pourrait être appliqué (ce qui reste en ligne avec les tarifs régionaux compte tenu du niveau Tier III). Les clients cibles ici sont les **entreprises privées** (banques, compagnies minières, grandes PME) souhaitant héberger leurs serveurs dans un environnement sécurisé local, ainsi que les **opérateurs télécom** (pour installer des équipements de cache de contenu, des routeurs de peering, etc.). Avec ~400 racks disponibles, dont on peut espérer louer 50 % la première année puis monter à 80 % en régime de croisière, ce segment pourrait rapporter autour de *240 racks × 1200 $/mois = 288 000 $/mois* en année 1 (env. 3,5 M$ annuels) et *320 racks × 1200 = 384 000 $/mois* en année 3 (4,6 M$ annuels). Ces chiffres dépendront du **taux d'occupation effectif**.

- *b)* **Services de Cloud souverain et ventes de solutions IT** : au-delà de la colocation brute, la société de projet offrira des services à valeur ajoutée sur son infrastructure mutualisée. Par exemple, de la **location de machines virtuelles/VMs** pour les ministères et institutions (mode IaaS), de l'hébergement d'applications (mode PaaS/SaaS – par ex une plateforme de messagerie gouvernementale, ou un service d'hébergement de sites web nationaux). L'État congolais sera un client primordial de ces services cloud pour l'e-gov : plutôt que de payer des licences cloud à AWS/Azure à l'étranger, les ministères paieront des redevances au cloud souverain local (ce qui en outre garde la dépense ICT dans l'économie locale). On peut imaginer un contrat-cadre où les principales agences (ministères, universités publiques, hôpitaux) se voient allouer X ressources (stockage en To, VMs en nombre) pour un montant global annuel. Si, par exemple, l'État garantit un forfait de ~**2 M$ par an** pour l'usage de la plateforme (ce qui correspond à l'hébergement de nombreux systèmes aujourd'hui externalisés), cela sécurisera une part stable des revenus. En parallèle, des entreprises privées pourraient consommer ces services cloud (sauvegarde en ligne, location de serveurs virtuels pour leurs applications locales) – segment encore naissant mais à développer avec le temps. On estime ces revenus cloud et services managés à **1–2 M$ par an** après quelques années, l'objectif étant d'augmenter ce ratio à mesure que la confiance en la plateforme grandit.

- *c)* **Connectivité et peering** : le data center, en hébergeant un IXP, pourrait facturer des **frais d'interconnexion** aux opérateurs (bien que souvent les IXP purs fonctionnent sur une base de cotisation modeste). Toutefois, en PPP, on peut imaginer des **services de transit IP local** vendus aux FAI plus petits. Par exemple, acheminer du trafic international via la capacité mutualisée du data center (qui, négociant en gros sur 2Africa/WACS, peut revendre aux ISP locaux de la bande passante à prix moindre que s'ils la prenaient individuellement). Ce volet est technique, mais pourrait générer un revenu additionnel tout en baissant les coûts pour les FAI – un modèle *win-win*. On reste prudent et on n'intègre pas de gros chiffres ici initialement, disons **0,5 M$/an** en vitesse de croisière

pour la revente de capacité/ports.

- *d)* **Services aux Big Tech / CDN globaux :** un des objectifs du centre souverain est d'attirer des caches de contenu de **Google (Youtube, Search), Meta (Facebook), Netflix, TikTok**, etc. Eux ne paieront pas forcément un loyer classique (souvent ils négocient l'hébergement de leurs serveurs de cache gratuitement en échange du bénéfice apporté aux réseaux locaux), mais ils pourraient contribuer en nature (par exemple Google installe un Google Global Cache à ses frais mais cela économise de la bande passante internationale pour tout le monde). Néanmoins, certains grands acteurs **cloud (AWS, Azure)** pourraient, eux, vouloir une présence locale pour adresser des clients en RDC. Ils pourraient alors louer des suites privées ou des cages dans le data center. C'est un scénario bonus : s'il se réalise, les revenus de colocation mentionnés en *a)* augmenteraient d'autant (car Amazon ou Microsoft paieraient comme n'importe quel client pour leur espace, voire plus cher pour des exigences particulières).

