

**INSTITUT DE RECHERCHE EN GEOPOLITIQUE ET
D'ETUDES STRATEGIQUES**

Revue
Intelligence Stratégique

Vol. 008, Numéro 020, Janvier-Mars 2025

E-ISSN : 3006-5488, P-ISSN : 3006-547X

<https://doi.org/10.62912/JYFU3565>



Siège social : 292, avenue Mweka, Commune de Lingwala, Kinshasa, République
Démocratique du Congo.

Téléphone : +243 82 006 1696 ; 81 86 19 121; 89 7175 074

E-mail : felly.lukunga@revue-is.org, article@revue-is.org, info@revue-is.org ;

Internet : www.revue-is.org ; www.irges.org

Europe : 59, Rue du Rhône, 1204 Genève, Suisse, + 41 22 810 88 68, Chambre de
Commerce Suisse-RD Congo, info@ccsc.ch



Revue Intelligence Stratégique
Journal des publications scientifiques

Volume 8, numéro 20

Janvier-Mars 2025

p-ISSN : 3006-547X ; e-ISSN : 3006-5488

<https://doi.org/10.62912/LHWC5495>

www.revue-is.org

**EXTERNALISATION DES DATA CENTERS EN REPUBLIQUE DEMOCRATIQUE DU
CONGO : ENJEUX DE SOUVERAINETE NUMERIQUE ET PERSPECTIVES DE
GESTION SECURISEE DES INFRASTRUCTURES DIGITALES**

Hermès MONDO KIGODI

Chef de Travaux et Doctorant à l'Université Pédagogique Nationale

RESUME

Cet article aborde les enjeux de l'externalisation des data centers en République Démocratique du Congo (RDC) et son impact sur la souveraineté numérique du pays. La révolution numérique, bien qu'apportant des avantages économiques et sociaux, soulève des défis en termes de sécurité, de contrôle des données et de dépendance à des acteurs étrangers. La RDC, confrontée à un manque d'infrastructures locales de qualité et à des coûts d'entretien élevés, choisit de plus en plus d'externaliser ses services numériques vers des fournisseurs internationaux tels qu'Amazon Web Services, Microsoft, ou Google Cloud.

Les motivations de cette externalisation sont principalement économiques : réduction des coûts d'infrastructure, accès à des technologies avancées comme le cloud computing et l'intelligence artificielle, ainsi que la gestion efficace des données malgré la faiblesse des infrastructures locales. Cette étude conclut que la RDC peut construire un avenir numérique souverain en renforçant ses capacités locales, en élaborant un cadre juridique adapté et en explorant des solutions technologiques novatrices, tout en maintenant une coopération avec les acteurs internationaux pour garantir un écosystème numérique sécurisé et compétitif.

Mots-clés : *Externalisation, Data centers, Souveraineté numérique et Infrastructures digitales.*

ABSTRACT

This article looks at the challenges of data center outsourcing in the Democratic Republic of Congo (DRC) and its impact on the country's digital sovereignty. The digital revolution, while bringing economic and social benefits, raises challenges in terms of security, data control and dependence on foreign players. Faced with a lack of quality local infrastructure and high maintenance costs, the DRC is increasingly opting to outsource its digital services to international providers such as Amazon Web Services, Microsoft, or Google Cloud.

The motivations for this outsourcing are mainly economic: reduced infrastructure costs, access to advanced technologies such as cloud computing and artificial intelligence, as well as efficient data management despite weak local infrastructures. This study concludes that the DRC can build a sovereign digital future by strengthening local capabilities, developing an appropriate legal framework and exploring innovative technological solutions, while maintaining cooperation with international players to ensure a secure and competitive digital ecosystem.

Keywords : *Outsourcing, Data centers, Digital Sovereignty and Digital Infrastructures.*

INTRODUCTION

La révolution numérique a transformé le paysage économique, social et politique de nombreuses nations, y compris la République Démocratique du Congo (RDC). Au cœur de cette transformation, les data centers jouent un rôle central, en servant de pivots pour le stockage et le traitement de données essentielles.

