



Académie Internationale de Droit du Numérique

ATELIER 9

INFRASTRUCTURES NUMÉRIQUES

ABIDJAN (COTE D'IVOIRE) – 17 AU 21 AOUT 2026

www.julienhounkpe.info



PRÉSENTATION DE L'INTERVENANT

- Expert Consultant en Droit du Numérique
- Enseignant Chercheur à l'Université d'Abomey-Calavi (Bénin)
- Ancien conseiller Technique Juridique du Président de l'Assemblée Nationale
- Auteur de : **Technology Law in Benin**, International Encyclopaedia of Laws Series, Wolters Kluwer, 2023



JULIEN HOUNKPE
— DOCTEUR EN DROIT —

POURQUOI CE MODULE, POUR QUI, ET COMMENT ?



Pourquoi ce module ?

Le droit du numérique s'écrit de plus en plus souvent au niveau de l'infrastructure elle-même (câble, cloud, datacenter) et non plus seulement au niveau du fichier ou du contrat.



Public cible

Juristes, magistrats, régulateurs et décideurs publics amenés à encadrer, négocier ou contrôler des infrastructures numériques.

POURQUOI CE MODULE, POUR QUI, ET COMMENT ?



Objectifs pédagogiques

Donner une grille de lecture juridique commune des infrastructures numériques, de leurs composantes à leur régulation.



Compétences visées

Identifier une infrastructure numérique, situer le cadre juridique applicable, et dialoguer avec un régulateur ou un opérateur technique.



Méthodologie

Approche notionnelle et structurée : définitions, cartographie des normes, étude des acteurs et des mécanismes, mise en perspective avec l'IA.

INTRODUCTION GÉNÉRALE

DE LA RÉVOLUTION INDUSTRIELLE À LA RÉVOLUTION NUMÉRIQUE

HIER — ÈRE INDUSTRIELLE

ROUTE · RAIL · ÉLECTRICITÉ

Chaque révolution économique s'est construite sur une infrastructure nouvelle et sur la ressource qu'elle permettait de faire circuler.



AUJOURD'HUI — ÈRE NUMÉRIQUE

RÉSEAU · CLOUD · DONNÉE

Ce que le pétrole ou l'électricité ont été pour l'industrie, la donnée et sa capacité de circulation le sont pour l'économie numérique.

DE LA RÉVOLUTION INDUSTRIELLE À LA RÉVOLUTION NUMÉRIQUE

Le juriste face à l'infrastructure :

on ne peut plus raisonner le droit du numérique en ignorant le support technique qui le rend, ou non, effectif.

Un nouveau champ du droit :

les infrastructures numériques deviennent un objet juridique à part entière, à la croisée du droit des télécommunications, du droit économique et du droit public.

Plan

- 01 Fondements conceptuels
- 02 Cadre juridique
- 03 Gouvernance et régulation
- 04 Cybersécurité et confiance
- 05 Intelligence artificielle

CINQ NOTIONS À DISTINGUER

01

**Infrastructure**

Ensemble des installations et services de base nécessaires au fonctionnement d'un système ou d'une société.

02

**Infrastructure critique**

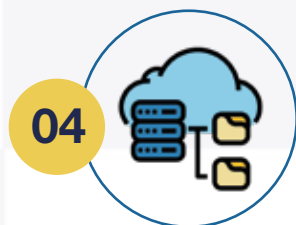
Infrastructure dont l'arrêt compromettrait gravement la sécurité, l'économie ou la santé publique.

03

**Infrastructure numérique**

Équipements, réseaux et services techniques qui permettent la production, le stockage et la circulation des données.

