

# L'injustice numérique des données de l'Afrique : un cri silencieux

## Avant-propos

Je suis parti à la rencontre des terres africaines, des dunes du Sahara aux forêts tropicales du Congo, des grands lacs de l'Est aux rivages de l'Atlantique. J'ai traversé plus de cinquante aéroports sur tous les continents, observant inlassablement la même mécanique invisible : le scan furtif des passeports et des visages, la capture biométrique – et, derrière, le transfert immédiat de ces données vers des serveurs européens ou américains.

En tant que sociologue, criminologue et médecin naturopathe, mais aussi conférencier et entrepreneur, je ne peux taire mon indignation. Jamais je n'ai vu nos autorités africaines s'émouvoir, ni nos gouvernements adresser la moindre question publique sur ce pillage de nos identités. Ce silence est d'autant plus assourdissant qu'il s'apparente à l'aveuglement prétentieux d'États qui ferment les yeux devant une guerre numérique larvée.

On parle de progrès, d'efficacité et de sécurité, alors qu'une partie de la population africaine – la majorité – voit ses données personnelles devenir la monnaie d'échange d'intérêts étrangers. Ces vols sournois, à peine dissimulés derrière des accords opaques, dessinent une « futile guerre » où nos nations sont à la fois cibles et otages.

Cet article se veut un cri d'alerte. Nous dresserons la cartographie des flux, dévoilerons les acteurs de ce nouveau colonialisme numérique et proposerons des pistes pour que l'Afrique reprenne enfin le contrôle de ses données. Parce que le silence des puissants africains ne doit plus être la caution de l'injustice.

## Introduction

À l'heure où chaque empreinte digitale et chaque balayage de passeport deviennent autant de pièces d'un gigantesque puzzle global, l'Afrique demeure spectatrice d'un pillage silencieux. Les données biométriques et personnelles recueillies sur son sol – depuis les aéroports jusqu'aux cliniques – s'évaporent hors de tout contrôle, stockées et exploitées par des géants européens ou américains.

Ce phénomène soulève une question cruciale : comment un continent riche de cultures et d'innovations peut-il laisser ses informations intimes se muer en actifs de puissances étrangères ?

Derrière les écrans et les flux TCP/IP, l'Afrique est aujourd'hui confrontée à une forme moderne de colonialisme. Les autoroutes numériques, censées faire avancer le progrès, sont détournées pour servir les intérêts de sociétés offshore. *Ce n'est pas une fatalité : comprendre l'injustice numérique, c'est déjà amorcer la voie d'une revanche technologique et souveraine.*

## Déploiement de la "pipeline" des données maghrébines vers l'Occident

Cette révélation met en lumière un maillage discret mais structuré entre les administrations maghrébines et leurs partenaires occidentaux : les fichiers biométriques, historiques de

navigation, géolocalisations et données de réseaux sociaux récoltés aux frontières ou via des accords de surveillance sont régulièrement transférés vers des serveurs hébergés en Europe et aux États-Unis. Sous couvert de coopération sécuritaire et de lutte contre la migration irrégulière, ces flux alimentent des plateformes de renseignement et de profilage destinées à anticiper les trajectoires migratoires, à contrôler les mouvements de populations et parfois à orienter les politiques d'asile.

Ce processus, encouragé par des financements conditionnels et soutenu par des entreprises technologiques occidentales, crée une asymétrie lourde de conséquences : les ressortissants sub-sahariens se retrouvent ainsi soumis à un traitement de données massives dont ils n'ont ni connaissance ni recours effectif.

En filigrane, c'est tout un pan de la souveraineté numérique africaine qui se joue, transférant le pouvoir de décision sur les parcours migratoires depuis les pays d'origine vers des commanditaires extérieurs.