Répartition et tarification préférentielle : Dans le PPP, on peut imaginer que l'État négocie des conditions préférentielles pour ses propres besoins (par ex. un tarif réduit de 30% par rapport aux prix de marché pour l'hébergement des données publiques, ou un espace dédié sécurisé pour certaines données sensibles gratuitement mis à disposition de l'ANR, etc.) comme **contrepartie de sa participation**. Le modèle d'affaires doit donc intégrer une part de **service public** (non lucrative ou subventionnée) couverte par la part commerciale privée.

Projection de rentabilité (ROI) : Sur la base des revenus ci-dessus et des coûts précédemment estimés, on peut esquisser une projection financière simplifiée sur 5 à 7 ans :

- **Année 0-1 (construction et lancement) :** Investissement ~30 M$. Pas de revenus pendant ~12 mois de construction. À l'ouverture (milieu d'Année 1), ramp-up lent : mettons 20% d'occupation moyenne sur la première année opérationnelle. Revenus estimés A1 : ~2,5 M$ (colocation + premiers contrats cloud). Coûts OPEX A1 : ~2 M$. ==> Flux de trésorerie A1 ≈ +0,5 M$ (faible, quasi à l'équilibre, l'État peut éventuellement garantir un minimum de revenus cette première année pour rassurer le PPP).

- **Année 2 :** Montée en puissance. Occupation 50%. Revenus ~5–6 M$. OPEX ~2,5 M$ (hausse modérée car une partie des coûts est fixe, et l'électricité augmentera avec l'usage). EBITDA positif solide ~3 M$. Amortissements en cours (sur 10-15 ans). On peut commencer à envisager un bénéfice net modeste si les charges financières sont faibles (si emprunt, il faut rembourser intérêts).

- **Année 3-4 :** Régime de croisière atteint, ~70-80% d'occupation. Revenus ~8–10 M$ par an (incluant plus de services cloud vendus). OPEX ~3 M$. EBITDA ~6–7 M$. À ce stade, la société de projet pourrait **dégager un profit net** significatif et envisager de verser des dividendes aux investisseurs privés et à l'État actionnaire.

Avec ce scénario, on obtient un **retour sur investissement** aux alentours de **6 à 7 ans** : c'est le délai pour que la somme des flux de trésorerie actualisés rembourse l'investissement initial de ~30 M$. En effet, dès l'Année 5, l'opération aurait généré cumulé ~15-20 M$ de cash-flow brut. En prenant en compte un discount rate (taux d'actualisation) raisonnable pour risque-pays, on arrive vers 6-7 ans pour un ROI > 0 en valeur actuelle. **En termes de TRI (taux de rentabilité interne)**, on peut viser un TRI à deux chiffres (15-20%), ce qui est attractif pour un investisseur, compte tenu du soutien étatique réduisant certains risques.

Il convient de noter que cette rentabilité dépend de plusieurs **hypothèses-clés** : l'adoption réelle par les clients (ne pas plafonner à 30% d'occupation, ce qui mettrait en péril l'équilibre), la stabilité économique et monétaire (les contrats idéalement libellés en USD pour se prémunir contre une dévaluation du franc congolais), et le maintien de la confiance (si un scandale de sécurité survient, les clients fuiront le cloud local). Néanmoins, étant donné la taille du marché potentiel – plus de **53 millions de connexions mobiles actives** en 2024 DATAREPORTAL.COM, des dizaines de milliers d'entreprises, et un État voulant numériser ses services – on peut considérer que la demande existera. Une **étude de marché préalable** sera menée dans la phase préparatoire du PPP pour affiner ces projections et sonder les engagements de grands clients "anchor" (par exemple, obtenir la promesse que tel ministère ou telle banque va migrer X serveurs dès l'ouverture).

Retombées économiques et ROI élargi : Au-delà du ROI financier direct pour le PPP, il faut souligner les retombées macroéconomiques positives, qui elles aussi **"remboursent" l'investissement sous forme de bénéfices pour la nation**. En rapatriant 95% des flux qui partaient à l'étranger, la RDC économisera des **devises** (moins d'achats de bande passante internationale coûteuse), stimulera la **création d'emplois qualifiés** (ingénieurs, techniciens de data center, experts cybersécurité formés localement), et favorisera l'**émergence de startups locales** (qui pourront héberger leurs applications à moindre coût localement, donc innover plus facilement). Le tout contribue à la croissance du PIB numérique. Par exemple, l'ouverture du data center OADC Texaf est présentée comme un moteur pour *« redynamiser l'économie numérique en RDC »* et réduire les coûts et latences VATICANNEWS.VA VATICANNEWS.VA. On peut s'attendre à des effets similaires, multipliés, avec un cloud souverain national : baisse des coûts internet pour les usagers (grâce au peering local, "local break-out"), amélioration de la qualité de service (sites web locaux plus rapides), et **confiance accrue des investisseurs** étrangers qui verront que la RDC possède une infrastructure numérique moderne (ce qui peut attirer des implantations de services numériques régionaux en RDC, plutôt qu'à l'étranger).

