ESI Preprints **Not Peer-reviewed**

Gouvernance numérique résiliente en République Démocratique du Congo : vers un modèle d'État-plateforme inclusif pour les contextes de faible connectivité et de fragilité institutionnelle

Lowembo A Tshotsho Raymond Albert
Université Pédagogique de Kananga (UPKAN),
République démocratique du Congo

Approved: 24 November 2026
Posted: 26 November 2026

Copyright 2026 Author(s)
Under Creative Commons CC-BY 4.0
OPEN ACCESS

Cite As:
Lowembo A Tshotsho, R.A. (2026). *Gouvernance numérique résiliente en République Démocratique du Congo : vers un modèle d'État-plateforme inclusif pour les contextes de faible connectivité et de fragilité institutionnelle*. ESI Preprints.
https://doi.org/10.19044/esipreprint.11.2026.p603

Résumé

La République démocratique du Congo (RDC) se trouve à un moment charnière de son histoire technologique et institutionnelle. Portée par la vision « DRC Digital Nation 2030 », le lancement du Plan National du Numérique 2026-2030 (PNN2) et de la Stratégie Nationale d'Intelligence Artificielle (SNAI) matérialise une ambition claire : faire du numérique le moteur principal de la gouvernance, de la croissance économique et de l'inclusion sociale. Cependant, la réalité territoriale impose un principe de réalité complexe : un territoire de plus de 2,3 millions de km², une connectivité inégalement répartie, une fragmentation institutionnelle persistante et des urgences humanitaires récurrentes coexistent avec cette ambition de dématérialisation des services publics.

Cet article propose une contribution théorique originale en introduisant le concept de **« Governance Resilience by Design »** (gouvernance résiliente dès la conception). Ce cadre postule que dans les États fragiles à forte dispersion territoriale, la performance de la gouvernance numérique ne dépend pas uniquement de l'interopérabilité des plateformes, mais fondamentalement de leur capacité à maintenir la continuité des services publics essentiels en conditions de dégradation prolongée de la connectivité, de l'énergie ou de la sécurité.

À travers une analyse narrative structurée des politiques publiques (2020-2026) et une comparaison internationale (Estonie, Inde, Rwanda, Singapour), l'article examine les fondations posées par la RDC, identifie cinq contraintes systémiques et propose un modèle d'État-plateforme à six couches. Il évalue également la maturité numérique du pays via un indice original (IMENR-RDC) et explore le rôle de l'intelligence artificielle comme accélérateur de cette gouvernance résiliente. L'article soutient que la réussite de l'État numérique congolais dépendra moins du nombre d'applications lancées que de la capacité à rendre les services publics fiables, accessibles, sécurisés et responsables dans l'ensemble du pays.

Mots-clés : Gouvernance numérique ; Résilience by Design ; Infrastructure publique numérique ; Faible connectivité ; Souveraineté numérique ; Intelligence artificielle

Resilient Digital Governance in the Democratic Republic of the Congo: Towards an Inclusive Platform-State Model for Low-Connectivity and Institutionally Fragile Contexts

Lowembo A Tshotsho Raymond Albert
Kananga Pedagogical University (UPKAN),
Democratic Republic of the Congo

Abstract

The Democratic Republic of the Congo (DRC) stands at a pivotal moment in its technological and institutional history. Driven by the 'DRC Digital Nation 2030' vision, the launch of the 2026–2030 National Digital Plan (PNN2) and the National Artificial Intelligence Strategy (SNAI) reflects a clear ambition: to make digital technology a key driver of governance, economic growth, and social inclusion. However, territorial realities impose significant constraints: a country spanning more than 2.3 million km², uneven connectivity, persistent institutional fragmentation, and recurring humanitarian emergencies coexist with this ambition to dematerialize public services. This article makes an original theoretical contribution by introducing the concept of 'Governance Resilience by Design'. The framework posits that, in fragile states characterized by wide territorial dispersion, the performance of digital governance depends not only on platform interoperability but fundamentally on the ability to maintain the continuity of essential public services under prolonged disruptions to connectivity, energy, or security. Through a structured narrative analysis of

public policies (2020–2026) and an international comparison (Estonia, India, Rwanda, and Singapore), the article examines the foundations established by the DRC, identifies five systemic constraints, and proposes a six-layer platform-state model. It also assesses the country's digital maturity through an original index (DGMI-DRC) and explores the role of artificial intelligence as an accelerator of resilient governance. The article argues that the success of the Congolese digital state will depend less on the number of applications launched than on its capacity to make public services reliable, accessible, secure, and accountable throughout the country.

Keywords: Digital governance; Resilience by Design; Digital public infrastructure; Low connectivity; Digital sovereignty; Artificial intelligence

1. Introduction

Les technologies numériques peuvent aider les pouvoirs publics à étendre les services, à améliorer la coordination administrative et à rendre les décisions publiques plus traçables. Toutefois, la numérisation ne produit pas automatiquement une meilleure gouvernance. La technologie peut reproduire les faiblesses institutionnelles existantes lorsque les administrations développent des systèmes déconnectés, que les institutions publiques ne disposent pas des capacités nécessaires pour gérer leurs fournisseurs ou que les citoyens ne peuvent accéder aux services en raison de problèmes de connectivité, de coût, de handicap, de langue ou de littératie. La transformation numérique est donc autant un processus politique, organisationnel et institutionnel qu'un processus technique (Dunleavy et al., 2006 ; Banque mondiale, 2016).

Dans un pays où l'État doit rester opérant même lorsque la connexion disparaît, la souveraineté numérique ne se réduit pas à l'hébergement des données : elle commence par la capacité des institutions publiques à continuer d'assurer leurs services essentiels en situation de connectivité dégradée ou d'interruption prolongée.

La RDC constitue un terrain particulièrement important pour examiner ces tensions. Son territoire dépasse 2,3 millions de kilomètres carrés, tandis que les infrastructures de transport, d'électricité et de télécommunications restent inégalement réparties. Dans certaines provinces, l'éloignement administratif est aggravé par l'insécurité, les déplacements de population et la pression exercée sur les services de santé et les services humanitaires. Parallèlement, cette ambition s'est récemment structurée autour de la vision « DRC Digital Nation 2030 », du PNN2 et de la SNAI, soutenue par une mobilisation annoncée de près de 1 milliard USD de ressources publiques sur cinq ans, adossée à plus de 500 millions USD d'appuis extérieurs (Banque mondiale, 2024).

Cet article pose trois questions : (1) Quelles conditions institutionnelles et infrastructurelles façonnent la gouvernance numérique en RDC ? (2) Quels risques apparaissent lorsque des systèmes d'identité numérique et des plateformes de services publics sont introduits dans un contexte de capacités étatiques inégales et de vulnérabilité humanitaire ? (3) Quels principes de conception et de gouvernance pourraient rendre la transformation numérique plus résiliente et inclusive à l'horizon 2030 ?

1.1. Contributions de l'étude

Cet article apporte quatre contributions principales à la littérature sur la gouvernance numérique :

1. **Une analyse actualisée** de la trajectoire de la gouvernance numérique congolaise (2020-2026) ;
2. **Un cadre d'interprétation** fondé sur l'infrastructure publique numérique (IPN) et adapté aux contextes de fragilité ;
3. **Un modèle conceptuel original** : l'État-plateforme résilient, articulé autour du concept de « Governance Resilience by Design » ;
4. **Une proposition d'indice de maturité** (IMENR-RDC) et d'indicateurs de suivi adaptés aux États à faible connectivité.

2. Méthodologie

Il s'agit d'un article conceptuel et d'analyse des politiques publiques. Il synthétise des documents de politique publique et institutionnels accessibles au public, des publications sur le développement international et des travaux scientifiques pertinents pour l'administration numérique.