## **1. Le pillage invisible des données**

La digitalisation de l'administration et des services publics africains a multiplié les points de collecte de données :

- Passeports scannés et photos biométriques aux contrôles frontaliers
- Dossiers médicaux électroniques synchronisés avec des cloud étrangers
- Transactions mobiles et historiques de navigation sur les réseaux 3G/4G

2

---

Ces données, originellement destinées à fluidifier le voyage, améliorer la prise en charge médicale ou suivre des paiements, sont détournées : stockées sur des serveurs hors du continent, analysées pour des finalités commerciales, revendue à l'envi. L'impact est, pour l'Afrique, doublement cruel : perte de souveraineté et absence de retombées économiques locales.

## **2. Mécanismes et acteurs du détournement**

Trois leviers principaux orchestrent ce transfert massif de données :

### **1. Contrats opaques**

- Clauses de localisation absentes
- Aucune obligation de réversibilité ou de transfert de compétences

### **2. Infrastructures externalisées**

- Centres de données installés en Europe ou aux États-Unis
- Usage de services « cloud » publics sans alternative locale

### **3. Interopérabilité unilatérale**

- API propriétaires imposées
- Formats de données standards mais privatisés

Ces jeux d'acteurs – multinationales du numérique, cabinets de conseil internationaux, prestataires de services biométriques – composent un écosystème qui tire profit d'un vide réglementaire et technique.

### 3. Conséquences structurelles

L'injustice numérique ne se limite pas à des fuites : elle façonne un rapport de force géopolitique et économique.

- Perte de souveraineté : incapacité à contrôler qui accède aux données, comment elles sont traitées, stockées, vendues.
- Disparité économique : absence de valorisation locale des données empêche la naissance d'une industrie africaine du big data.
- Risques sécuritaires : serveurs offshore sont plus vulnérables aux cyberattaques ciblant des informations stratégiques (identité, santé, profil de risque).

### 4. Études de cas emblématiques

| Cas                                | Flux de données             | Prestataire                    | Impact pour l'Afrique                        |
|------------------------------------|-----------------------------|--------------------------------|--|
| Contrôle biométrique – Sénégal     | Passeports + empreintes     | Leader européen de la sécurité | Serveurs en France : pas de traitement local |
| Dossiers médicaux – Afrique du Sud | DME hospitaliers            | Plateforme cloud américaine    | Analyses génomiques hébergées aux USA        |
| Portail d'e-immigration – Kenya    | Données de voyage + e-visas | Société américaine de tech     | Algorithmes propriétaires sans audits locaux |

3

Ces exemples montrent que, loin d'être des cas isolés, les pratiques de transfert de données hors du continent sont devenues la règle.

### 5. Racines historiques et résonances coloniales

La « colonisation numérique » s'inscrit dans une longue histoire :

- Au XIX<sup>e</sup> siècle, l'Afrique était cartographiée sans qu'on lui demande son avis.
- Aujourd'hui, ses données sont exploitées sans qu'elle puisse décider de leurs usages.

Ce parallèle n'est pas une simple métaphore : il révèle la continuité d'un rapport de domination, où l'infrastructure technique remplace les compagnies coloniales. L'ordinateur devient le nouveau comptoir, l'API le nouveau traité inégal.

## 6. Les barrières structurelles en Afrique

Plusieurs freins empêchent la mise en place d'une vraie souveraineté numérique :

- **Infrastructures** : rares sont les centres de données de classe mondiale, les liaisons fibre optique continentales ou les réseaux 5G robustes.
- **Cadre légal** : législations protégeant la vie privée souvent incomplètes, absence de régulateurs indépendants avec des moyens d'investigation.
- **Compétences** : fuite des talents (« brain drain »), manque de formation pointue en cybersécurité, data science ou gestion de cloud souverain.