Pour l'État, le ROI c'est aussi la **maîtrise de ses données sensibles** : celles-ci seront stockées sous juridiction congolaise, réduisant les risques d'espionnage ou de pressions extérieures. Il est difficile de quantifier en dollars ce bénéfice, mais il est stratégique. De même, la souveraineté numérique a un impact positif sur la **souveraineté juridique** : en cas de litige ou d'enquête (cybercriminalité par ex.), les données étant localement accessibles, les forces de l'ordre congolaises pourront plus efficacement agir, plutôt que de dépendre de l'entraide judiciaire internationale pour accéder à des serveurs à l'étranger.

Soutenabilité et extension : Si le modèle fonctionne bien, le PPP pourrait décider de réinvestir les profits pour **étendre la capacité** (passer de 2 MW à 5 MW en construisant un second bâtiment modulaire sur site) ou pour **déployer des sites secondaires** (ex: un conteneur data center Tier II à Lubumbashi pour réplication de certaines données et servir de cache régional). Ces décisions se prendront en fonction du taux d'adoption. L'accord PPP devra prévoir ce cadre d'extension et peut-être accorder un droit de premier refus à l'opérateur pour toute nouvelle implantation (afin de l'encourager à investir plus si le marché grandit). L'État, de son côté, bénéficiera d'une **augmentation des recettes fiscales** indirectes (TVA sur services numériques en hausse, imposition des revenus du PPP dès qu'il sera bénéficiaire, etc.), contribuant aussi au retour sur investissement national.

En synthèse, le modèle économique repose sur une combinaison de **ventes de services d'hébergement et cloud** à des acteurs publics et privés, adossé à un engagement fort de l'État pour utiliser en priorité l'infrastructure nationale (effet "locomotive"). Les chiffres préliminaires suggèrent qu'avec une occupation de ~70% et une tarification compétitive, le data center pourrait générer autour de **8 millions $ de CA annuel**, pour des coûts opérationnels d'environ 3 millions $, soit une marge permettant d'amortir l'investissement en une **demi-douzaine d'années**. Ce délai de ROI d'environ 6-7 BUSINESSWIRE.COM GLOBENEWSWIRE.COM ans est tout à fait raisonnable dans le secteur des infrastructures, d'autant plus compte tenu des **externalités positives** très importantes pour le pays (souveraineté, emploi, économies de devises). Le partenariat public-privé permet de répartir les risques : le privé assume le risque commercial (trouver des clients, exploiter efficacement), tandis que le public apporte un environnement stable et la garantie d'une utilisation par l'administration, ce qui sécurise une partie des revenus.

Copyright Août 2025 office@cyberastre.com

crédit photo LeonardJospin1



 Copyright Août 2025 office@cyberastre.com

4. LIVRABLE – VERS UN CAHIER DES CHARGES POUR UNE INFRASTRUCTURE STRATÉGIQUE

Le présent rapport a dressé un état des lieux chiffré de la **perte de souveraineté numérique de la RDC** et a proposé un **plan d'action détaillé** pour y remédier via la mise en place d'un data center national en PPP. En guise de synthèse, et pour évoluer vers un véritable *cahier des charges*, voici les **principaux points** à retenir et à formaliser pour une entreprise candidate à la construction et à la gestion de cette infrastructure stratégique :

- **Contexte justificatif :** Plus de *95% du trafic numérique congolais* est acheminé hors du pays, les données nationales (privées comme publiques) sont majoritairement stockées à l'étranger, créant une dépendance dangereuse INTERNETSOCIETY.ORG. Le cahier des charges rappellera ces chiffres et soulignera l'urgence d'une solution souveraine. Il mentionnera les lois en vigueur (Code du numérique imposant le stockage local 7SUR7.CD) pour lesquelles l'infrastructure proposée est une réponse nécessaire.