2.1. Sélection documentaire

La revue documentaire couvre la période 2020-2026. Les sources ont été sélectionnées selon quatre catégories :

- **Institutions internationales** : Enquête des Nations Unies sur l'administration en ligne (UN DESA, 2024), documentation du Projet de transformation numérique de la RDC (Banque mondiale), cadre sur l'IPN (Groupe de la Banque mondiale, 2025), rapports GSMA (2025).
- **Sources gouvernementales** : annonces relatives au PNN2, à la SNAI, à RDC-PASS et au Code du Numérique (RDC, 2023).
- **Littérature académique indexée** : travaux sur la gouvernance à l'ère numérique (Dunleavy et al., 2006), le saut technologique et l'infrastructure publique numérique.
- **Documents stratégiques** : plans sectoriels (santé, finances, télécommunications).

2.2. Cadre d'analyse

L'analyse mobilise une grille de lecture à cinq dimensions pour évaluer la gouvernance numérique congolaise :

Tableau 1 : Grille de lecture du cadre analytique

Dimension	Questions directrices
Gouvernance	Qui décide ? Comment sont réparties les responsabilités ?
Technologie	Comment interopérer ? Quelles architectures pour les contextes contraints ?
Inclusion	Qui est laissé de côté ? Comment garantir l'accès universel ?
Résilience	Le système survit-il aux crises (énergétiques, sécuritaires, réseau) ?
Souveraineté	Qui contrôle les données et les infrastructures critiques ?

Les éléments de preuve sont répartis en trois catégories : (a) les faits documentés ; (b) les ambitions politiques ou annonces de projets ; et (c) l'interprétation analytique et les recommandations de l'auteur.

3. Cadre théorique

3.1. Gouvernance à l'ère numérique et modèle de l'État-plateforme

La gouvernance à l'ère numérique met l'accent sur la réintégration des services publics, une approche globale centrée sur les usagers et la numérisation étendue des processus administratifs (Dunleavy et al., 2006). Cette perspective remet en question l'idée selon laquelle chaque ministère devrait acquérir et gérer ses technologies de manière indépendante. Une approche de l'État-plateforme consiste plutôt à créer des capacités communes — telles que la vérification de l'identité, l'échange sécurisé de données, les paiements et les signatures électroniques — que plusieurs administrations peuvent réutiliser. Une infrastructure partagée peut réduire les doublons, mais elle concentre également les risques : des défaillances, des cyberattaques ou une gouvernance déficiente à un niveau fondamental peuvent affecter simultanément de nombreux services.

3.2. Infrastructure Publique Numérique

L'Infrastructure Publique Numérique (IPN), également désignée dans la littérature internationale sous l'appellation *Digital Public Infrastructure* (DPI), désigne des composants numériques fondamentaux qui soutiennent plusieurs services publics et privés. Parmi les exemples courants figurent l'identité numérique, les paiements numériques et les mécanismes de partage des données. Le Groupe de la Banque mondiale (2025) souligne que ces fondations devraient être ouvertes, modulaires, inclusives, centrées sur les utilisateurs et encadrées par des garanties de protection de la vie privée et de sécurité. L'IPN ne doit pas être assimilée à une application nationale unique ni à une base de données centralisée contenant toutes les informations de chaque citoyen. Une architecture saine sépare les fonctions, limite les

échanges de données aux finalités légitimes, enregistre les accès et permet un contrôle.

Les modèles internationaux reconnus — l'India Stack en Inde, SingPass à Singapour ou X-Road en Estonie — illustrent cette approche modulaire : une couche d'identité, une couche d'échange (API interopérables) et une couche d'applications sectorielles. La RDC s'en inspire en associant le RDC-PASS au Répertoire National d'Identification des Personnes Physiques (RNI), première pierre d'un modèle où toute administration ou entreprise privée autorisée peut greffer ses services sur le socle étatique de manière sécurisée. Cette approche modulaire permettra à n'importe quelle administration ou entreprise privée autorisée de greffer ses services sur le socle étatique de manière sécurisée et instantanée.

3.3. Saut technologique (Leapfrogging) et contraintes des pays arrivés plus tard

Le saut technologique (*leapfrogging*) désigne la possibilité d'adopter des technologies plus récentes sans reproduire toutes les étapes du développement antérieur des infrastructures (Perkins, 2024). Les théories du développement tardif montrent que les pays en développement peuvent contourner les étapes intermédiaires d'infrastructures lourdes (comme les réseaux filaires en cuivre) pour adopter directement des paradigmes de rupture (mobile-first, cloud-native). Les services mobiles, les plateformes infonuagiques et l'identité numérique peuvent accroître rapidement les capacités.

Toutefois, le saut technologique ne signifie pas importer des technologies sans adaptation. En l'absence d'électricité stable, de fonctionnaires qualifiés, d'expertise en passation des marchés, de budgets de maintenance et de garanties juridiques dignes de confiance, les systèmes avancés risquent de devenir des îlots technologiques coûteux. Pour que ce saut ne se transforme pas en « mimétisme institutionnel » inefficace, la gouvernance numérique congolaise doit s'articuler autour de spécificités endogènes : l'enclavement territorial comme moteur de dématérialisation, la démographie « mobile-first » (plus de 65 % de la population a moins de 25 ans), le nexus humanitaire-développement et la transition institutionnelle en cours. La question pertinente n'est pas de savoir si la RDC peut adopter des outils modernes, mais si elle peut les exploiter, les gouverner et les adapter dans la durée.

3.4. Inclusion, droits et résilience

Les services publics numériques doivent être évalués non seulement selon leur disponibilité, mais aussi selon leur accessibilité effective, leur fiabilité, leur coût abordable, leur facilité d'utilisation et l'existence de voies

de recours. Dans les contextes fragiles, les données relatives à l'identité, à la santé, aux déplacements ou à l'aide sociale peuvent exposer les personnes à la fraude, à la discrimination, à la surveillance ou à des préjudices physiques si elles sont collectées de manière excessive ou divulguées de façon inappropriée. La résilience doit donc inclure la continuité technique, la responsabilité institutionnelle et la protection des personnes, et pas seulement la disponibilité du système.

Le contexte congolais introduit une variable inédite dans l'étude des systèmes d'information : la nécessité de concevoir des architectures numériques résilientes en zone de crise humanitaire prolongée. La numérisation des données biométriques ou sanitaires dans les zones de déplacement de l'Est (Nord-Kivu, Ituri) présente un niveau de risque élevé ; elle exige un cadre éthique strict, intégrant la minimisation des données et des techniques de chiffrement avancé, pour s'assurer que les outils d'inclusion numérique ne se transforment pas en instruments de vulnérabilité.

3.5. Contribution théorique originale : le concept de « Governance Resilience by Design »

Cette étude propose le concept de **« Governance Resilience by Design »** (gouvernance résiliente dès la conception) pour les États fragiles à forte dispersion territoriale.

Définition : La gouvernance numérique résiliente désigne la capacité d'un État à maintenir la continuité des services numériques essentiels malgré les défaillances simultanées de la connectivité, de l'énergie, des infrastructures ou des institutions.

Ce concept postule que l'évaluation d'un système de gouvernance numérique ne doit pas se limiter à son taux de numérisation ou à son interopérabilité en conditions optimales, mais doit intégrer nativement sa capacité à fonctionner en mode dégradé. Il s'agit de passer d'une logique de « résilience par l'ajout » (backup) à une logique de « résilience par l'architecture » (by design).

4. Comparaison internationale : quelles leçons pour la RDC ?

Pour évaluer la trajectoire congolaise, il est utile de la comparer aux modèles internationaux de référence.