CINQ NOTIONS À DISTINGUER

**Infrastructure essentielle**

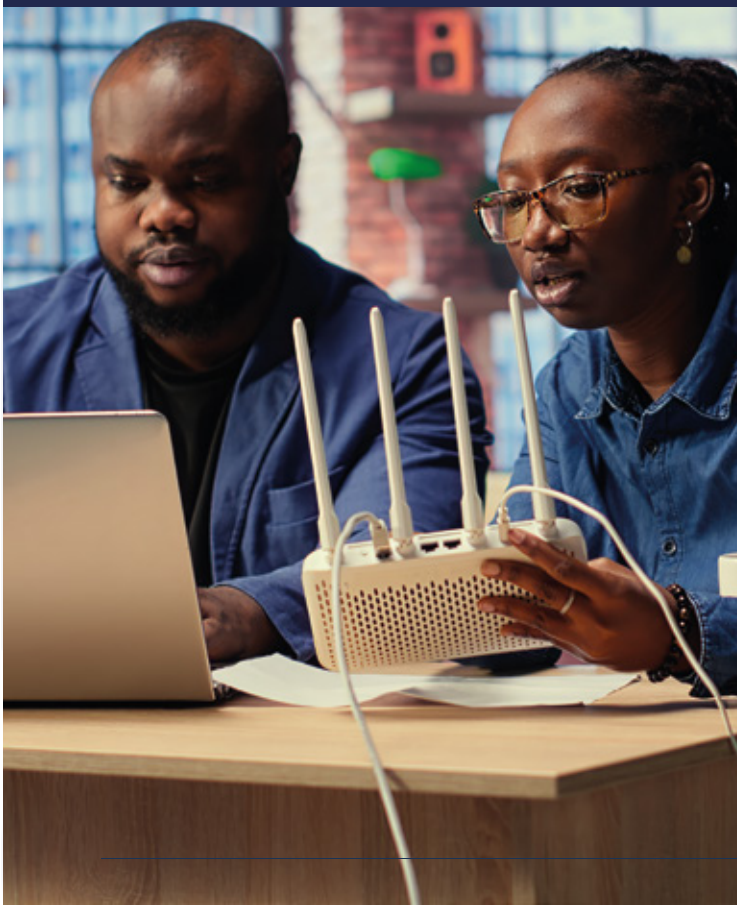
Infrastructure indispensable à un service reconnu vital pour la collectivité — catégorie souvent définie par le droit national.

**Écosystème numérique**

Ensemble interdépendant d'acteurs, de technologies et de règles qui organisent l'usage du numérique dans un espace donné.

Ces catégories se recoupent souvent dans les textes. Elles ne sont pas toujours distinguées avec la même rigueur d'un cadre juridique à l'autre.

DE QUOI UNE INFRASTRUCTURE NUMÉRIQUE EST-ELLE FAITE ?



Réseaux

Dorsales de transmission
qui font circuler les données.



Fibre optique

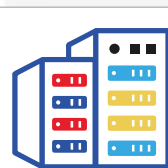
Support physique de très haut débit,
colonne vertébrale du transport de données.



Satellites

Connectivité complémentaire,
précieuse pour les zones enclavées.

DE QUOI UNE INFRASTRUCTURE NUMÉRIQUE EST-ELLE FAITE ?



Data centers

Sites d'hébergement physique des serveurs et des données.



Cloud

Mise à disposition élastique et à distance de ressources informatiques.



Internet Exchange Points

Points d'échange qui interconnectent localement les réseaux, réduisant coûts et latence.

DE QUOI UNE INFRASTRUCTURE NUMÉRIQUE EST-ELLE FAITE ?



DNS

Système d'annuaire qui traduit noms de domaine et adresses réseau.



CDN

Réseau de diffusion de contenu qui rapproche le contenu de l'utilisateur final.



Services de confiance

Authentification, signature, horodatage — la couche qui sécurise les échanges.

CE QUI QUALIFIE JURIDIQUEMENT UNE INFRASTRUCTURE NUMÉRIQUE

01 Interconnexion

Capacité des réseaux à se relier entre eux pour former un système continu.

02 Interopérabilité

Capacité des systèmes à fonctionner ensemble malgré des origines techniques différentes.

03 Résilience

Capacité à maintenir le service en cas de défaillance, d'attaque ou de choc externe.