Cependant, face à un manque d'infrastructures locales performantes et à des coûts d'entretien élevés, de plus en plus d'entreprises et d'institutions publiques en RDC choisissent l'externalisation de leurs data centers vers des fournisseurs internationaux. Cette évolution soulève des questions cruciales

concernant la souveraineté numérique nationale et les risques associés à la dépendance vis-à-vis d'acteurs étrangers.¹

L'objectif de cet article est d'analyser les enjeux et défis liés à l'externalisation des data centers en RDC, notamment en ce qui concerne la protection de la souveraineté numérique nationale. Nous explorons les motivations qui poussent les entreprises congolaises à externaliser leurs infrastructures numériques, avant d'étudier les risques liés à la sécurité des données, la perte de contrôle sur des informations stratégiques et les implications géopolitiques de cette dépendance. Enfin, nous proposerons des solutions pour sécuriser la gestion des infrastructures numériques et garantir la souveraineté du pays dans un contexte de mondialisation technologique.

L'externalisation des data centers en République Démocratique du Congo (RDC) soulève des questions cruciales liées à la souveraineté numérique nationale. En effet, alors que la demande pour des services numériques évolue rapidement, les entreprises et institutions publiques congolaises se tournent de plus en plus vers des fournisseurs étrangers pour gérer leurs infrastructures numériques. Cette dépendance vis-à-vis des acteurs internationaux soulève des préoccupations importantes concernant la sécurité des données, le contrôle des informations stratégiques et les implications géopolitiques pour le pays.

Sur ce, les questions suivantes méritent d'être posées : Quelles sont les principales motivations qui poussent les entreprises et les institutions publiques en RDC à externaliser leurs data centers ? Quels sont les risques associés à l'externalisation des data centers en RDC pour la souveraineté numérique du pays ? Quelles sont les implications géopolitiques de l'externalisation des data centers en RDC ? Quelles solutions pourraient être mises en place pour garantir une gestion sécurisée et souveraine des infrastructures numériques en RDC ?

Suite à ces interrogations, il y a lieu d'être ces hypothèses selon lesquelles l'externalisation des data centers en RDC serait principalement

¹ BOUCHER J-F., *La souveraineté numérique et l'infrastructure des données*, éd. Technopolis, Paris, 2022, p. 53.

motivée par la réduction des coûts d'infrastructure et l'accès à des technologies avancées, comme le cloud et l'intelligence artificielle.

La dépendance croissante des entreprises congolaises vis-à-vis des acteurs étrangers pour la gestion des données sensibles représenteraient un risque majeur pour la souveraineté numérique du pays, notamment en termes de sécurité des données et de perte de contrôle sur des informations stratégiques.

L'externalisation des data centers en RDC entraînerait des défis géopolitiques, notamment en raison de l'impact des législations étrangères (telles que le RGPD en Europe ou les lois américaines sur la surveillance) sur le traitement des données nationales. Le renforcement des infrastructures locales, un cadre juridique adapté et le développement de partenariats sécurisés pourraient permettre à la RDC de garantir la souveraineté numérique tout en bénéficiant des avantages des technologies avancées.

Les hypothèses sous-jacentes à cette analyse sont que d'une part, l'externalisation des data centers pourrait accroître les risques pour la sécurité et la souveraineté numérique de la RDC ; d'autre part, des solutions hybrides et des partenariats stratégiques pourraient permettre de concilier les avantages technologiques de l'externalisation avec une gestion sécurisée et souveraine des données.

Pour ce faire, cet article s'appuie sur une revue de la littérature existante sur l'externalisation des infrastructures numériques, les problématiques de souveraineté numérique et les tendances géopolitiques associées aux data centers. Il nous permettra de formuler des hypothèses sur les impacts de l'externalisation en RDC et d'élaborer des pistes pour un développement local des infrastructures tout en maintenant un contrôle sur les données nationales.

L'externalisation des data centers et la souveraineté numérique ont été des sujets largement étudiés, notamment dans des contextes où la gestion des données nationales par des acteurs étrangers est perçue comme une menace.