Tableau 2 : Comparaison de quelques modèles de référence

Pays	Infrastructure (DPI)	Identité numérique	Priorité « Offline »	Leçon principale pour la RDC
Estonie	X-Road	Oui (e-ID)	Faible besoin	Gouvernance des données et interopérabilité poussée.
Inde	India Stack	Aadhaar	Partiel	Inclusion massive et échelle démographique.
Rwanda	Irembo	Oui	Croissante	Simplification

Pays	Infrastructure (DPI)	Identité numérique	Priorité « Offline »	Leçon principale pour la RDC
				administrative et volonté politique.
RDC	En construction	RDC-PASS	**Critique**	**Résilience territoriale et continuité en mode dégradé.**

Analyse : Contrairement à l'Estonie ou à l'Inde, la RDC ne peut pas présumer d'une connectivité permanente. Là où l'Inde utilise l'identité pour l'inclusion de masse, la RDC doit utiliser l'architecture numérique pour garantir la survie de l'administration dans les zones enclavées.

5. Paysage de la gouvernance numérique en RDC

5.1. Ambitions nationales et référence internationale

L'Enquête des Nations Unies sur l'administration en ligne 2024 fournit un point de comparaison mondial couvrant 193 États membres et met en évidence la persistance d'écarts régionaux en matière de services en ligne, d'infrastructures de télécommunications et de capacités humaines (UN DESA, 2024). La RDC occupe la 179e place sur 193 au classement de l'E-Government Development Index (EGDI) en 2024. Ces classements sont des indicateurs utiles, mais ils ne rendent pas pleinement compte des disparités locales au sein d'un pays de grande taille ni de la qualité des services telle qu'elle est vécue par les communautés rurales. Ils devraient être complétés par des mesures nationales portant sur le coût, la fiabilité, l'utilisation, l'inclusion et les résultats des services.

La RDC a exprimé son ambition de doter le secteur public de capacités numériques accrues, désormais structurée par le PNN2 et la SNAI, présentés lors de l'Assemblée générale des Nations Unies à New York sous la bannière « DRC Digital Nation 2030 ». Toutefois, les plans politiques, les annonces budgétaires, les accords signés, les étapes de passation des marchés et les services effectivement opérationnels correspondent à des phases de mise en œuvre différentes. Les analyses internationales devraient indiquer la source et la date de chaque affirmation et éviter de présenter les investissements annoncés comme des dépenses intégralement décaissées ou des infrastructures achevées.

5.2. RDC-PASS et identité numérique

Le 13 juin 2026, la Présidence a annoncé le lancement de RDC-PASS, présenté comme un système national d'identification numérique destiné à fournir aux citoyens un identifiant numérique unique et à faciliter l'accès à certains services publics, financiers et sociaux. Doté d'un budget annoncé de 97,1 millions USD et structuré en partenariat public-privé avec Trident Digital Tech DRC Africa, le projet vise à interconnecter les services (passeports, permis, prestations sociales) sans remplacer la carte d'identité

physique. La Présidence a également précisé que RDC-PASS n'est pas une carte nationale d'identité et ne remplace pas les documents d'identité prévus par la loi (Présidence de la République démocratique du Congo, 2026). Cette annonce constitue une évolution importante des politiques publiques, mais l'annonce d'un lancement ne prouve pas à elle seule que l'enrôlement universel, l'interopérabilité à l'échelle nationale, la disponibilité des services ou une assurance indépendante de la sécurité ont déjà été réalisés.

Sur le plan conceptuel, le RDC-PASS suit la logique de l'infrastructure publique numérique : il ne s'agit pas d'un produit isolé, mais d'une couche de base interopérable permettant l'authentification cross-administrative. L'identité numérique peut réduire la répétition des démarches administratives, mais elle peut également créer de l'exclusion si l'enregistrement est difficile, si les dossiers comportent des erreurs, si l'authentification échoue ou si une personne ne dispose pas d'un appareil ou d'une connexion fiable. Le système doit donc prévoir des procédures accessibles de correction et de recours, des solutions alternatives pour les personnes incapables de s'enregistrer numériquement, une supervision indépendante, des règles claires de conservation des données et des protections contre l'extension progressive des finalités. La vérification d'identité ne devrait révéler que les informations strictement nécessaires à une transaction donnée.

En septembre 2026, les informations publiques faisaient état d’une première phase opérationnelle, avec la formation de 50 agents chargés de l’enregistrement et un déploiement appelé à s’étendre progressivement. Cette évolution marque le passage d’une annonce institutionnelle à une phase préparatoire d’exécution, sans permettre encore d’établir l’ampleur territoriale de l’enrôlement, le nombre d’identifiants effectivement délivrés, le niveau d’interopérabilité atteint ou la disponibilité réelle des services dans les provinces (Agence Ecofin, 2026).

5.3. Connectivité et services rendus possibles par le numérique

Le Projet de transformation numérique de la RDC de la Banque mondiale (P180495), approuvé en juin 2024 avec un engagement total de 400 millions de dollars américains et une date de clôture fixée au 31 décembre 2029, vise à élargir l'accès à un haut débit abordable et de qualité, à promouvoir les services et solutions numériques et à renforcer les compétences numériques adaptées aux besoins de l'industrie (Banque mondiale, s. d.). La documentation du projet présente la connectivité et les fondations numériques comme des objectifs liés plutôt que distincts. Le rapport de la GSMA publié en 2025 estime que des réformes numériques ciblées pourraient connecter 9,7 millions d'utilisateurs uniques supplémentaires à l'internet mobile et ajouter 9 800 milliards de francs

congolais au PIB d'ici 2029 ; il s'agit de projections conditionnelles et non de résultats déjà obtenus (GSMA, 2025). Les prévisions sectorielles de la GSMA évoquent par ailleurs une valeur ajoutée directe d'environ 4,1 milliards USD à l'économie congolaise d'ici 2029.

À ces financements s'ajoutent des initiatives structurantes : l'accord United Investment LMT (150 millions USD) pour l'extension de la dorsale nationale en fibre optique (60 000 à 80 000 km additionnels) et la construction de trois centres de données nationaux ; la digitalisation fiscale et douanière (DGI et DGDA) ; le Guichet Unique de Création d'Entreprises ; et la création de l'Agence Nationale d'Ingénierie Clinique et du Numérique de la Santé (ANICNS) pour la télémédecine et la gestion prédictive des crises sanitaires.

Ces sources confirment l'importance de la connectivité et des compétences numériques, mais elles ne justifient pas de considérer la couverture nationale comme uniforme. Une liaison de fibre optique, un signal mobile, des données abordables, une électricité fiable et un service public utilisable sont des composantes distinctes. Les données sectorielles disponibles appellent à distinguer couverture et usage. La GSMA indiquait en septembre 2025 que seuls 45 % de la population étaient couverts par l'Internet mobile et que l'abordabilité des terminaux et des données, ainsi que l'irrégularité de l'approvisionnement électrique dans les zones rurales, demeuraient des obstacles majeurs (GSMA, 2025). Les communautés rurales et éloignées peuvent cumuler plusieurs obstacles. Les politiques publiques devraient donc suivre l'accès effectif et la qualité des services, et non le seul nombre de kilomètres d'infrastructure déployés.

Le rapport de mise en œuvre publié par la Banque mondiale le 28 mai 2026 situe toutefois le Projet de transformation numérique dans une phase encore précoce. La progression vers l’objectif de développement et l’avancement global de la mise en œuvre y sont tous deux classés « modérément satisfaisants », tandis que le risque global demeure substantiel. À cette date, les décaissements atteignaient environ 20 millions USD pour l’IDA et 7 millions EUR pour l’Agence française de développement, soit un taux global estimé à 3,9 %. Le rapport indique également que la mise en œuvre physique et technique progressait plus lentement que prévu. Ces éléments renforcent la nécessité de distinguer les financements approuvés, les ressources effectivement décaissées, les infrastructures déployées et les services réellement accessibles aux usagers (Banque mondiale, 2026).

5.4. Coordination institutionnelle et capacité de mise en œuvre

Un État numérique exige une répartition claire des responsabilités en matière de normes, d'architecture, de cybersécurité, de passation des marchés, de gouvernance des données et de responsabilité des services.