CE QUI QUALIFIE JURIDIQUEMENT UNE INFRASTRUCTURE NUMÉRIQUE

04 Disponibilité

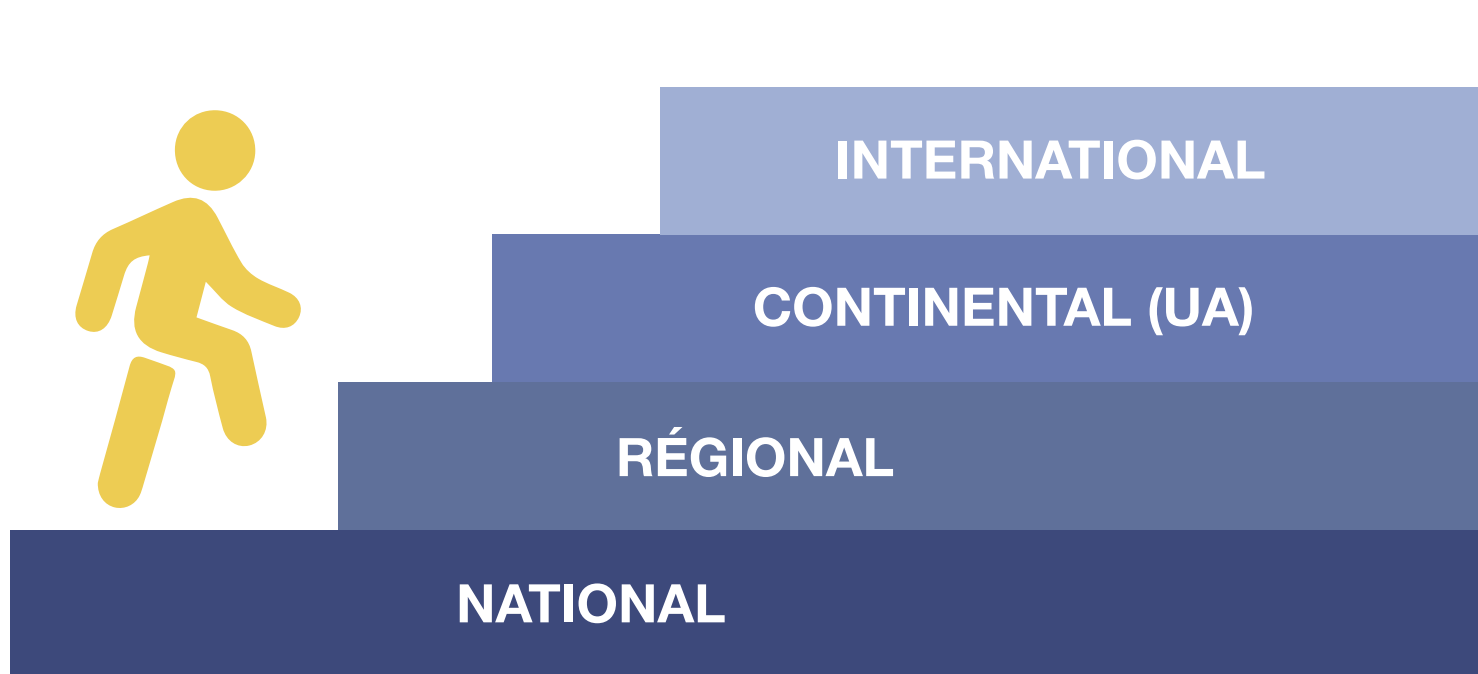
Continuité effective de l'accès au service pour ses utilisateurs.

02 Neutralité technologique

Principe selon lequel la règle de droit ne doit pas favoriser une technologie particulière.



UNE ARCHITECTURE NORMATIVE À QUATRE ÉTAGES



Chaque étage pose des règles ; aucun ne suffit seul à garantir l'effectivité de la norme sur le terrain.

QUI POSE LA RÈGLE, À CHAQUE ÉTAGE ?

