WWW.CYBERCERCLEAFRICAIN.ORG

NOTE 1

PROTECTION DES DONNÉES

Analyse de la sécurité des données : enjeux, dispositifs africains et impacts concrets

Jeanine TANO-BIAN

Eric BÁRENZUNG

Jean DE DIEU SIDIBÉ

Hyacinthe KOFFI

30 novembre 2025

CERCLE AFRICAIN DE CYBERSÉCURITÉ

Titre de la Note: PROTECTION DES DONNEES

Sous-titre / Thématique : Analyse de la sécurité des données : enjeux, dispositifs africains et impacts concrets

Auteurs /Autrice: Jeanine TANO-BIAN, Eric BÄRENZUNG, Jean DE DIEU SIDIBE, Hyacinthe KOFFI,

Date: 30/11/2025

Contents

Résumé Exécutif

Introduction : Enjeux humains et sociaux de la sécurité des données

La protection des données sensibles représente aujourd'hui un défi central pour le droit pénal du numérique, particulièrement en Afrique. Les récentes cyberattaques, telles que celle ayant visé la direction générale des impôts du Sénégal, illustrent la vulnérabilité d'institutions dépositaires d'informations confidentielles sur des millions de citoyens. Les conséquences d'une fuite de données sont multiples : les individus s'exposent à l'usurpation d'identité, au vol de fonds ou à la manipulation de leurs informations personnelles, tandis que la confiance envers les institutions publiques peut être profondément ébranlée. Pour les institutions, ces incidents entraînent non seulement des pertes financières mais aussi une atteinte à leur légitimité et à leur crédibilité auprès du public.

Niveau continental : Convention de Malabo – objectifs et limites d'application

Au niveau continental, la Convention de Malabo, adoptée par l'Union Africaine en 2014, vise à harmoniser les législations en matière de cybersécurité et de protection des données à caractère personnel. Ce texte établit un socle commun de principes destinés à protéger les citoyens africains contre la cybercriminalité et les abus de données. L'objectif est d'assurer que chaque État membre dispose de lois et de mécanismes effectifs pour prévenir, détecter et sanctionner les atteintes à la sécurité des données.

Cependant, l'application concrète de la Convention demeure limitée : sur 55 pays africains, seuls 21 l'ont signée et 16 l'ont ratifiée à ce jour, restreignant ainsi son impact à une minorité d'États. Cette situation freine l'harmonisation continentale et laisse persister des disparités importantes dans la protection effective des citoyens selon les pays. Malgré son entrée en vigueur en juin 2023, la Convention peine encore à générer un effet structurant à grande échelle.

Niveau régional : Acte additionnel CEDEAO – obligations et disparités d'application

Sur le plan régional, l'Acte additionnel A/SA.1/01/10 adopté par la Communauté Économique des États de l'Afrique de l'Ouest (CEDEAO) impose des obligations strictes en matière de protection des données personnelles. Ce texte a permis de poser des bases communes pour la sécurité des données dans l'espace ouest-africain, notamment en exigeant la création d'autorités de contrôle indépendantes et en fixant des standards minimaux pour la collecte, le traitement et la conservation des données.

Malgré ces avancées, l'application de l'Acte additionnel varie fortement selon les pays. Certains États, comme le Sénégal ou la Côte d'Ivoire, se sont dotés d'autorités de

protection actives et ont engagé des politiques ambitieuses. D'autres, faute de moyens ou de volonté politique, peinent à mettre en œuvre les exigences régionales. Cette hétérogénéité expose les citoyens à des niveaux de risques différents et limite l'efficacité globale du dispositif.

Niveau national : Loi sénégalaise et rôle de la CDP – avancées concrètes et exemples d'actions

Au niveau national, le Sénégal s'est distingué comme pionnier en Afrique de l'Ouest en adoptant la Loi n°2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel, première du genre dans la région. Cette loi a permis la création de la Commission de Protection des Données Personnelles (CDP), chargée de veiller au respect des droits des citoyens et de contrôler les traitements de données.