## 7. Scénarios prospectifs

| Scénario   | Description   | Probabilité | Impact                                 |
|------------|---|-------------|--|
| Pessimiste | Maintien du statu quo, renforcement du modèle offshore                  | Élevée      | Souveraineté numérique toujours faible |
| Réaliste   | Adoption progressive de lois plus strictes et d'infrastructures locales | Moyenne     | Émergence lente d'une industrie locale |
| Optimiste  | Consortium panafricain pour un cloud souverain et standards ouverts     | Faible      | Indépendance et retombées économiques  |

4

## 8. Stratégies de riposte

### 1. Légiférer et réguler

- Obligation de localisation des données critiques
- Création d'autorités indépendantes de protection des données

### 2. Investir dans l'infrastructure

- Centres de données africains certifiés
- Câbles sous-marins et interconnexions régionales

### 3. Stimuler l'écosystème local

- Incubateurs et fonds d'investissement dédiés à la e-santé, la fintech, l'agritech
- Partenariats avec des acteurs open source (OpenMRS, FHIR)

### 4. Former et retenir les talents

- Programmes universitaires en cybersécurité et data science
- Incentives pour la recherche appliquée et les start-ups

# Les conséquences multidimensionnelles de la collecte massive de données en Afrique

## 1. Atteinte à la souveraineté et au pouvoir décisionnel

- Perte de contrôle sur les lois et règlements : l'externalisation systématique des serveurs prive les États africains de leur pouvoir de légiférer et de faire appliquer des standards de protection adaptés à leurs réalités.
- Sentiment d'impuissance institutionnelle : face à des contrats opaques, les gouvernements demeurent spectateurs, sans réelle marge de manœuvre pour renégocier ou rediriger l'exploitation de ces données.

## 2. Risques économiques et compétitifs

- Absence de retombées financières locales : les modèles d'affaires des prestataires offshore captent la valeur ajoutée, sans redistribution ni co-investissement dans l'écosystème numérique africain.
- Frein à l'émergence de champions technologiques africains : verrouillage des API et des plateformes privatives empêchent la création de start-ups locales capables d'innover sur ces mêmes données.

## 3. Menaces sécuritaires et d'espionnage

- Vulnérabilité accrue aux cyberattaques : des serveurs concentrés en Europe ou aux États-Unis peuvent devenir des cibles de piratage, exposant des millions de profils africains.
- Usage détourné à des fins géopolitiques : exploitation des données biométriques et de déplacement pour profiler des leaders d'opinion, repérer des dissidents ou orienter des stratégies d'influence.

## 4. Atteintes aux droits individuels et collectifs

- Profilage et discrimination : algorithmes décisionnels peuvent catégoriser les citoyens selon leur origine, leur santé ou leurs habitudes de voyage, sans transparence ni recours.
- Érosion de la confiance : le sentiment d'être constamment « scruté » engendre une défiance vis-à-vis des services publics et des innovations numériques, freine l'adoption d'e-administrations et de e-santé.

## 5. Impacts psychosociaux et culturels

- Sentiment de dépossession identitaire : la migration de données personnelles vers des entités étrangères renforce l'idée d'une « double peine » post-coloniale, où l'intimité même devient patrimoine extérieur.
- Fragmentation du tissu social : la crainte d'une surveillance généralisée peut dissuader la participation citoyenne, limiter les espaces d'expression et affaiblir la cohésion communautaire.

## 6. Conséquences pour la santé publique et la recherche

- Accès inégal aux innovations médicales : absence de consortiums africains de données de santé freine les avancées locales en épidémiologie, en pharmacogénomique et en médecine préventive.
- Biais de représentativité : les jeux de données centrés sur les populations européennes ou américaines conduisent à des diagnostics erronés et à des traitements mal adaptés aux spécificités génétiques africaines.

Reprendre le contrôle de ces données n'est pas qu'une question technique : c'est un enjeu de justice, d'équité et de dignité. Dans le prochain chapitre, nous détaillerons les mécanismes de riposte – juridiques, technologiques et sociétaux – pour transformer cette injustice numérique en levier d'émancipation et d'innovation pour l'Afrique.