INTERNATIONAL

- Union internationale des télécommunications (UIT)
- Standards techniques
- Gouvernance mondiale de l'Internet

CONTINENTAL

- Union africaine
- Convention de Malabo
- Pacte numérique africain
- Smart Africa

RÉGIONAL

- CEDEAO
- UEMOA
- OHADA

NATIONAL

- Code du numérique
- Régulation des télécommunications
- Protection des données
Cybersécurité

Trois cadres régionaux se chevauchent en Afrique de l'Ouest : la CEDEAO pour l'intégration économique, l'UEMOA pour l'union monétaire, l'OHADA pour le droit des affaires. Au niveau continental, la Convention de Malabo n'est entrée en vigueur qu'en 2023, et ne compte à ce jour qu'une quinzaine d'États ratifiants.

LES ACTEURS DE LA GOUVERNANCE DES INFRASTRUCTURES



Entre le premier acteur, qui fixe la politique publique, et le dernier, qui exploite l'infrastructure au quotidien, la chaîne de décision est longue : c'est souvent là que la régulation perd en effectivité.

LES MÉCANISMES DE RÉGULATION

**Licences**

Autorisation formelle d'exercer une activité d'infrastructure ou de service numérique réglementée.

**Autorisations**

Régime plus souple que la licence, pour des activités à moindre enjeu réglementaire.

**Partage d'infrastructures**

Mutualisation imposée ou négociée des réseaux entre opérateurs, pour limiter les doublons coûteux.

**Concurrence**

Contrôle des positions dominantes et des pratiques anticoncurrentielles dans le secteur.

**Accès universel**

Obligation de desservir l'ensemble du territoire, y compris les zones peu rentables commercialement.

LE RÔLE DES AUTORITÉS DE RÉGULATION



Elles ne se contentent pas d'appliquer un texte : elles traduisent une norme en surveillance de marché effective — licences, contrôle technique, sanctions.

Leur pouvoir réel dépend de leur capacité à voir l'infrastructure : sans outils de monitoring et de compétence technique, la régulation reste déclarative.

Elles sont le point de contact concret entre l'État et des opérateurs souvent multinationaux — c'est là que la souveraineté formelle devient, ou non, une souveraineté réelle.

Sur le terrain : former des régulateurs à la surveillance de marché, comme lors de la session organisée pour l'ARCEP du Bénin en juillet 2026, revient précisément à construire cette capacité de voir l'infrastructure.

QUI FAIT QUOI, À CHAQUE NIVEAU ?

NIVEAU	ACTEURS CLÉS	MISSIONS PRINCIPALES
NIVEAU 1 Internationale	UIT (ITU) · ICANN · IETF · W3C · ISO · IEC · Forum sur la gouvernance de l'Internet (IGF)	Normalisation internationale · Gestion des ressources critiques de l'Internet · Attribution des fréquences · Coordination mondiale · Standards techniques
NIVEAU 2 Continentale	Union africaine · Smart Africa · Africa CDC · Organes spécialisés africains	Vision stratégique continentale · Marché numérique africain · Souveraineté numérique · Intelligence artificielle · Cybersécurité · Coopération continentale
NIVEAU 3 Régionale	CEDEAO · UEMOA · OHADA · CEMAC · SADC · EAC (selon les régions)	Harmonisation des législations · Interconnexion régionale · Itinérance (roaming) · Protection des données · Cybersécurité · Intégration des marchés numériques
NIVEAU 4 Nationale	État · Parlement · Gouvernement · Ministère chargé du Numérique · Autorité de régulation · Autorité de protection des données · Agence nationale de cybersécurité · Autorité de concurrence	Élaboration des politiques publiques · Législation · Régulation économique · Attribution des licences · Gestion du spectre · Contrôle des opérateurs · Protection des consommateurs
NIVEAU 5 Opérationnelle	Opérateurs télécoms · Gestionnaires de data centers · Fournisseurs cloud · IXP · Opérateurs satellitaires · Prestataires de services de confiance · Entreprises · Utilisateurs	Déploiement des infrastructures · Exploitation des réseaux · Hébergement des données · Cybersécurité opérationnelle · Maintenance · Innovation · Qualité de service

SÉCURISER L'INFRASTRUCTURE, SÉCURISER L'ÉCHANGE

SÉCURITÉ DES INFRASTRUCTURES

- »»» Infrastructures critiques
- »»» Gestion des risques
- »»» Continuité des services
- »»» CERT — équipe de réponse aux incidents
- »»» SOC — centre de supervision de la sécurité

SERVICES DE CONFIANCE

- »»» Signature électronique
- »»» Horodatage
- »»» Cachet électronique
- »»» Identité numérique
- »»» Services de confiance au sens large

Les deux colonnes se répondent : l'une protège l'infrastructure elle-même, l'autre garantit la valeur juridique de ce qui y transite.