L'action de la CDP a eu des impacts concrets : par exemple, lors de l'incident de rançongiciel ayant visé la direction générale des impôts, la CDP est intervenue rapidement pour accompagner l'institution dans la gestion de crise, conseiller sur les mesures de remédiation et informer les citoyens sur les risques encourus. Cette réactivité a contribué à limiter les conséquences pour les victimes potentielles et à renforcer la sensibilisation du public aux enjeux de la cybersécurité. De plus, la loi sénégalaise a servi de modèle pour d'autres pays de la région, favorisant ainsi la diffusion de bonnes pratiques et la montée en compétence des institutions nationales.

Par ailleurs, l'application de la législation a permis de sanctionner des entreprises ou administrations ne respectant pas les obligations de sécurité, incitant ainsi l'ensemble des acteurs à renforcer leur vigilance et à adopter des politiques de protection plus strictes.

1. Contexte et Enjeux

Des attaques récentes comme celle ayant visé la direction générale des impôts du Sénégal via un rançongiciel, menaçant de divulguer les données de millions de citoyens, souligne la nécessité d'une vigilance accrue, d'une législation adaptée et d'une jurisprudence protectrice.

Le Règlement Général sur la Protection des Données (RGPD) et les décisions des juridictions européennes offrent un cadre robuste, mais les États africains doivent renforcer leurs dispositifs pour faire face aux menaces croissantes.

Les institutions africaines, qui gèrent de nombreuses informations confidentielles, sont particulièrement exposées à ces risques.

Cette note stratégique a pour défi d’analyser les tendances observées, telles que la multiplication des cyberattaques, la sophistication croissante des menaces et la dépendance aux technologies étrangères.

Les enjeux concernent la souveraineté numérique, la protection des citoyens, la confiance dans les institutions, et la nécessité d’une gouvernance adaptée pour anticiper et répondre efficacement aux risques.

2. Analyse des Vulnérabilités

2.1. Vulnérabilités Techniques

Les faiblesses logicielles et matérielles des systèmes d'information se manifestent à plusieurs niveaux :

- **Obsolescence technologique** : L'utilisation de systèmes d'exploitation ou d'applications en fin de vie expose les organisations à des risques majeurs, car ces solutions ne bénéficient plus de mises à jour de sécurité ni de support technique.
- **Mauvaise configuration des environnements cloud** : Les paramètres par défaut non modifiés, les politiques d'accès trop permissives et l'absence de contrôles rigoureux dans les architectures multiclouds constituent un défi de sécurité majeur identifié par les experts en 2024.
- **Interfaces et APIs insuffisamment protégées** : Les points d'interconnexion entre systèmes, notamment ceux permettant l'échange de données avec des partenaires ou des clients externes, représentent des vecteurs d'attaque privilégiés lorsqu'ils ne sont pas correctement sécurisés.
- **Gestion défaillante des accès et des identités (IAM)** : L'utilisation de mots de passe faibles, l'absence d'authentification multifacteur (MFA) et l'attribution de privilèges excessifs facilitent les mouvements latéraux des attaquants au sein du réseau en cas de compromission initiale.
- **Manque de visibilité et de supervision** : L'incapacité à surveiller et détecter les activités malveillantes en temps réel constitue une vulnérabilité critique, particulièrement dans les environnements informatiques hybrides complexes combinant infrastructures cloud et on-premise.

2.2. Vulnérabilités organisationnelles et humaines

Ces faiblesses relèvent des processus, de la gouvernance et de la dimension humaine de la sécurité :

- **Déficit de sensibilisation et de formation** : Le facteur humain demeure un composant clé de la chaîne de sécurité. Les erreurs comportementales telles que le clic sur un lien malveillant, l'utilisation de supports amovibles non sécurisés ou la divulgation involontaire d'informations sensibles figurent parmi les principales causes de violations de données.
- **Insuffisance de ressources qualifiées en cybersécurité** : La pénurie de personnel spécialisé en interne limite la capacité des organisations à assurer une surveillance continue, une réponse rapide aux incidents et la mise en œuvre rigoureuse des meilleures pratiques de sécurité.
- **Gouvernance de la sécurité déficiente** : L'absence ou l'inadéquation des politiques de sécurité, l'inexistence de plans de réponse aux incidents (PRI) formalisés ou le manque de tests réguliers des plans de continuité d'activité (PCA) affaiblissent considérablement la posture de sécurité globale.
- **Informatique fantôme (Shadow IT)** : L'utilisation non contrôlée de services, d'applications ou de solutions cloud échappant à la supervision du service informatique multiplie les surfaces d'attaque et crée des angles morts en matière de sécurité.
- **Menace interne malveillante ou négligente** : Les employés actuels ou anciens, ainsi que les sous-traitants disposant d'accès légitimes, peuvent compromettre la sécurité par abus de privilèges délibéré ou par négligence involontaire.