### Exemples récents de vol de données en Afrique

Voici quelques cas emblématiques illustrant l'ampleur du pillage silencieux des données sur le continent :

- Piratage de l'ARTP (Autorité de régulation des télécommunications et des postes) au Sénégal par le groupe Karakurta. 150 Go de données personnelles, incluant des informations de télécommunications et des documents d'identification, ont été exposés et partiellement divulgués en ligne.
- Extorsion des données de la banque BOA au Mali. En échange d'un paiement de 10 M\$ (plus de 6 129 000 000 FCFA), les hackers menaçaient de rendre publiques les informations personnelles et financières de milliers de clients.
- Fuite de 50 Go de dossiers militaires ivoiriens, comprenant numéros de matricule, extraits de naissance et conversations internes sensibles de l'armée de Côte d'Ivoire. Ces données ont été diffusées sans aucun contrôle étatique préalable, illustrant une attaque aux motivations probablement géopolitiques.
- Violation massive chez Experian en Afrique du Sud, où 24 millions de profils de consommateurs (noms, adresses, numéros d'identification) ont été frauduleusement extraits pour donner suite à une demande illégitime d'un individu prétendant représenter un client légitime.
- Intrusion interne à la Postbank sud-africaine, contraignant la banque à remplacer 12 millions de cartes bancaires après qu'un passe-partout ait été copié et utilisé pour compromettre les données des titulaires de compte.
- Compromission des données clients de Nedbank via ingénierie sociale ciblant un prestataire tiers en charge de l'envoi de SMS et messages WhatsApp. Près de 1,7 million de profils (noms, adresses, numéros de téléphone) ont été affectés, exposant les clients à des tentatives de phishing et d'usurpation d'identité

## Pistes pour que l'Afrique reprenne le contrôle de ses données

### 1. Consolider les cadres réglementaires

- Adopter et ratifier massivement la Convention de Malabo pour créer une base légale commune à l'échelle de l'UA.
- Transposer les principes clés du RGPD (finalités limitées, consentement éclairé, portabilité) dans chaque loi nationale.
- Renforcer les autorités de protection des données (APD) : indépendance budgétaire, pouvoirs d'audit et de sanction, permanence des effectifs.

### 2. Mettre en place une infrastructure souveraine

- Déployer un réseau de centres de données régionaux certifiés ISO 27001, gérés par des consortiums publics-privés africains.
- Construire ou mutualiser des « zones cloud souveraines » pour les secteurs critiques (santé, passeports, finances).
- Encourager l'implantation de câbles sous-marins et de dorsales nationales pour améliorer la latence et l'autonomie.

### 3. Favoriser l'écosystème technologique local

- Soutenir les start-ups africaines de cyber-sécurité, de blockchain et de data science via des incubateurs et fonds dédiés.
- Promouvoir les logiciels open source (OpenMRS, FHIR, Linux) pour éviter le verrouillage propriétaire.
- Organiser des hackathons et concours régionaux pour résoudre des cas concrets de souveraineté des données.

### 4. Développer les compétences et la recherche

- Intégrer la protection des données et la cybersécurité dans les cursus universitaires et les écoles d'ingénieurs.
- Mettre en place des centres de recherche appliquée (Big Data, IA éthique) en partenariat avec les universités africaines et la diaspora scientifique.
- Créer des programmes de certification et de mentorat pour retenir les talents sur le continent.

### 5. Instaurer des mécanismes de gouvernance et de transparence

| Action  | Objectif  | Bénéfices clés                           |
|---|---|--|
| Chartes de gouvernance multi-acteurs          | Impliquer États, privés, ONG et citoyens        | Décision partagée, meilleure acceptation |
| Portails publics de suivi des flux de données | Visualiser où et comment circulent les données  | Traçabilité, responsabilisation          |
| Audits réguliers et rapports publics          | Vérifier la conformité et publier les résultats | Confiance citoyenne, pression positive   |

## 6. Encourager les partenariats équitables

- Inscrire dans les contrats de prestation des clauses de localisation des données et de transfert de savoir-faire.
- Prévoir des mécanismes de réversibilité afin que les États africains puissent rapatrier leurs données à tout moment.
- Lancer des projets pilotes co-financés (50 % public – 50 % privé) pour tester des architectures souveraines avant mise à l'échelle.