Parmi les travaux pertinents, on peut citer : Sullivan et Powell, qui ont étudié les enjeux de sécurité et de souveraineté numérique dans le cadre de l'externalisation des infrastructures IT, notamment pour les pays en développement.²

Bernhard et al. ont exploré les implications géopolitiques de l'externalisation des data centers, en se concentrant sur l'impact des législations sur la protection des données en Europe et aux États-Unis.³

Lopes et Silva ont analysé la dépendance des pays émergents vis-à-vis des fournisseurs internationaux de services cloud et les risques de perte de contrôle sur les données sensibles⁴ et de leur côté, Moulin et Dupont, qui ont mis en évidence l'importance de renforcer les infrastructures locales pour préserver la souveraineté numérique dans des pays comme le Brésil et l'Afrique du Sud, présentant des stratégies applicables à la RDC.⁵

Afin de répondre à ces enjeux, cette étude recourt à une méthode descriptive et analytique, en combinant des études de cas sur les expériences d'externalisation dans d'autres pays en développement, des entretiens avec des experts locaux et internationaux, ainsi qu'une analyse des politiques publiques en matière de gestion des données numériques en RDC.

L'article est structuré de manière telle que dans le premier point, on expose le contexte de l'externalisation des data centers en RDC, les motivations qui sous-tendent cette dynamique, ainsi que les acteurs impliqués.

² SULLIVAN M. et POWELL, P., *L'externalisation des infrastructures IT et les enjeux de souveraineté numérique*

Editions XYZ, Paris, 2020, pp. 134-145.

³ BERNHARD F., SCHMIDT T. et GAUTHIER M., *Les implications géopolitiques de l'externalisation des data centers*, PUF, Paris, 2018, pp. 89-102.

⁴ LOPES M. et SILVA J., *Dépendance et souveraineté numérique : L'impact des fournisseurs internationaux sur les pays émergents*, éd. Sciences du Numérique, Lisbonne, 2019, pp. 210-225.

⁵ MOULIN A. et DUPONT P., *Renforcer les infrastructures locales pour la souveraineté numérique : Stratégies pour les pays en développement*, éd. Futur Numérique, São Paulo, 2021, pp. 50-68.

Dans le deuxième point, les analyses portent sur les enjeux associés à la souveraineté numérique, notamment les risques pour la sécurité et la confidentialité des données. Le troisième et dernier point présente les défis à relever et les solutions possibles pour garantir une gestion souveraine des infrastructures numériques en RDC.

I. EXTERNALISATION DES DATA CENTERS EN RD CONGO

D'entrée de jeu, il sied de signifier que ce point table sur le paysage numérique en RDC ; les motivations pour l'externalisation des data centers ainsi que les acteurs impliqués.

I. 1. Le paysage numérique en RDC

La République Démocratique du Congo (RDC) a connu une évolution technologique marquée, bien que dans un contexte socio-économique difficile. Le pays, riche en ressources naturelles, a progressivement pris conscience de l'importance des technologies numériques, notamment à partir des années 2000, avec la généralisation de l'internet mobile et la croissance des infrastructures télécoms. L'adoption des smartphones, la couverture mobile qui s'est étendue et l'usage des réseaux sociaux ont permis une montée en puissance du secteur numérique.⁶

Les secteurs de la finance, de la santé, de l'éducation et de l'administration ont progressivement adopté les solutions numériques, créant une demande croissante pour les services numériques. De plus, la population jeune, dynamique et de plus en plus formée a accéléré cette transition vers une économie numérique. Cela a conduit à l'émergence d'un marché numérique de plus en plus compétitif, où les entreprises cherchent à exploiter le potentiel des données.

Avec la numérisation, la gestion et l'analyse des données sont devenues essentielles. Les entreprises congolaises, dans les secteurs de la télécommunication, de l'énergie, de la finance, ainsi que des administrations

⁶ MUNGANGA G., *Les défis de la transition numérique en République Démocratique du Congo : Entre espoirs et réalités*. Editions Universitaires Africaines, Kinshasa, 2021, p. 142.

publiques, ont compris que les données sont un atout stratégique pour leur compétitivité.

L'importance de la gestion des données est en forte croissance, car elles permettent une meilleure prise de décision, l'amélioration des services et l'optimisation des processus. De plus, avec la mise en place d'initiatives gouvernementales visant à moderniser l'administration et à renforcer la transparence, les institutions publiques voient dans l'exploitation des données un levier pour améliorer l'efficacité et la gouvernance.⁷

I. 2. Motivations pour l'externalisation des data centers

L'externalisation des data centers en RDC est principalement motivée par des considérations économiques. Le coût d'installation et d'entretien d'infrastructures locales de data centers peut être élevé, surtout dans un pays où les services énergétiques sont souvent coûteux et peu fiables.