Le facteur humain : dernier rempart plutôt que maillon faible

Contrairement au discours traditionnel, l'humain ne constitue pas le maillon faible de la chaîne de sécurité, mais représente au contraire le dernier rempart face aux menaces.

Cette perception s'explique par une réalité tactique : il est considérablement plus simple pour un cybercriminel de déployer massivement des campagnes de phishing que de s'attaquer frontalement à une infrastructure informatique correctement protégée. Lorsqu'un email d'hameçonnage parvient jusqu'à un utilisateur, cela signifie que l'ensemble des dispositifs de filtrage et de protection en amont ont échoué à le bloquer. De même, si un simple clic peut rediriger vers un site malveillant, c'est que les solutions de protection des accès web se révèlent inadéquates ou mal configurées.

Cette analyse révèle une vérité essentielle : qualifier l'humain de « maillon faible » revient à transférer la responsabilité d'échecs techniques et organisationnels sur les collaborateurs. En réalité, ces derniers interviennent en bout de chaîne pour compenser les défaillances des systèmes de défense automatisés.

Il est donc primordial de former et d'entraîner régulièrement le personnel aux cybermenaces, non pas parce qu'il serait intrinsèquement vulnérable, mais parce qu'il constitue la dernière ligne de défense lorsque tous les autres mécanismes de protection ont failli.

2.3. Vulnérabilités Juridiques et de conformité

Ces vulnérabilités découlent d'un non-respect ou d'une interprétation erronée du cadre légal et réglementaire :

- **Non-conformité aux exigences réglementaires** : Le défaut de mise en œuvre des obligations prévues par les référentiels ISO 27701, le RGPD, la directive NIS 2 ou leurs équivalents génère des risques juridiques et opérationnels majeurs. Les manquements les plus fréquents concernent l'absence de base légale ou de consentement valide pour le traitement de données sensibles (notamment dans les secteurs de la santé et de la finance), le non-respect du délai de 72 heures pour notifier les violations de données aux autorités compétentes (CNIL en France), ainsi que l'absence de registre des traitements ou d'analyse d'impact relative à la protection des données (AIPD) pour les traitements présentant des risques élevés.

- **Lacunes contractuelles avec les sous-traitants** : L'insuffisance ou l'absence de clauses contractuelles rigoureuses encadrant la sécurité et la confidentialité des données traitées par des tiers constitue une vulnérabilité significative. La dépendance croissante aux services cloud, sans définition claire de la répartition des responsabilités entre client et fournisseur (matrice de responsabilité partagée), amplifie cette exposition.

- **Incertitude sur la souveraineté et la localisation des données** : Le recours à des solutions cloud ou à des prestataires étrangers, sans garanties juridiques suffisantes contre l'accès par des législations extraterritoriales (telles que le Cloud Act américain), pose une problématique critique pour les données à caractère hautement sensible : données médicales, financières, de transport ou relevant de secteurs d'importance vitale.

3. Impacts Stratégiques

Dans un contexte où la donnée devient le nouvel actif stratégique du développement, la protection des informations sensibles au sein des secteurs vitaux africains (énergie, santé, finance, transport, télécommunications, défense) est un enjeu central de sécurité, de souveraineté et de durabilité.

Les vulnérabilités techniques, organisationnelles et réglementaires observées sur le continent exposent les États et les opérateurs essentiels à des risques systémiques aux répercussions multiples :

- économiques, affectant la compétitivité et la stabilité ;
- sociales, fragilisant la confiance et la cohésion ;
- géopolitiques, compromettant la souveraineté et l'influence africaine dans la gouvernance mondiale du numérique.