LE TRIANGLE DE LA CONFIANCE NUMÉRIQUE

CONFIANCE NUMÉRIQUE

SÉCURITÉ TECHNIQUE

(Cybersécurité)

- » Confidentialité
- » Intégrité
- » Disponibilité
- » Résilience
- » Continuité d'activité
- » Gestion des incidents

SÉCURITÉ JURIDIQUE

(Services de confiance)

- » Signature électronique
- » Cachet électronique
- » Horodatage électronique
- » Identité numérique
- » Archivage électronique
- » Certification

GOVERNANCE

(Régulation)

- » Régulation sectorielle
- » Protection des données
- » Contrôle des opérateurs
- » Gestion des risques
- » Audit et conformité
- » Supervision

Les trois piliers sont interdépendants : la défaillance d'un seul suffit à compromettre la confiance dans l'ensemble de l'infrastructure.

CE QUE L'IA EXIGE, TECHNIQUEMENT

01**GPU**

Puissance de calcul spécialisée, indispensable à l'entraînement des modèles.

02**CLOUD**

Élasticité de ressources pour absorber les pics de calcul.

03**CENTRES DE DONNÉES**

Localisation physique de la puissance de calcul et du stockage.

04**ÉNERGIE**

L'IA est un secteur intensif en électricité — souvent le facteur limitant réel.

05**DONNÉES**

La matière première de l'entraînement et de l'inférence.

06**CONNECTIVITÉ**

Le transport rapide des données entre utilisateurs, modèles et infrastructures.

LA PYRAMIDE DES INFRASTRUCTURES DE L'IA

NIVEAU 5 — INTELLIGENCE ARTIFICIELLE

Applications et modèles — ChatGPT, Copilot, diagnostic médical, justice, agriculture, finance, éducation

NIVEAU 4 — PUISSANCE DE CALCUL

GPU · TPU · NPU · Cloud Computing
· Supercalculateurs (HPC)

NIVEAU 3 — DONNÉES ET STOCKAGE

Data centers · Bases de données · Data lakes ·
Stockage distribué

NIVEAU 2 — CONNECTIVITÉ

Fibre optique · Internet · 4G/5G/6G · Satellites
· Câbles sous-marins · IXP

NIVEAU 1 — INFRASTRUCTURES FONDAMENTALES

Énergie · Réseaux électriques · Bâtiments techniques · Refroidissement
· Sécurité physique · Ressources humaines

Chaque niveau conditionne le suivant : aucune stratégie d'IA ne peut ignorer les quatre niveaux qui la portent.

CE QUE L'IA POSE, JURIDIQUEMENT



1- Gouvernance des données

Qui décide de la collecte, de l'usage et de la circulation des données d'entraînement ?

2- Responsabilité

À qui imputer un dommage causé par un système dont la chaîne de décision est distribuée ?