Lorsque les administrations développent leurs plateformes de manière indépendante, l'État risque d'accumuler des bases de données qui se chevauchent, des identifiants incompatibles, des contrats propriétaires et des coûts récurrents de maintenance. La coordination centrale peut contribuer à établir des normes communes, mais une centralisation excessive peut aussi créer des goulets d'étranglement et un point unique de défaillance. Une gouvernance fédérée est plus adaptée : des règles communes et des composants partagés, avec des responsabilités clairement attribuées et une prestation de services adaptée aux besoins sectoriels et locaux.

La création du Ministère de l'Économie Numérique, les travaux du PNN2 et la validation en 2026 de nouvelles orientations nationales relatives à l'économie numérique et à l'intelligence artificielle témoignent d'une volonté d'harmonisation. Le défi est désormais institutionnel : harmoniser, standardiser, sécuriser. Les quatre piliers du PNN2 — infrastructures et connectivité ; transformation des services publics ; capital humain et inclusion ; cybersécurité et confiance — s'articulent autour de cinq axes transversaux : entrepreneuriat technologique, innovation locale, intelligence artificielle, souveraineté numérique et partenariats stratégiques.

La Politique sectorielle de l’économie numérique (PSEN) et la Stratégie nationale de l’intelligence artificielle (SNIA), validées en 2026, doivent être distinguées tout en étant articulées au PNN2. Le PNN2 organise les priorités nationales de transformation ; la PSEN fournit un cadre sectoriel de planification, de coordination et de suivi ; la SNIA encadre plus spécifiquement le développement et la gouvernance de l’intelligence artificielle. Leur cohérence opérationnelle dépendra de la clarification des responsabilités, de l’établissement d’indicateurs, de la budgétisation et de la traduction des orientations en programmes exécutables (Agence Ecofin, 2026).

5.5. Cadre juridique et réglementaire

Le Code du Numérique (Ordonnance-loi n° 23/010 de 2023) constitue la pierre angulaire. Cependant, son application opérationnelle reste balbutiante. Une analyse des textes révèle des lacunes dans :

- **La protection des données** : manque d'autorité de contrôle indépendante pleinement opérationnelle ;
- **La signature électronique** : reconnaissance juridique à généraliser ;
- **La cybersécurité** : besoin de renforcer l'arsenal répressif face à la cybercriminalité ;
- **L'e-commerce** : régulation encore insuffisante pour sécuriser les transactions

6. Intelligence artificielle publique responsable

La Stratégie nationale de l'intelligence artificielle fait désormais partie des orientations nationales validées en 2026. Cette évolution renforce l'intérêt d'un cadre d'IA publique responsable articulant innovation, gouvernance des données, cybersécurité, compétences et contrôle humain. L'IA peut agir comme un accélérateur de la gouvernance résiliente, sous conditions (Agence Ecofin, 2026).

6.1. Cas d'usage prioritaires

- **Administration fiscale** : détection de la fraude via l'analyse des données DGI/DGDA.
- **Santé publique** : prédiction épidémique via l'ANICNS.
- **Logistique humanitaire** : optimisation des chaînes d'approvisionnement dans les zones de déplacement.
- **Maintenance prédictive** : surveillance des infrastructures critiques (réseaux, data centers).

6.2. Conditions d'adoption

Pour être résiliente, l'IA publique doit être encadrée par :

- **L'auditabilité** : traçabilité des algorithmes.
- **La supervision humaine** : décision finale laissée à l'agent public.
- **La transparence** : explicabilité des modèles.
- **La protection des données** : conformité stricte avec le Code du Numérique.



Figure 1 : Condition d'adoption de l'IA Publique responsable

L'adaptation linguistique constitue également une condition d'inclusion. Le projet annoncé de collecte de données en lingala pour contribuer au développement d'outils d'intelligence artificielle adaptés au contexte congolais ouvre une perspective importante pour les interfaces et services publics multilingues. Une telle initiative devrait être accompagnée de règles explicites relatives à la provenance des données, au consentement, à la représentativité des variantes linguistiques, à la prévention des biais et aux droits des contributeurs (Agence Ecofin, 2026).

7. Maturité numérique de l'État : l'indice IMENR-RDC

Pour situer la RDC, nous proposons le **Indice de maturité de l'État numérique résilient en RDC (IMENR-RDC)**, un modèle à 5 niveaux adapté aux États fragiles :

L'IMENR-RDC est un cadre conceptuel proposé par l'auteur. Il se distingue des instruments internationaux existants, notamment du Digital Government Model Framework présenté par l'ONU en 2024 et des indices de maturité employés par d'autres organisations. Sa finalité n'est pas de produire un classement officiel, mais d'évaluer conjointement la numérisation, l'interopérabilité, la continuité en mode dégradé, la souveraineté opérationnelle et la protection des droits.

Niveau 1 : Administration papier (registres physiques).
Niveau 2 : Numérisation documentaire (bureautique, fichiers locaux).
Niveau 3 : Services en ligne (portails isolés).
Niveau 4 : Interopérabilité nationale (API, identité unique).
Niveau 5 : État-plateforme résilient (offline-first, souveraineté, continuité).

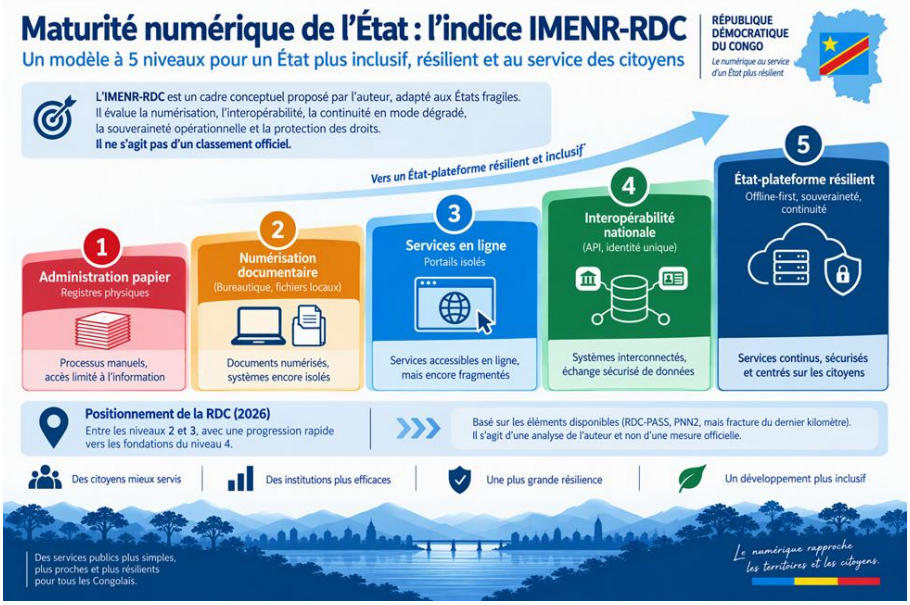

Figure 2 : Indice de maturité du gouvernement numérique IMENR-RDC

Positionnement de la RDC (2026) : Sur la base des éléments disponibles (lancement du RDC-PASS, PNN2, mais fracture du dernier kilomètre), la RDC se situe entre les **niveaux 2 et 3**, avec une progression rapide vers les fondations du niveau 4. Il s'agit d'une analyse de l'auteur et non d'une mesure officielle.