(Cadres de référence : Convention de Malabo – Union Africaine, Acte Additionnel CEDEAO

A/SA.1/01/10, Stratégie UA pour la transformation digitale 2020–2030, ISO/IEC 27001 –27701 – 22301, Directive européenne NIS2, Indice mondial de cybersécurité UIT 2024.)

I. Axe Économique

1. Impacts économiques majeurs

Les vulnérabilités liées à la protection des données affectent directement la performance économique des entreprises et des États africains, avec des conséquences mesurables à plusieurs niveaux :

- **Pertes opérationnelles** : Les attaques par rançongiciels (ransomwares), les pannes systèmes et les cyberattaques visant les infrastructures critiques entraînent des interruptions d'activité coûteuses, paralysant parfois des secteurs entiers pendant des jours, voire des semaines.
- **Coûts juridiques et réglementaires** : La non-conformité aux cadres législatifs nationaux et régionaux expose les organisations à des amendes substantielles, des pénalités administratives et des contentieux prolongés, mobilisant des ressources considérables en frais juridiques et en temps de gestion.
- **Escalade des dépenses de sécurité** : La nécessité de renforcer les dispositifs de protection, de mettre en place des solutions de reprise d'activité et de souscrire à des polices d'assurance cyber de plus en plus onéreuses grève les budgets informatiques et réduit les marges opérationnelles.

- **Dépendance technologique structurelle** : Le recours massif à des fournisseurs extracontinentaux pour les services cloud, les logiciels de sécurité et les solutions de gestion des données limite l'autonomie stratégique et expose à des risques géopolitiques et économiques à long terme.

Selon les données de la Banque mondiale (2024), la mauvaise gouvernance de la donnée coûte chaque année plus de 3 % du PIB numérique africain, réduisant substantiellement la capacité d'investissement dans l'innovation locale et freinant le développement du secteur technologique continental.

2. Facteurs explicatifs

Plusieurs facteurs structurels et opérationnels expliquent la persistance de ces vulnérabilités :

- **Obsolescence technologique** : Le maintien en exploitation de systèmes informatiques vieillissants, d'équipements en fin de vie et d'infrastructures réseaux obsolètes crée des brèches de sécurité critiques, d'autant plus que ces environnements ne bénéficient plus de correctifs ni de support technique.
- **Défaillances dans la sécurisation des environnements cloud** : Les configurations par défaut non modifiées, l'absence de politiques de contrôle d'accès granulaire et le manque de segmentation des ressources exposent les données hébergées dans le cloud à des risques d'accès non autorisés et de fuites massives.
- **Gouvernance insuffisante de la chaîne de sous-traitance** : La multiplication des prestataires et partenaires technologiques, combinée à l'absence de clauses contractuelles rigoureuses et de mécanismes d'audit réguliers, dilue les responsabilités et affaiblit la maîtrise globale de la sécurité des données.
- **Pénurie de compétences locales en cybersécurité** : Le déficit critique de professionnels qualifiés contraint les organisations à externaliser la gestion des incidents et la supervision de leurs infrastructures, créant une dépendance problématique vis-à-vis de prestataires externes et ralentissant les capacités de réaction en cas d'attaque.

3. Enjeux stratégiques

La sécurisation des données sensibles représente un levier de transformation structurelle dont dépend l'avenir numérique du continent africain :

- **Renforcement de la résilience opérationnelle** : Le développement et la mise en œuvre de plans de continuité d'activité (PCA) et de reprise d'activité (PRA) conformes aux standards internationaux tels que l'ISO 22301 permettent de garantir la pérennité des services critiques face aux incidents de sécurité et aux catastrophes, tout en minimisant les temps d'interruption et les pertes de données.

- Affirmation de la souveraineté numérique : La maîtrise de la chaîne de valeur numérique passe par le déploiement d'infrastructures d'hébergement locales et régionales, le développement de capacités cryptographiques souveraines et la mise en place de systèmes de redondance à l'échelle continentale, réduisant ainsi la dépendance aux acteurs extérieurs et préservant le contrôle sur les données stratégiques.