## 7. Sensibiliser et responsabiliser les citoyens

- Mener des campagnes d'éducation aux droits numériques dans les administrations, écoles et médias.
- Déployer des tableaux de bord grand public indiquant l'usage des données collectées (par ex. : dans les aéroports).
- Promouvoir des applications de consentement granulaire pour que chaque voyageur ou patient sache précisément à quoi servent ses données.

## Impact des injustices numériques sur les communautés africaines

Les injustices numériques se traduisent par une marginalisation croissante des populations qui n'ont pas accès ou peu accès aux technologies de l'information et de la communication. Cette fracture numérique exacerbe les inégalités préexistantes en termes d'éducation, d'emploi, de genre et de participation citoyenne.

8

---

### Fracture d'accès à l'Internet et marginalisation

En 2023, seulement 37 % de la population africaine disposait d'une connexion Internet, limitant l'accès à l'information et aux services en ligne pour la majorité des Africains.

Dans de nombreuses régions, les infrastructures restent insuffisantes et les coûts trop élevés pour les foyers les plus vulnérables.

### Entrave à l'éducation

*La privation d'accès aux plateformes numériques entraîne des conséquences directes sur l'apprentissage :*

Pendant la pandémie, un tiers des enfants dans le monde n'a pas pu suivre l'enseignement à distance.

En Afrique subsaharienne, 49 % des élèves ont été privés d'éducation en ligne lors des fermetures d'écoles en 2020, contre 40 % en Afrique du Nord et au Moyen-Orient.

### Frein au développement économique

*L'exclusion numérique réduit sensiblement les opportunités économiques :*

Une augmentation de 10 % de la couverture haut débit pourrait accroître le PIB des pays en développement de 0,5 % à 1,5 % en moyenne, selon la Banque mondiale.

Les petites et moyennes entreprises peinent à exploiter les marchés en ligne et à bénéficier de la digitalisation des chaînes de valeur.

### **Amplification des disparités de genre**

*Les femmes et les jeunes filles subissent une double peine :*

Elles sont souvent les premières exclues des programmes de formation numérique et de la distribution d'équipements, renforçant un fossé déjà pénalisant pour leur insertion professionnelle et sociale.

Dans de nombreux foyers, les stéréotypes culturels limitent encore leur accès aux outils et à la formation technologique.

### **Atteintes à la cohésion sociale et à la souveraineté numérique**

*L'injustice numérique se traduit aussi par :*

Une perte de souveraineté : transfert massif de données personnelles et biométriques vers des serveurs étrangers sans contrôle local.

Un profilage et un contrôle renforcés des mouvements migratoires, dont sont souvent victimes des communautés déjà fragilisées.

Un affaiblissement du tissu social : sentiment d'exclusion, méfiance accrue envers les institutions et montée des tensions communautaires. En somme, les injustices numériques profondes qui touchent l'Afrique ont un impact multiforme, allant de l'école à l'économie, en passant par les droits fondamentaux et la cohésion sociale.

Pour y remédier, il est crucial de renforcer les infrastructures, de garantir l'accès universel et abordable à l'Internet, de promouvoir des formations inclusives et de remettre la maîtrise des données entre les mains des acteurs locaux.

## **Conclusion**

### **Il est savoir que**

L'injustice numérique dont souffre l'Afrique n'est pas une fatalité. Elle est le produit de choix technologiques et politiques qu'il est encore possible de renverser. Reprendre le contrôle des données, c'est se donner les clés d'une croissance souveraine, d'une sécurité renforcée et d'une créativité region-centrée. Le temps est venu d'écrire une nouvelle page de l'histoire numérique africaine : celle de la revanche et de la renaissance

Reprendre le contrôle des données n'est pas un luxe, c'est la condition d'une souveraineté politique, d'une sécurité accrue et d'un développement économique endogène. En combinant législation solide, infrastructures souveraines, montée en compétences et gouvernance transparente, l'Afrique peut transformer cette « guerre des données » en levier d'émancipation et d'innovation.

**Dr Alpha Grace, PhD**

**Sociocriminologue**