En externalisant, les entreprises peuvent éviter les frais liés à l'achat de matériel informatique de pointe, à la gestion d'une infrastructure locale et à la maintenance des installations. Cela permet une gestion plus efficace des coûts opérationnels tout en réduisant les risques associés à l'infrastructure.⁸

Les services cloud (stockage, traitement de données, etc.), l'intelligence artificielle (IA) et d'autres technologies avancées nécessitent des équipements et des compétences spécifiques que beaucoup d'entreprises en RDC ne possèdent pas en interne.

En externalisant leurs data centers, elles peuvent avoir accès à des technologies modernes sans avoir à investir dans des infrastructures coûteuses et complexes. Ces services sont généralement fournis par des fournisseurs spécialisés qui offrent non seulement une meilleure performance mais aussi un support professionnel adapté à la gestion des données. De plus, cela permet

⁷ KASONGO S., *La révolution numérique en Afrique centrale : cas de la République Démocratique du Congo*. Presses Universitaires du Congo, Kinshasa, 2020, p. 115.

⁸ KABAGEMA J-P., « L'externalisation des data centers en Afrique : défis et opportunités », dans *Le Journal du Numérique*, Edition spéciale, Kinshasa, 2023, pp. 22-24.

aux entreprises de rester compétitives en profitant des innovations technologiques mondiales.

Une des raisons majeures de l'externalisation des data centers en RDC est le manque d'infrastructures locales robustes et fiables. En raison des défis liés à la stabilité énergétique, de la faible qualité des connexions internet et de la disponibilité limitée des services de data centers de qualité dans le pays, de nombreuses entreprises choisissent de confier leur gestion des données à des prestataires étrangers.

Cela garantit la sécurité et la continuité des services numériques, même en cas de perturbations locales. Ainsi, en externalisant, elles bénéficient d'une infrastructure plus stable, dotée de mécanismes de sauvegarde et de récupération des données en cas de sinistre.

I. 3. Acteurs impliqués dans l'externalisation

L'externalisation des data centers en RDC repose principalement sur des partenariats avec des fournisseurs internationaux bien établis dans le domaine des infrastructures numériques. Les grands acteurs comme Amazon Web Services (AWS), Microsoft Azure, Google Cloud, et d'autres opérateurs mondiaux sont souvent les principaux prestataires pour les entreprises congolaises.

En outre, des entreprises locales ou régionales telles que Liquid Telecom (qui offre des services de data center en Afrique) s'associent également à des entreprises congolaises pour proposer des solutions adaptées aux besoins du marché local. Ces partenariats permettent d'offrir des services de qualité tout en prenant en compte les spécificités du marché africain et congolais.⁹

Pour les entreprises, externaliser leurs data centers présente de multiples avantages. En premier lieu, on parle de la flexibilité et l'évolutivité qui peuvent facilement adapter leurs besoins en fonction de la croissance de leur activité sans devoir investir massivement dans des infrastructures physiques.

⁹ TSHILOMBO, S., « L'impact économique de l'externalisation des infrastructures IT en RDC », in *Revue d'Économie et Technologie*, Kinshasa, n°15, 2022, pp. 98-105.

En second, on relève la sécurité des données. Celles-ci bénéficient de mesures de sécurité plus strictes et d'une meilleure gestion des risques grâce à des prestataires spécialisés dans la gestion des données. En troisième lieu, il y a l'accès à l'innovation. Il peut intégrer de nouvelles technologies comme le cloud computing, l'IA, et l'Internet des objets (IoT), ce qui les aide à se moderniser et à se développer.

Pour les administrations publiques, externaliser peut apporter une amélioration de l'efficacité des services gouvernementaux, en facilitant la gestion des données, l'amélioration de la transparence et la simplification des processus. Les services publics peuvent ainsi se concentrer sur leur mission principale, tout en bénéficiant de la performance des solutions technologiques proposées par des experts internationaux.