- **Émergence d'un écosystème africain de cybersécurité** : La structuration d'un marché continental de la cybersécurité, soutenu par des investissements dans la recherche, l'innovation technologique et la formation de talents locaux, créera des emplois hautement qualifiés et favorisera l'apparition de champions régionaux capables de rivaliser sur la scène internationale.

- **Intégration transversale dans les politiques publiques** : La protection des données sensibles doit être érigée en priorité stratégique des politiques industrielles, des programmes de transformation numérique et des mécanismes de financement du développement, assurant ainsi une approche cohérente et coordonnée à l'échelle nationale et régionale.

II. Axe Social

1. Impacts majeurs

Les violations de données et les défaillances dans leur gouvernance génèrent des répercussions profondes sur le tissu social africain :

- **Érosion de la confiance institutionnelle** : Les fuites de données personnelles et les atteintes à la vie privée sapent durablement la confiance des citoyens envers les institutions publiques et les acteurs privés, freinant l'adoption des services numériques et la participation citoyenne aux initiatives de transformation digitale.

- **Fragilisation des services essentiels** : Les cyberattaques et dysfonctionnements affectant les systèmes de santé, les infrastructures de paiement, les réseaux énergétiques ou les services de mobilité ont un impact direct et immédiat sur les conditions de vie des populations, particulièrement dans les zones où l'accès à ces services reste précaire.

- **Aggravation de la fracture numérique** : L'absence de sensibilisation et de formation à la protection des données renforce l'exclusion numérique des groupes vulnérables – personnes âgées, populations rurales, personnes à faible niveau d'alphabétisation – qui deviennent des cibles privilégiées de la cybercriminalité tout en étant privés des bénéfices de l'économie numérique.

- **Hémorragie des compétences critiques** : La fuite des talents qualifiés dans les métiers du numérique et de la cybersécurité vers des marchés plus matures accentue la dépendance du continent vis-à-vis de l'expertise étrangère et compromet le développement d'un écosystème technologique autonome et résilient.

Selon l'Union internationale des télécommunications (UIT, 2024), plus de 65 % des incidents cyber déclarés en Afrique trouvent leur origine dans le facteur humain – erreur involontaire, négligence ou malveillance interne –, confirmant la nécessité impérieuse d'investir massivement dans la formation et la sensibilisation à tous les niveaux de la société.

2. Facteurs explicatifs

Plusieurs facteurs socioculturels et éducatifs expliquent la vulnérabilité sociale face aux enjeux de protection des données :

- **Déficit généralisé de sensibilisation** : L'absence de campagnes d'information accessibles et adaptées aux différents publics laisse le personnel des organisations, comme les citoyens ordinaires, largement démunis face aux risques numériques. Cette méconnaissance des menaces, des bonnes pratiques de sécurité et des droits fondamentaux en matière de données personnelles favorise les comportements à risque et la manipulation par des acteurs malveillants.

- **Insuffisance de l'offre de formation qualifiante** : Le manque criant de programmes de formation spécialisés en gouvernance de la donnée, en cybersécurité et en protection des infrastructures critiques limite la constitution d'un vivier de compétences locales. Cette lacune affecte autant la formation initiale universitaire que la formation continue des professionnels, perpétuant ainsi la dépendance aux expertises étrangères.

- **Culture de l'opacité en cas d'incident** : La faible culture de transparence qui prévaut dans de nombreuses organisations se traduit par des notifications tardives, incomplètes ou totalement absentes lors de violations de données. Cette opacité entrave non seulement la protection des personnes affectées, mais empêche également l'apprentissage collectif et l'amélioration des pratiques de sécurité à l'échelle du secteur ou du pays.

3. Enjeux stratégiques

La dimension sociale de la protection des données appelle une transformation culturelle profonde et des investissements structurants dans le capital humain :

- **Ancrage d'une culture africaine de la cybersécurité** : L'intégration systématique de l'éducation numérique et de la sensibilisation aux enjeux de protection des données dès les cycles primaire et secondaire, prolongée par des modules obligatoires dans la formation professionnelle et universitaire, permettra de former des générations de citoyens et de professionnels conscients des risques et dotés des réflexes de sécurité indispensables à l'ère numérique.