- **Objectifs du projet :** Créer un **Cloud Souverain de la RDC** – concrétisé par un centre de données Tier III/Tier IV – capable d'héberger des services d'identification des personnes, des paiements, de l'e-éducation, de la santé, de l'e-agriculture, etc., localement VATICANNEWS.VA VATICANNEWS.VA. Il s'agit d'améliorer la fiabilité et la rapidité des services numériques, de réduire les coûts d'accès internet VATICANNEWS.VA, et d'assurer la **souveraineté et la sécurité** des données congolaises.

- **Description technique de l'infrastructure attendue :** Niveau Tier III minimum (redondance N+1 sur énergie et refroidissement) 7SUR7.CD, capacité initiale ~2 MW / 400 racks, évolutive. Systèmes de secours (groupes électrogènes) dimensionnés 7SUR7.CD, sécurité physique maximale, connexion à au moins 2 routes fibre distinctes. Intégration d'un IXP national et possibilité d'héberger des nœuds de cache de grands fournisseurs (Google, Microsoft, etc.) 7SUR7.CD. Respect des standards internationaux (certification ISO 27001, PCI-DSS si bancaire, etc.). Le cahier des charges devra inclure des **SLA** (niveaux de service garantis) sur la disponibilité (ex : 99,982% uptime annuel pour Tier III), le délai de rétablissement en cas de panne, etc.

- **Plan de localisation et d'aménagement :** Site retenu : **Kinshasa**, pour les raisons évoquées (le document explicitera le choix et attendra du candidat des propositions de site précis, analyses géotechniques, etc.). Le soumissionnaire devra proposer un plan d'implantation détaillé, incluant les accès au réseau électrique (postes SNEL) et télécom

(opérateurs fibre). Une attention sera portée aux futurs aménagements : par exemple, réservation de terrain pour une extension, ou plan d'un second site de backup éventuel (ex: Lubumbashi en phase 2).

- **Estimation financière et montage PPP :** Le rapport présente un budget indicatif de ~30 M$ CAPEX INTERNETSOCIETY.ORG GLOBENEWSWIRE.COM. Le cahier des charges demandera aux entreprises candidates de fournir *leur* estimation détaillée, poste par poste, et un plan de financement. Le montage PPP attendu : l'État offre facilités (foncier, avantages fiscaux, garantie d'abonnement pour administrations) et le privé apporte financement majoritaire et exploitation. Le candidat devra indiquer le modèle de revenus qu'il envisage (tarifs de colocation, services cloud) et comment il compte atteindre la rentabilité en accord avec les projections (ROI ~7 ans visé). Un plan d'affaires sur 10 ans sera exigé, montrant le point mort, les flux de trésorerie, etc., afin de vérifier la viabilité économique.

- **Calendrier de réalisation :** Sur la base des expériences (Raxio a construit en ~18 mois BUSINESSWIRE.COM), on attend du soumissionnaire un **planning** depuis la conception jusqu'à la mise en service, par exemple : Études (3-4 mois), Construction (12-15 mois), Tests et certification (2 mois), Ouverture au public sous 18 mois après signature. Des jalons clés seront définis (fin du gros œuvre, installation des systèmes électriques, période d'essai à froid/hot tests, audit de certification Tier). Le respect des délais sera crucial pour commencer à rapatrier les données au plus tôt.

- **Engagements en matière de transferts de compétences :** Étant un projet de souveraineté, le cahier des charges insistera sur la formation de techniciens congolais. L'entreprise devra proposer un plan de **capacity building** (ateliers de formation, tutorat, éventuellement partenariat avec des universités locales pour former des ingénieurs réseaux et sécurité, etc.). L'objectif est qu'au bout de quelques années, la majorité de l'exploitation courante puisse être effectuée par des Congolais, le partenaire privé passant sur un rôle de support/tierce maintenance.

- **Cadre juridique et gouvernance :** Il faudra intégrer les aspects légaux : conformité au Règlement Général sur la Protection des Données (RGPD) si des données de citoyens UE sont stockées, mais surtout conformité aux lois congolaises (loi sur la protection des données personnelles en gestation, dispositions du Code du numérique). La gouvernance du PPP sera définie (comité paritaire de suivi État/Privé, rapport d'activité annuel, audit de sécurité annuel par une tierce partie, etc.).

Avec ce cahier des charges, les entreprises candidates (opérateurs de data center, consortiums BTP/Tech) auront une vision claire des **exigences** et **objectifs chiffrés**. Elles devront démontrer, références à l'appui, leur capacité à délivrer une telle infrastructure. La sélection privilégiera un acteur combinant **expérience internationale** (pour garantir le standard Tier III/IV) et **ancrage local** (pour s'intégrer au contexte RDC). Le partenaire retenu deviendra un **pilier de l'écosystème**

 Copyright Août 2025 office@cyberastre.com

numérique congolais, accompagnant la RDC dans la construction de sa souveraineté numérique.