L'externalisation des data centers en RDC est une réponse stratégique à plusieurs défis : réduire les coûts d'infrastructure, pallier le manque d'infrastructures locales et accéder à des technologies avancées pour soutenir l'essor numérique du pays.

II. ENJEUX POUR LA SOUVERAINETE NUMERIQUE NATIONALE

La souveraineté numérique nationale est un concept qui englobe la capacité d'un pays à contrôler et à protéger ses infrastructures et ses données numériques. Dans un contexte de mondialisation et d'interconnexion, les enjeux liés à cette souveraineté sont devenus cruciaux.

II. 1. Sécurité des données et confidentialité

La gestion des données numériques soulève plusieurs risques liés à la sécurité et à la confidentialité¹⁰ :

- Risques de piratage, espionnage industriel, et fuites de données sensibles : Les entreprises et les gouvernements collectent des quantités massives de données personnelles et sensibles. Si ces informations ne sont pas correctement protégées, elles peuvent être

¹⁰ BESSON P., et JEAN-MARC T., *La souveraineté numérique : Enjeux et défis pour les États*, éd. PUF, Paris, 2022, p. 154.

sujettes à des cyberattaques, des intrusions ou des fuites. Cela peut exposer des données stratégiques sur des secteurs sensibles comme la défense, les infrastructures critiques ou les données personnelles des citoyens.

- Dépendance vis-à-vis d'acteurs étrangers pour la gestion des données nationales : De nombreux services cloud et infrastructures numériques sont dominés par des entreprises étrangères, comme celles des États-Unis ou de la Chine. Cela crée une dépendance vis-à-vis de ces acteurs étrangers pour la gestion, l'hébergement et le traitement des données nationales. Cela peut engendrer des risques en matière de sécurité, mais aussi de souveraineté, car ces acteurs peuvent potentiellement accéder à ces données ou être soumis à des pressions politiques.

II. 2. Souveraineté numérique et contrôle des informations stratégiques

La souveraineté numérique est essentielle pour que l'État puisse exercer son autorité sur ses données et ses citoyens¹¹ :

- Risque de perte de contrôle sur les données sensibles : La délégation du stockage et du traitement des données à des acteurs étrangers ou à des entreprises privées peut entraîner une perte de contrôle sur des informations sensibles. Par exemple, les données personnelles des citoyens ou des données économiques et stratégiques peuvent être partagées sans consentement explicite ou protégées de manière insuffisante.
- Impact sur la capacité de régulation et de surveillance de l'État : L'État doit pouvoir réguler et surveiller les données qui circulent au sein de son territoire pour assurer la sécurité nationale, protéger la vie privée des citoyens et garantir l'application de ses lois. Cependant, si les données sont gérées par des acteurs étrangers ou échappent au contrôle national, cela peut rendre difficile l'application des lois locales et la régulation des flux de données.

¹¹ DELSOL, H. *La guerre numérique : Souveraineté et cybersécurité à l'heure des réseaux mondiaux*, Éditions du CNRS, Paris, 2021, p. 103.

II. 3. Implications géopolitiques

Les enjeux géopolitiques associés à la souveraineté numérique sont de plus en plus marqués dans le contexte international¹² :

- Les enjeux géopolitiques liés à la localisation des data centers à l'étranger : De nombreux pays ont recours à des data centers situés à l'étranger pour stocker leurs données, souvent dans des régions comme les États-Unis, l'Europe ou l'Asie. Cela soulève des questions de souveraineté, car un pays peut perdre la maîtrise de ses données si elles sont sous la juridiction d'un autre gouvernement. Par exemple, un gouvernement étranger pourrait imposer des restrictions ou des demandes d'accès aux données qui seraient difficiles à contester.
- Impact des politiques étrangères des fournisseurs : Les grandes entreprises technologiques qui fournissent des services de cloud et d'infrastructure numérique sont soumises aux lois de leur pays d'origine. Par exemple, les entreprises américaines sont tenues de se conformer à des législations comme le Cloud Act, qui permet au gouvernement des États-Unis d'accéder à certaines données stockées à l'étranger, même sans l'accord du pays concerné. De même, l'Union européenne a ses propres réglementations, telles que le Règlement général sur la protection des données (RGPD), qui a des implications sur la gestion des données personnelles à l'échelle mondiale. Ces lois peuvent avoir un impact direct sur la souveraineté numérique des pays qui utilisent ces services.