8. Obstacles structurels et risques

8.1. Fragmentation des systèmes et faible interopérabilité

Des applications déconnectées compliquent l'échange d'informations fiables et peuvent contraindre les citoyens à soumettre plusieurs fois les mêmes documents. L'interopérabilité ne se réduit pas à une question d'API : elle exige des définitions de données convenues, des règles de rapprochement des identités, une base juridique, des accords de niveau de service, des journaux d'audit et une procédure de résolution des erreurs de données. La traçabilité est un complément indispensable : la journalisation inaltérable des modifications (qui a modifié quoi, quand et pourquoi) permet l'auditabilité et l'imputabilité des opérations administratives. Sans elle, l'interopérabilité peut accélérer la circulation d'informations erronées ou frauduleuses au lieu de renforcer la fiabilité des services. Les contrats de passation des marchés devraient exiger des interfaces documentées, la portabilité des données, des dossiers exportables et une assistance à la transition afin de réduire la dépendance à l'égard d'un fournisseur.

En dépit des directives de l'ADN, la persistance d'une gouvernance en silos mène à une prolifération de plateformes propriétaires non interopérables, augmentant les coûts de maintenance transactionnelle et dégradant l'expérience utilisateur des citoyens.



Figure 3 : Fragmentation des systèmes et faible interopérabilité

8.2. Le dernier kilomètre : connectivité, énergie et coût

Les services publics qui exigent une connexion haut débit permanente, des smartphones récents ou une alimentation électrique ininterrompue peuvent exclure précisément les communautés auxquelles ils sont destinés. La planification de la résilience devrait prévoir une alimentation électrique de secours, la mise en cache locale, des interfaces à faible consommation de données, le SMS ou l'USSD lorsque cela est pertinent, des centres de services accessibles et des procédures de fonctionnement lors de pannes prolongées.

Dans plusieurs provinces, les interruptions de réseau peuvent dépasser plusieurs heures par jour et les microcoupures électriques empêchent le maintien de serveurs classiques. Le principe directeur devrait être que la connectivité ne constitue jamais un point unique de défaillance des services publics essentiels : une administration ne doit pas cesser de fonctionner parce qu'un câble a été coupé. Cela implique de dimensionner les services prioritaires pour un fonctionnement local, avec une alimentation de secours et des procédures de continuité testées, plutôt que de supposer une disponibilité permanente du réseau et de l'énergie.

Le fonctionnement hors ligne doit être soigneusement conçu : les dossiers locaux nécessitent chiffrement, contrôle des accès, résolution des conflits et synchronisation sécurisée au rétablissement de la connectivité.

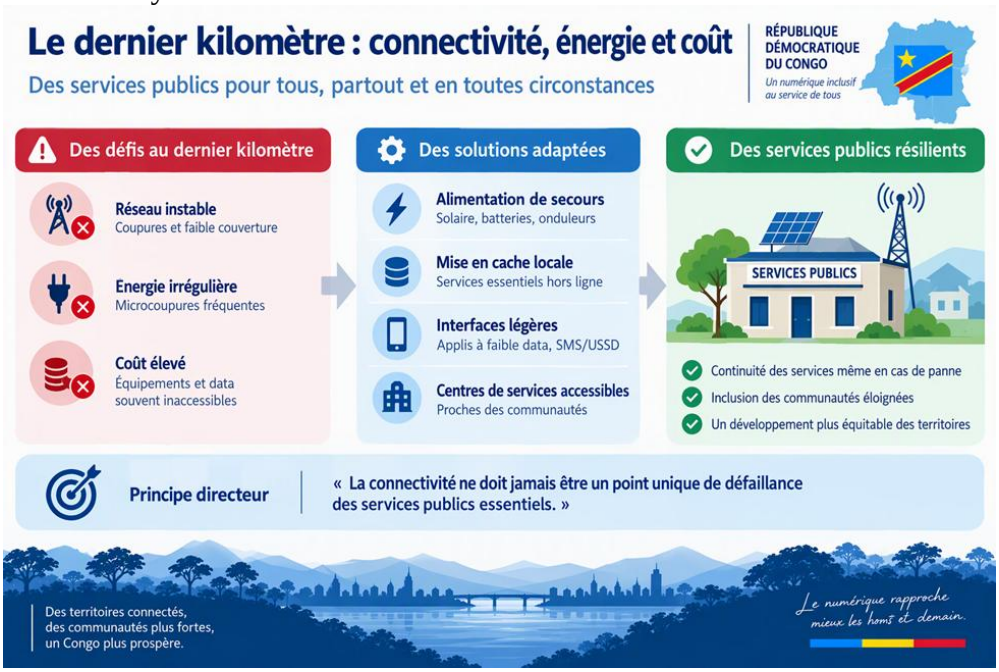

Figure 4 : Le dernier kilomètre

8.3. Compétences, marchés publics et mémoire institutionnelle

Les capacités techniques ne se limitent pas au développement logiciel. Les institutions publiques ont besoin de responsables de produits, d'architectes d'entreprise, de spécialistes de la cybersécurité, de gestionnaires de données, de spécialistes des marchés publics, de gestionnaires d'archives et d'agents de première ligne capables d'accompagner les usagers. L'externalisation peut apporter de l'expertise, mais elle ne devrait pas transférer toute la capacité décisionnelle aux fournisseurs. Les contrats devraient inclure la formation, la documentation, le transfert de connaissances, les engagements de maintenance, les tests de sécurité et les plans de sortie. Les universités et les entreprises technologiques locales peuvent soutenir la recherche appliquée et le développement des compétences, à condition que les partenariats poursuivent des objectifs d'intérêt public clairement définis.

L'écosystème institutionnel congolais souffre d'un écart critique entre l'ambition technologique (IA, architectures cloud) et la disponibilité locale de compétences hautement qualifiées (architectes cloud, data scientists, ingénieurs en cybersécurité, gestionnaires de projets complexes). Sans transferts de compétences massifs, la dépendance vis-à-vis des prestataires internationaux pose un risque pour la souveraineté. L'annonce de la création de l'Académie Congolaise de l'Intelligence Artificielle, destinée à centraliser la recherche appliquée, la formation d'élite et l'incubation de start-ups, répond à cette préoccupation, mais son effectivité reste à documenter.

8.4. Vie privée, cybersécurité et vulnérabilité humanitaire

Les systèmes d'identité numérique, les dossiers médicaux et les dispositifs de protection sociale peuvent traiter des informations hautement sensibles. Dans les contextes de déplacement ou de conflit, une divulgation inappropriée peut avoir des conséquences qui dépassent la simple atteinte à la vie privée. La RDC abrite près de 6,9 millions de déplacés internes, concentrés principalement dans les provinces de l'Est (Nord-Kivu, Sud-Kivu, Ituri, Tanganyika, Haut-Uele, Kasaï), auxquels s'ajoutent plus de 517 000 réfugiés. Cette fragmentation humaine exige des systèmes d'information humanitaires et sanitaires résilients, capables d'assurer la protection des données et de rétablir un accès minimal aux droits fondamentaux.

Une approche fondée sur les droits exige la minimisation des données, la limitation des finalités, des contrôles d'accès, le chiffrement en transit et au repos, des durées de conservation limitées, une capacité de réponse aux incidents, un examen indépendant et des mécanismes de plainte accessibles. Lorsque des données biométriques sont envisagées, les autorités devraient démontrer leur nécessité et leur proportionnalité et évaluer des solutions moins intrusives. L'accès aux services essentiels ne devrait pas

dépendre exclusivement de l'authentification biométrique ou d'une connexion permanente. L'incomplétude du cadre cyber-juridique — notamment en matière de protection des données à caractère personnel, de cybercriminalité et de régulation du commerce électronique — freine l'adoption citoyenne et expose les données des populations vulnérables à des risques de fuites ou d'exploitations malveillantes.