En conclusion, la mise en place d'un data center souverain via un PPP représente un **tournant stratégique** pour la RDC. Les données chiffrées présentées dans cette étude – du **taux de dépendance extérieure (>95%)** aux **millions d'utilisateurs concernés**, en passant par les **coûts et bénéfices économiques** – justifient pleinement l'ampleur du projet. Il en va de la **maîtrise du futur numérique** du pays : rapatrier les données, c'est rapatrier une part de sa souveraineté. Grâce à une planification rigoureuse et à l'alliance du public et du privé, la RDC peut combler son retard et assurer, à l'horizon des prochaines années, que **l'immense potentiel numérique de ses 100 millions d'habitants** soit exploité sur son sol, pour son développement, en toute sécurité et autonomie 7SUR7.CD 7SUR7.CD.

Sources et Références :

- Plan National du Numérique Horizon 2025 – Présidence de la RDC (2019) DROITNUMERIQUE.CD 7SUR7.CD
- Code du Numérique 2020 (RDC) – Exigences de souveraineté des données 7SUR7.CD
- Agence pour le Développement du Numérique (ADN), Communiqués 2024 sur le data center Raxio (Kinshasa) ADN.CD ADN.CD
- Articles de presse : *7sur7.cd* (15/08/2024) sur l'inauguration de OADC Texaf (Tier III Kinshasa) 7SUR7.CD 7SUR7.CD; *Businesswire* (22/08/2024) – *La RDC inaugure le Raxio Data Centre (30 M$)* BUSINESSWIRE.COM BUSINESSWIRE.COM; *Actualité.cd* (2024) – *Vers la souveraineté numérique avec l'inauguration du data center*; *ADN.cd* (30/03/2024) – visite chantier Raxio ADN.CD.
- Données ARPTC (Autorité de Régulation des Postes et Télécoms) via Africa24 (21/06/2024) sur la pénétration Internet (1,9% en 2013 -> 30,4% en 2023) AFRICA24TV.COM et les abonnés Internet mobile (28,9 millions en 2023) AFRICA24TV.COM.
- Internet Society – Blog (2022) sur l'IXP GOMIX et l'initiative DRC-IX (95% de la connectivité disponible branchée sur 3 IXPs, 85% des utilisateurs concernés) INTERNETSOCIETY.ORG; Initiative "80/20" pour l'Afrique (garder 80% du trafic localement) INTERNETSOCIETY.ORG.
- DataReportal (Kepios, 2024) – Statistiques digital 2024 en RDC (28,3 M d'internautes, 6,45 M utilisateurs réseaux sociaux, 53,3 M abonnements mobiles) DATAREPORTAL.COM DATAREPORTAL.COM DATAREPORTAL.COM.
- GlobeNewsWire/Arizton (2025) – *Africa Data Center Construction Market* (coûts de construction 10 M$/MW, tendances PPP en Afrique) GLOBENEWSWIRE.COM.
- UNICEF/UNESCO – Informations COVID-19 et éducation à distance en RDC (2020) UNICEF.ORG.
- Tribune 7sur7.cd (17/05/2025) – Alerte sur la gestion étrangère des données ONIP 7SUR7.CD.
- Documents techniques World Bank (2021) – Évaluation de l'économie numérique RDC (infrastructures fibre, risque WACS, etc.) THEDOCS.WORLDBANK.ORG.

 Copyright Août 2025 office@cyberastre.com

NOTE.

LES TABLEAUX ET CHIFFRES PRÉSENTÉS DANS CE RAPPORT PROVIENNENT DES SOURCES CI-DESSUS OU D'ESTIMATIONS CALCULÉES À PARTIR DE CELLES-CI. ILS VISENT À ÉCLAIRER LA PRISE DE DÉCISION ET DEVRONT ÊTRE VALIDÉS ET AJUSTÉS LORS DES ÉTUDES DE FAISABILITÉ TECHNIQUES FINALES.



CYBERASTRE

ÉTUDE SUR LA SOUVERAINETÉ NUMÉRIQUE DE LA RDC – RAPPORT CYBERSTRATÉGIQUE

crédit photo LeonardJospin1

Copyright Août 2025 office@cyberastre.com