Les enjeux de souveraineté numérique sont nombreux et complexes, impliquant des questions de sécurité, de contrôle des informations stratégiques et de géopolitique. Les pays doivent prendre conscience de ces risques et mettre en place des stratégies pour protéger leurs données, réduire leur dépendance à des acteurs étrangers et garantir leur capacité à réguler le secteur numérique à l'échelle nationale.

¹² PASCUAL M. A., « Les enjeux géopolitiques de la souveraineté numérique », *Revue de géopolitique*, n°46, éd. La Découverte, Paris, 2023, pp. 45-68.

Dans ce contexte, les politiques de gouvernance des données et les choix d'infrastructure numérique doivent être soigneusement réfléchis pour maintenir la souveraineté numérique et assurer la sécurité des citoyens.

III. DEFIS ET SOLUTIONS POUR UNE GESTION SECURISEE ET SOUVERAINE DES INFRASTRUCTURES NUMERIQUES

Les défis et solutions pour une gestion sécurisée et souveraine des infrastructures numériques en République Démocratique du Congo touchent plusieurs aspects fondamentaux de la transformation numérique.

III. 1. Renforcement des capacités locales

La RDC, comme de nombreux pays en développement, fait face à des défis importants en matière d'infrastructure numérique et de compétences locales. L'un des principaux obstacles est le manque d'infrastructures locales adaptées (data centers, réseaux sécurisés, etc.), ce qui oblige souvent à dépendre des services étrangers pour l'hébergement et la gestion des données. De plus, la formation locale en technologies avancées reste limitée, ce qui freine l'innovation et la création d'entreprises spécialisées dans la gestion des données.

Il est crucial de former des professionnels locaux dans des domaines tels que la gestion des données, le cloud computing, la cybersécurité, etc. De plus, la construction de data centers locaux est essentielle pour garantir que les données sensibles restent sur le sol national, renforçant ainsi la souveraineté numérique et la sécurité des informations.

En soutenant les startups locales et en facilitant l'accès aux financements, la RDC pourrait favoriser l'émergence de solutions adaptées aux besoins spécifiques du pays tout en créant des emplois et en renforçant la compétitivité locale.

III. 2. Cadre juridique et réglementaire

Un autre défi majeur réside dans l'absence de lois locales suffisantes pour protéger les données des citoyens et des entreprises. La gestion des données sensibles est souvent soumise aux lois des pays étrangers, ce qui peut compromettre la souveraineté numérique de la RDC. De plus, le manque de

réglementation sur la cybersécurité expose les infrastructures locales à des risques d'attaques et de violations de données.

L'élaboration d'une législation claire sur la protection des données personnelles et des données sensibles est indispensable. Cela inclut la création de mécanismes de régulation et de surveillance des données pour garantir leur sécurité et leur gestion appropriée, en tenant compte des contextes culturels et sociaux de la RDC.

Les partenariats entre le gouvernement et des acteurs privés peuvent faciliter la mise en place d'infrastructures sécurisées et d'une gestion des données plus transparente. Ces collaborations doivent garantir que les données sensibles restent sous contrôle national tout en permettant l'accès à des technologies de pointe.

III. 3. Technologies alternatives et stratégies hybrides

La RDC, comme d'autres pays en développement, fait face à des défis technologiques en matière d'adoption et de mise en œuvre d'innovations numériques. L'intégration de technologies de pointe (comme le cloud computing) dans un cadre local peut poser des risques liés à la dépendance à des prestataires étrangers et à la vulnérabilité des données stockées à l'extérieur du pays.

Une approche hybride, combinant des solutions locales et étrangères, permettrait de réduire la dépendance à des fournisseurs externes tout en bénéficiant de technologies de pointe. Ces partenariats devraient être régis par des accords clairs sur la gestion des données et la sécurité.

La RDC pourrait investir dans des technologies comme la blockchain, qui offre un haut niveau de sécurité et de transparence pour la gestion des données, ainsi que les réseaux décentralisés, qui permettent de réduire la centralisation des données et d'améliorer la résilience des systèmes numériques.