8.5. Confiance, exclusion et responsabilité

Les citoyens peuvent se méfier des services numériques lorsqu'ils ne comprennent pas l'utilisation de leurs données, ne peuvent pas corriger des dossiers inexacts ou ne disposent d'aucun moyen de contester une décision automatisée. La numérisation peut également reproduire les inégalités géographiques, de genre, de handicap, de langue et de revenu. Chaque service majeur devrait maintenir, pendant la transition, une voie d'accès assistée ou non numérique, publier des informations compréhensibles sur la vie privée, prévoir un examen humain des décisions ayant des conséquences importantes et communiquer les volumes de plaintes ainsi que les délais de résolution. La confiance est le résultat d'institutions responsables ; elle ne peut être fournie par la technologie à elle seule. La lutte contre la falsification documentaire doit elle aussi être systémique : elle combine des mécanismes techniques de certification, une politique institutionnelle claire, des procédures de signalement et de sanction, ainsi qu'une formation des agents. Un dispositif purement technologique, sans règles déontologiques ni voies de recours, ne suffit pas à protéger la crédibilité des actes administratifs.

9. Un modèle résilient et inclusif pour la RDC

Cet article propose un modèle d'« **État numérique résilient et fédéré** » composé de six couches qui se renforcent mutuellement, sous-tendu par une couche transversale de gouvernance et de confiance. Il s'agit d'une proposition conceptuelle à évaluer et à adapter, et non de la description d'une architecture nationale déjà déployée.



Figure 5 : Un modèle d'Etat numérique résilient et fédéré pour la RDC

Couche 1 — Services fondamentaux de confiance. Mettre en place une vérification d'identité interopérable, des signatures électroniques lorsqu'elles sont reconnues par le droit, des paiements sécurisés lorsque cela s'applique et une couche d'échange de données. Chaque composant devrait avoir une finalité définie, un responsable de gouvernance, une politique d'accès et un processus d'assurance indépendant. Le RDC-PASS, associé au Répertoire National d'Identification des Personnes Physiques (RNI), constitue la première pierre de cette couche.

Couche 2 — Interopérabilité fédérée. Utiliser des API documentées et versionnées ainsi que des normes de données partagées, tout en laissant aux administrations la responsabilité de leurs systèmes opérationnels. Les échanges de données devraient être autorisés, consignés et limités au strict nécessaire. Il convient d'éviter la création par défaut d'un lac de données universel. Cette approche, inspirée de l'India Stack, de SingPass et de X-Road, permet à toute administration ou entreprise privée autorisée de greffer ses services sur le socle étatique de manière sécurisée.

Couche 3 — Prestation conçue pour fonctionner hors ligne et à faible débit. Concevoir les services prioritaires de manière à permettre l'exécution des tâches essentielles lors d'interruptions de connectivité, la mise en file d'attente sécurisée des transactions et leur synchronisation asynchrone. Utiliser, selon le service et le modèle de menace, les SMS, l'USSD, des interfaces web légères, les codes QR ou des points de service

assistés. Les justificatifs hors ligne doivent comporter des règles claires d'expiration, de révocation et de vérification afin de limiter la fraude.

La vérification des documents administratifs et des titres illustre cette approche. Le calcul d'une empreinte cryptographique (par exemple SHA-256) du document, sa signature avec la clé privée de l'institution émettrice et l'encapsulation de cette signature dans un QR code permettent à un tiers — employeur, administration ou institution partenaire — de vérifier l'authenticité du document à l'aide d'un simple terminal, sans connexion à une base centrale. La validité repose alors sur une preuve cryptographique vérifiable hors ligne, et non sur la disponibilité d'un serveur distant. Ce type de mécanisme ne dispense toutefois pas d'une gouvernance rigoureuse des clés, d'une procédure de révocation et d'une supervision indépendante.

Couche 4 — Infrastructure sécurisée et résiliente. Combiner des choix d'hébergement adaptés aux régions, des sauvegardes chiffrées, une reprise après sinistre testée, une alimentation électrique fiable, une réponse aux incidents et une surveillance de sécurité. La localisation des données doit être évaluée au regard des obligations juridiques, de la résilience opérationnelle, des coûts et de la capacité à entretenir des installations sécurisées ; la localisation, à elle seule, ne garantit ni la souveraineté ni la sécurité. La résilience énergétique constitue un volet à part entière de cette couche. Des équipements locaux à basse consommation, alimentés par des sources solaires et capables de fonctionner en mode dégradé, permettent de maintenir les services essentiels pendant les interruptions. Ces dispositifs doivent être conçus pour se synchroniser par lots vers les nœuds centraux dès le rétablissement de la connectivité, afin de concilier continuité locale et consolidation nationale des données.

Couche 5 — Droits, contrôle et recours. Réaliser des évaluations d'impact sur la vie privée et la cybersécurité avant les déploiements à haut risque ; publier les règles de partage des données ; attribuer une fonction de contrôle indépendante ; prévoir des mécanismes de correction, d'appel et de plainte ; et interdire les usages secondaires sans base légale ni garanties appropriées. Les populations vulnérables devraient participer à la conception des services et à l'évaluation des risques.

Couche 6 — Personnes, institutions et innovation locale. Financer le développement professionnel continu, le leadership technique dans le secteur public, les partenariats de recherche entre universités et pouvoirs publics ainsi que le développement des fournisseurs locaux. Les grands contrats technologiques devraient imposer le transfert de connaissances et le renforcement mesurable des capacités locales. La littératie numérique et l'accès assisté doivent figurer dans les budgets des programmes plutôt que d'être considérés comme de simples activités facultatives de sensibilisation. Les partenariats tripartites (universités – État – écosystème privé) et les

programmes de certification pour les agents de la fonction publique constituent le moteur de cette mutation culturelle.

Couche transversale — Gouvernance et Confiance : L'ensemble est chapeauté par une gouvernance assurant la cohérence, la sécurité et l'éthique. Le principe central du modèle est celui de la **proportionnalité** : normaliser les fonctions qui bénéficient de règles communes, décentraliser la prestation lorsque l'adaptation locale améliore l'accès, et réduire au minimum les données et la connectivité nécessaires à chaque service.

Le modèle peut également être lu comme une chaîne institutionnelle : Processus → Preuves → Données → Pilotage, sous un socle transversal de gouvernance. Le processus désigne l'acte public à maintenir ; la preuve permet d'établir ce qui a été réalisé et sous quelle autorité ; la donnée structure l'information issue de cet acte ; le pilotage mobilise cette information pour décider, contrôler et rendre compte. Cette chaîne, adaptée du cadre HBR-ESR, évite de réduire la dématérialisation au remplacement du papier par un fichier ou une plateforme (LOWEMBO A TSHOTSHO, 2026).

Deux principes complètent cette lecture. Premièrement, la cohérence différée maîtrisée autorise certaines opérations locales pendant une interruption, à condition que leur statut, leur ordre, les conflits éventuels et leur réconciliation ultérieure soient gouvernés et auditables. Deuxièmement, le principe de non-fragmentation exige que la résilience locale ne produise pas de systèmes parallèles incompatibles avec les registres et plateformes de référence. La capacité locale n'a de valeur publique durable que si elle peut se synchroniser, se vérifier et se réconcilier avec l'architecture nationale.

10. Feuille de route de mise en œuvre et indicateurs de suivi

Une feuille de route pratique devrait établir les fondations institutionnelles avant d'accélérer le déploiement. Les jalons suivants sont des recommandations à examiner et ne constituent pas une déclaration d'engagements gouvernementaux déjà pris.



Figure 6 : Feuille de route de mise en œuvre et indicateurs de suivi

Court terme (0 à 12 mois) : établir un inventaire des systèmes numériques publics et des contrats ; repérer les registres redondants et les services prioritaires ; publier des indicateurs de référence ; adopter des normes minimales d'interopérabilité, de cybersécurité, d'accessibilité et de gouvernance des données ; et sélectionner quelques services pour des projets pilotes conçus pour fonctionner hors ligne, dans des contextes urbains, ruraux et touchés par des crises.