3- Calcul souverain

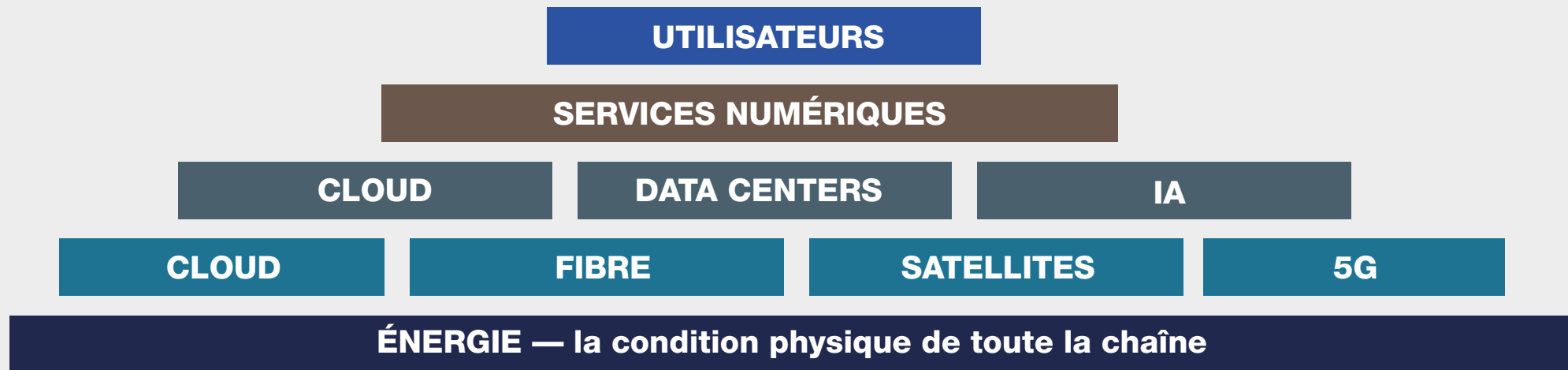
La capacité, ou non, de faire tourner ses propres modèles sur une infrastructure maîtrisée — le Rwanda, avec son autorité unique RISA, en est l'exemple africain le plus abouti à ce jour.

4- IA générative

Un régime encore largement à construire, entre droit d'auteur, données personnelles et transparence algorithmique.

Aucune stratégie nationale d'IA ne réussit sans infrastructures numériques

Une politique d'intelligence artificielle qui ignore le GPU, l'énergie, le datacenter et la connectivité qui la portent reste un texte d'intention. L'infrastructure n'est pas la mise en œuvre de la stratégie IA — elle en est la condition d'existence.



Chaque couche dépend de celle qui la porte — retirez l'énergie, et rien au-dessus ne fonctionne. C'est cette dépendance, plus que la liste des composants, qui doit guider la lecture juridique de l'infrastructure.

99%

du trafic Internet
international transite
par les câbles
sous-marins

Source : UIT, 2026

**950
TWh**

consommation électrique
mondiale des data centers
projetée d'ici 2030, contre
415 TWh en 2024

Source : AIE, 2026

+50%

de hausse de la
consommation élec-
trique des data centers
dédiés à l'IA, en 2025
seulement

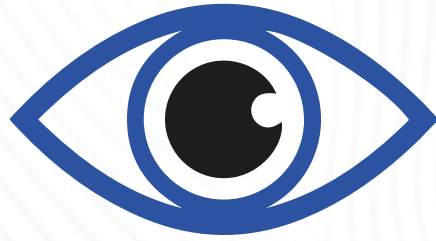
Source : AIE, avril 2026

CONCLUSION GÉNÉRALE

CE QU'IL FAUT RETENIR

- » Les infrastructures numériques sont devenues des infrastructures critiques.
- » Elles constituent la condition d'existence de l'intelligence artificielle.

- » Leur gouvernance est désormais un enjeu de souveraineté.
- » Le droit du numérique ne régle plus seulement les données ; il régle désormais les infrastructures qui les produisent, les transportent, les hébergent et les sécurisent.



« Au XXI^e siècle, les États ne se distingueront plus seulement par leurs ressources naturelles ou leur puissance économique, mais par leur capacité à construire, gouverner et protéger leurs infrastructures numériques. »



JULIEN HOUNKPE
— DOCTEUR EN DROIT —

MERCI..



+229 01 95 88 79 25



julien coomlan hounkpe



julienhounkpe@gmail.com



www.julienhounkpe.info

Étude de cas

Un gouvernement africain souhaite lancer une plateforme nationale d'intelligence artificielle destinée à améliorer les services publics.

Questions :

01

Quelles infrastructures numériques doivent être mises en place avant le lancement du projet ?

02

Quels sont les principaux risques juridiques liés au traitement des données ?

03

Comment garantir la sécurité et la souveraineté des infrastructures mobilisées ?