Pour réussir une gestion sécurisée et souveraine des infrastructures numériques, la RDC doit surmonter plusieurs défis, notamment en termes d'infrastructures, de régulation et d'adoption technologique.

Les solutions proposées visent à renforcer les capacités locales, à développer un cadre juridique adapté et à explorer des technologies innovantes, tout en s'assurant que la souveraineté numérique du pays soit préservée. L'investissement dans ces domaines pourrait non seulement renforcer la sécurité numérique, mais aussi stimuler l'innovation et la croissance économique à long terme.

CONCLUSION

La révolution numérique, tout en apportant des avantages indéniables à la République Démocratique du Congo (RDC), soulève également des défis significatifs, notamment en matière de souveraineté numérique. L'externalisation des data centers, bien que motivée par des considérations économiques et technologiques, engendre des risques de dépendance vis-à-vis des acteurs étrangers, ce qui fragilise le contrôle local sur les données sensibles et expose le pays à des menaces de sécurité et de perte de souveraineté.

Les implications géopolitiques de cette externalisation sont également préoccupantes, car elles soulignent les tensions entre les législations nationales et les obligations des fournisseurs internationaux.

Afin de sécuriser la gestion des infrastructures numériques tout en préservant sa souveraineté, la RDC doit adopter une approche multifacette. D'abord, le renforcement des infrastructures locales et la formation de talents en technologies avancées sont des impératifs pour réduire la dépendance aux fournisseurs étrangers.

Ensuite, un cadre juridique national adapté à la protection des données et à la cybersécurité est essentiel pour garantir la confidentialité et la sécurité des informations stratégiques. Enfin, l'adoption de stratégies hybrides et l'exploration de technologies comme la blockchain permettront de mieux gérer les risques tout en tirant parti des innovations globales.

Ainsi, la RDC a la possibilité de construire un avenir numérique souverain, en conciliant développement technologique et contrôle national. Cette démarche nécessite une coopération renforcée entre le gouvernement, les

entreprises locales et les acteurs internationaux, afin de créer un écosystème numérique sécurisé et compétitif à l'échelle mondiale.

REFERENCE BIBLIOGRAPHIE

- BERNHARD F., SCHMIDT T. et GAUTHIER M., *Les implications géopolitiques de l'externalisation des data centers*, PUF, Paris, 2018.
- BESSON P. et JEAN-MARC T., *La souveraineté numérique : Enjeux et défis pour les Etats*, éd. PUF, Paris, 2022.
- BOUCHER J-F., *La souveraineté numérique et l'infrastructure des données*, éd. Technopolis, Paris, 2022.
- DELSOL H., *La guerre numérique : Souveraineté et cybersécurité à l'heure des réseaux mondiaux*, Éditions du CNRS, Paris, 2021.
- KABAGEMA J. P., « L'externalisation des data centers en Afrique : défis et opportunités », in *Le Journal du Numérique*, Édition spéciale, Kinshasa, 2023.
- KASONGO S., *La révolution numérique en Afrique centrale : cas de la République Démocratique du Congo*, Presses Universitaires du Congo, Kinshasa, 2020.
- LOPES M. et SILVA J., *Dépendance et souveraineté numérique : L'impact des fournisseurs internationaux sur les pays émergents*, éd. Sciences du Numérique, Lisbonne, 2019.
- MOULIN A. et DUPONT P., *Renforcer les infrastructures locales pour la souveraineté numérique : Stratégies pour les pays en développement*, éd. Futur Numérique, São Paulo, 2021.
- MUNGANGA G., *Les défis de la transition numérique en République Démocratique du Congo : Entre espoirs et réalités*, Editions Universitaires Africaines, Kinshasa, 2021.
- PASCUAL M. A., « Les enjeux géopolitiques de la souveraineté numérique », dans *Revue de géopolitique*, n° 46, éd. La Découverte, Paris, 2023.
- SULLIVAN M. et POWELL P., *L'externalisation des infrastructures IT et les enjeux de souveraineté numérique*, éd. XYZ, Paris, 2020.

-
- TSHILOMBO S., « *L'impact économique de l'externalisation des infrastructures IT en RDC* », in *Revue d'Économie et Technologie*, Kinshasa, n°15, 2022.