Moyen terme (12 à 36 mois) : évaluer les projets pilotes de manière indépendante ; étendre les composants partagés uniquement lorsque leurs avantages et leurs garanties sont démontrés ; introduire des clauses communes de passation des marchés et des exigences de sortie des fournisseurs ; établir un mécanisme de réponse aux incidents à l'échelle de l'administration ; et financer une formation pratique pour les responsables des services, les équipes informatiques et le personnel de première ligne.

Long terme (36 à 48 mois et jusqu'en 2030) : étendre les services dont l'efficacité est démontrée, retirer les plateformes redondantes, renforcer les capacités locales de maintenance et de recherche, et publier les résultats chaque année. L'expansion devrait dépendre de preuves de fiabilité des services, de bénéfices pour les usagers, de sécurité et d'accès équitable, plutôt que du nombre de plateformes lancées.

Un tableau de bord public pourrait suivre : (1) le pourcentage de services prioritaires accessibles par des canaux à faible débit ou assistés ; (2)

les taux d'achèvement et d'échec des services par province et groupe d'usagers ; (3) le temps et le coût médians nécessaires à l'accomplissement de démarches administratives sélectionnées ; (4) la disponibilité et le temps de rétablissement des services critiques ; (5) le pourcentage de systèmes conformes aux normes d'interopérabilité et de sécurité ; (6) les incidents liés aux données et les délais de notification et de remédiation ; (7) les délais de résolution des plaintes et de correction des dossiers ; (8) le coût total de possession et les dépenses de maintenance ; (9) le nombre d'agents locaux formés et maintenus dans les fonctions concernées ; et (10) le pourcentage de documents administratifs critiques émis avec un mécanisme de vérification hors ligne opérationnel, ainsi que le nombre de vérifications réussies par des tiers autorisés. Les indicateurs devraient avoir des définitions publiques, des valeurs de référence, des organismes responsables et, lorsque cela est possible, une vérification indépendante.

11. Dimension économique et cybersécurité

11.1. Retombées économiques attendues

La transformation numérique résiliente génère des gains directs (productivité administrative, réduction du papier et des déplacements), des gains indirects (formalisation, attractivité) et des gains macroéconomiques (PIB, emploi). La réduction de la corruption administrative et l'amélioration du climat des affaires (Guichet Unique) sont des leviers directs.

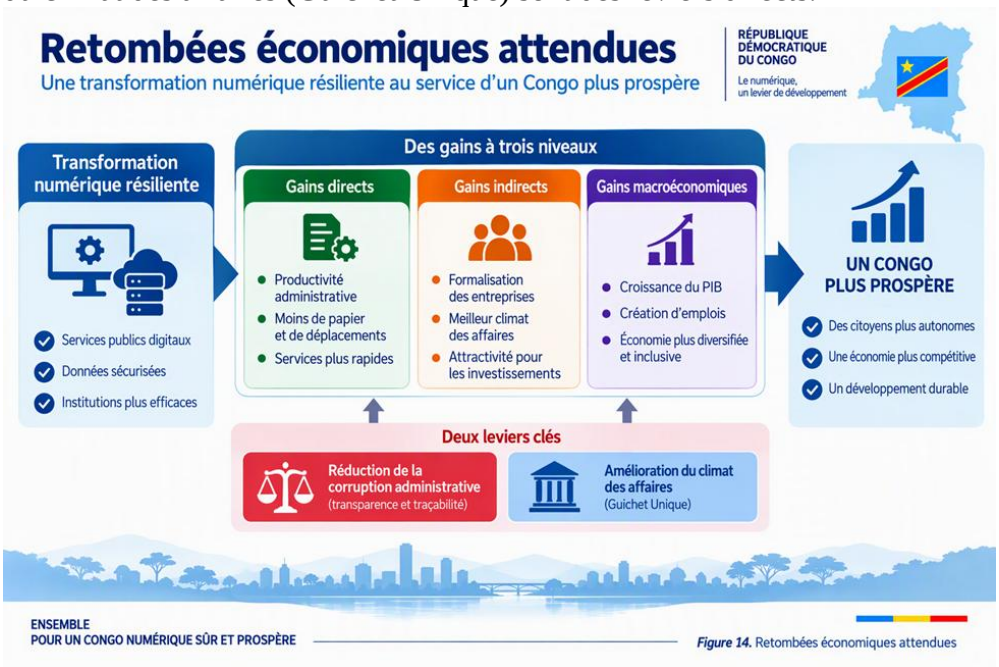

Figure 7 : Une transformation numérique résiliente

11.2. Architecture nationale de cyber-résilience

Pour sécuriser cet écosystème, la RDC doit structurer :

- Un **CERT national** (réponse aux incidents).
- Un **SOC gouvernemental** (surveillance).
- Une **PKI nationale** (infrastructure à clé publique pour la confiance).
- Une **stratégie cloud souverain** (protection des données sensibles).
- La **protection des infrastructures critiques** (data centers, dorsale fibre).



Figure 8 : Une architecture de cyber-résilience

L'actualisation institutionnelle de 2026 impose néanmoins de distinguer trois niveaux : les structures juridiquement créées, leur opérationnalisation administrative et leurs capacités techniques effectivement disponibles. Les informations publiques mentionnent la création de l'Agence nationale de cybersécurité, du Guichet numérique et de l'Agence nationale de certification électronique. Leur existence juridique ne démontre pas encore, à elle seule, la disponibilité opérationnelle d'un CERT national, d'un SOC gouvernemental, d'une infrastructure nationale de gestion des clés ou de mécanismes coordonnés de réponse aux incidents. L'évaluation devrait donc porter sur les mandats, les ressources, les procédures, les exercices réalisés et les résultats observables (Agence Ecofin, 2026).

11.3. Actualisation institutionnelle au second semestre 2026

Au second semestre 2026, la transformation numérique congolaise est entrée dans une phase davantage opérationnelle mais toujours progressive. Après le lancement officiel de RDC-PASS le 13 juin 2026, la Présidence a explicitement présenté son déploiement comme graduel. En septembre 2026, des informations publiques faisaient état d'une première phase de formation d'agents d'enregistrement, tandis que la Politique sectorielle de l'économie numérique et la Stratégie nationale de l'intelligence artificielle figuraient parmi les orientations validées. Ces éléments invitent à distinguer, dans l'évaluation des politiques numériques, la validation stratégique, l'activation d'une infrastructure, l'enrôlement effectif des usagers et la disponibilité mesurable des services à l'échelle provinciale (Présidence de la République démocratique du Congo, 2026 ; Agence Ecofin, 2026).

12. Discussion

L’analyse suggère que le principal défi n'est pas le manque d'ambitions numériques, mais la transformation de ces ambitions en services qui fonctionnent dans des conditions locales diverses. L'IPN peut réduire les doublons et accélérer le développement des services, mais elle peut aussi amplifier les défaillances si les systèmes fondamentaux sont mal gouvernés. Une coordination centrale est nécessaire pour les normes et les capacités partagées, tandis qu'une flexibilité locale est indispensable à la prestation dans des territoires où les langues, la connectivité, l'électricité et les capacités administratives diffèrent.

Le cas de la RDC invite également à nuancer les récits optimistes sur le saut technologique. Sauter certaines étapes d'infrastructure peut être avantageux, mais sauter le développement institutionnel ne l'est pas. Un service conçu d'abord pour le mobile n'est pas inclusif simplement parce que les téléphones mobiles sont répandus : les usagers ont toujours besoin d'une connectivité abordable, d'interfaces accessibles, d'une authentification digne de confiance, d'une alimentation électrique fiable et de recours lorsque le système échoue. De même, la souveraineté numérique ne doit pas être réduite à l'hébergement des données à l'intérieur des frontières nationales. Elle exige aussi la capacité de définir les politiques, d'auditer les systèmes, de négocier les contrats, d'entretenir les infrastructures et de changer de fournisseur sans perdre le contrôle des fonctions publiques.

Cette conception de la souveraineté a une traduction concrète : elle se mesure à la capacité de l'État à maintenir ses services essentiels lorsque le réseau, l'énergie ou un fournisseur font défaut. Un système qui ne fonctionne que dans des conditions optimales de connectivité transfère de fait une partie de la souveraineté aux opérateurs techniques et aux aléas infrastructurels. À l'inverse, des services conçus pour fonctionner hors ligne, avec des données

maîtrisées localement et des mécanismes de vérification autonomes, renforcent la continuité de l'État et la confiance des usagers.

La trajectoire congolaise offre ainsi un cas d'étude pour les théories du développement et de la gouvernance numérique dans les économies post-conflit à grande échelle. Elle démontre que le succès du leapfrogging technologique dépend d'une ingénierie institutionnelle et sociale rigoureuse.
Trois leviers opérationnels se dégagent :
Un quatrième levier consiste à construire une administration hybride de proximité. Les points de service physiques, les bureaux postaux lorsque leur capacité le permet, les centres numériques assistés et les dispositifs mobiles peuvent compléter les plateformes en ligne. Cette combinaison réduit le risque que la dématérialisation transforme les contraintes de connectivité, de handicap, de langue ou de littératie en exclusion administrative.

1. déployer une infrastructure publique numérique modulaire, en dépassant la simple numérisation de documents pour concevoir une véritable architecture de plateforme ;
2. standardiser le modèle « low-tech / haut impact », avec des applications offline-first, une résilience adaptée aux contextes à faible connectivité et des centres physiques d'assistance numérique pour inclure les populations non connectées ou analphabètes ;
3. opérer une mise à niveau massive des compétences publiques, via des filières d'excellence et des programmes de certification obligatoires pour les agents de la fonction publique.



Figure 9 : La trajectoire congolaise de leapfrogging technologique

Les limites des éléments de preuve de cet article sont importantes. Il repose sur des sources secondaires et des annonces officielles ; il ne réalise pas d'audit indépendant des marchés publics, ne vérifie pas les dépenses des programmes, ne mesure pas la connectivité sur le terrain et ne mène pas d'entretiens auprès des usagers. Le modèle proposé constitue donc un cadre de mise en œuvre et de validation empirique, et non l'affirmation que les réformes identifiées ont déjà produit des résultats mesurables. Les recherches futures devraient comparer certains services dans plusieurs provinces, examiner les parcours et les coûts pour les usagers, évaluer l'application des garanties de protection des données et comparer des projets pilotes hors ligne aux services conventionnels exclusivement en ligne.

Une limite conceptuelle supplémentaire concerne l'IMENR-RDC : ses niveaux et dimensions n'ont pas encore fait l'objet d'une validation empirique, d'une pondération statistique ni d'un test inter-évaluateurs. Une prochaine étape devrait opérationnaliser les variables, documenter les sources de données, tester l'indice dans plusieurs provinces et comparer ses résultats à des cadres internationaux. De même, la cohérence différée maîtrisée, la vérification hors ligne et le principe de non-fragmentation doivent être testés sur des processus publics clairement délimités avant toute généralisation.

Conclusion

La RDC a l'occasion d'utiliser les technologies numériques pour améliorer l'administration publique, élargir l'accès aux services et renforcer la coordination institutionnelle. Cette opportunité ne se concrétisera pas par les seuls investissements dans les infrastructures ou par l'identité numérique. Elle dépend de l'interaction entre une connectivité fiable, des systèmes interopérables, des institutions responsables, des équipes locales qualifiées, des garanties de protection de la vie privée et de cybersécurité, ainsi que des canaux de prestation qui restent utilisables lorsque les réseaux ou l'électricité sont interrompus. Dans les États caractérisés par une faible connectivité, une forte dispersion territoriale et des contraintes institutionnelles persistantes, la résilience doit devenir le principe fondateur de toute architecture numérique publique.

La performance d'un État numérique résilient devrait être mesurée à l'aune de ce que les citoyens peuvent accomplir de manière fiable et sûre, et non des annonces, des applications ou des montants d'investissement. Une approche fédérée, capable de fonctionner hors ligne et centrée sur les droits offre à la RDC une voie plausible vers la transformation numérique, tout en réduisant le risque que les inégalités territoriales et sociales existantes soient inscrites dans les systèmes publics. Pour les pays confrontés à des contraintes comparables, la leçon plus générale est qu'un saut technologique durable

exige que les capacités institutionnelles et la confiance du public progressent en même temps que la technologie.

En conjuguant investissements annoncés, volonté de souveraineté et inclusion des populations les plus vulnérables, la RDC est en mesure de transformer son immensité géographique en avantage stratégique et de devenir un laboratoire d'innovation pour l'Afrique subsaharienne.

La trajectoire numérique de la RDC ne doit pas être évaluée à travers le volume des investissements ou le nombre d'applications déployées, mais selon un triptyque fondamental : **continuité du service public, confiance citoyenne et souveraineté opérationnelle**. Un État devient véritablement numérique lorsqu'il demeure capable de servir ses citoyens même en situation de crise, d'isolement territorial ou de rupture technologique. En érigeant la résilience en principe de conception (« Governance Resilience by Design »), la RDC peut transformer son immensité géographique en avantage stratégique et inspirer d'autres nations du Sud global confrontées aux mêmes défis.

Conflit d'intérêts : L'auteur a déclaré n'avoir aucun conflit d'intérêts.

Disponibilité des données : Toutes les données figurent dans le corps de l'article.

Déclaration de financement : L'auteur n'a bénéficié d'aucun financement pour cette recherche.

References:

1. Agence Ecofin. (2026, 30 septembre). RDC : stratégies, identité numérique et cybersécurité au bilan d'un an de réformes. https://www.agenceecofin.com/actualites-numerique/3009-142019-rdc-strategies-identite-numerique-et-cybersecurite-au-bilan-d-un-an-de-reformes
2. Banque mondiale. (2016). World development report 2016: Digital dividends. World Bank. https://doi.org/10.1596/978-1-4648-0671-1
3. Banque mondiale. (2026, 28 mai). DRC Digital Transformation Project (P180495): Implementation Status & Results Report, Sequence No. 4. World Bank.
4. Banque mondiale. (2024). Democratic Republic of Congo digital transformation project (P180495). World Bank.
5. Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New public management is dead—Long live digital-era governance. Journal of Public Administration Research and Theory, 16(3), 467–494. https://doi.org/10.1093/jopart/mui057

6. GSMA. (2025, September 18). Digital reforms could connect 9.7 million more Congolese and add CDF 9.8 trillion to GDP by 2029 in DRC, GSMA report reveals. https://www.gsma.com/newsroom/press-release/digital-reforms-could-connect-9-7-million-more-congolese-and-add-cdf-9-8-trillion-to-gdp-by-2029-in-drc-gsma-report-reveals/
7. LOWEMBO A TSHOTSHO, R. A. (2026). Gouvernance numérique, assurance qualité et dématérialisation dans l'ESR en RDC : HBR-ESR, inclusion numérique, souveraineté des données et continuité des preuves académiques. Communication, États généraux de l'enseignement supérieur et de la recherche au Cambodge, Phnom Penh, Cambodge.
8. Présidence de la République démocratique du Congo. (2026, 13 juin). Le Président Félix Tshisekedi lance « RDC-PASS », l'identité numérique unique pour chaque Congolais. https://www.presidence.cd/actualite-detail/actualite/le_president_felix_tshisekedi_lance_rdc_pass_lidentite_numerique_unique_pour_chaque_congolais
9. République démocratique du Congo. (2023). Ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique.
10. United Nations Department of Economic and Social Affairs. (2024). United Nations e-government survey 2024: Accelerating digital transformation for sustainable development. United Nations. https://publicadministration.un.org/egovkb/Reports/UN-E-Government-Survey-2024
11. World Bank Group. (2025). Digital public infrastructure and development: A World Bank Group approach. World Bank.