- **Création de pôles régionaux d'excellence** : Le déploiement de centres régionaux de compétences en cybersécurité – académies spécialisées, équipes nationales et régionales d'intervention d'urgence (CERT/CIRT), laboratoires de recherche appliquée – structurera l'écosystème de formation, favorisera la mutualisation des expertises et des ressources, et accélérera le développement de capacités endogènes de réponse aux menaces.

- **Institutionnalisation de la transparence** : L'adoption de protocoles rigoureux de communication en cas d'incident, assortis d'obligations de notification claires et de sanctions dissuasives en cas de dissimulation, établira une culture de responsabilité qui restaurera la confiance des citoyens et permettra un apprentissage collectif des failles identifiées.

- **Protection des données comme levier d'inclusion numérique** : En érigeant la protection des données en droit fondamental accessible à tous, indépendamment du niveau d'éducation ou de la situation socio-économique, le continent africain peut transformer ce qui est souvent perçu comme une contrainte en véritable vecteur d'inclusion, créant ainsi les conditions de confiance nécessaires à l'adoption massive des services numériques et à la réussite de la transformation digitale.

III. Axe Géopolitique

1. Impacts majeurs

La donnée s'est imposée comme un instrument stratégique de pouvoir et de diplomatie au XXIe siècle. Dans ce contexte, les vulnérabilités africaines en matière de protection des données engendrent des conséquences géopolitiques considérables :

- **Érosion de la souveraineté numérique** : L'hébergement massif de données critiques – gouvernementales, économiques, sanitaires – dans des infrastructures situées sous juridictions étrangères expose le continent à des législations extraterritoriales telles que le Cloud Act américain, permettant à des puissances

tierces d'accéder légalement à des informations stratégiques sans contrôle ni consentement des États africains concernés.

- **Vulnérabilité à l'espionnage économique et stratégique** : L'exploitation des failles dans les infrastructures numériques, les interfaces de programmation (API) sensibles et les systèmes de communication gouvernementaux offre à des acteurs étatiques ou para-étatiques étrangers la capacité de collecter des renseignements économiques, politiques et militaires, compromettant ainsi la compétitivité des entreprises africaines et la confidentialité des processus décisionnels stratégiques.
- **Asymétrie de puissance technologique** : La dépendance structurelle vis-à-vis des géants technologiques extra-continentaux pour les services cloud, les logiciels critiques, les équipements réseau et les solutions de cybersécurité place le continent en position de subordination technologique, limitant ses marges de manœuvre diplomatiques et son autonomie stratégique dans les négociations internationales.
- **Fragmentation du cadre réglementaire continental** : L'absence d'harmonisation des législations nationales en matière de protection des données et de cybersécurité affaiblit considérablement la capacité de l'Afrique à parler d'une seule voix dans les forums internationaux et à peser dans l'élaboration des normes mondiales de gouvernance numérique, la condamnant à subir des règles définies ailleurs.

Selon l'Union Africaine, seule la moitié des pays du continent dispose d'un cadre juridique complet de protection des données, tandis qu'à peine un tiers ont effectivement mis en œuvre un plan national de cybersécurité. Cette disparité illustre la fragilité de la posture africaine face aux enjeux géopolitiques du numérique.

2. Facteurs explicatifs

Plusieurs déficits structurels et institutionnels expliquent la vulnérabilité géopolitique du continent africain face aux enjeux de protection des données :

- **Insuffisance des infrastructures numériques souveraines** : L'absence critique de centres de données (data centers) de classe internationale à l'échelle régionale et le sous-développement de solutions d'hébergement cloud locales contraignent les États, les entreprises et les institutions africaines à externaliser le stockage et le traitement de leurs données sensibles vers des infrastructures extra-continentales, transférant de facto le contrôle de ressources stratégiques à des acteurs étrangers.
- **Fragmentation de la coopération en matière de cybersécurité** : Le manque de coordination opérationnelle entre les États membres de l'Union Africaine, l'absence d'interopérabilité entre les équipes nationales d'intervention d'urgence informatique (CERT), et la faiblesse des mécanismes de partage d'informations

sur les menaces empêchent l'émergence d'une réponse collective et efficace face à des cybermenaces de plus en plus transfrontalières et sophistiquées.

- **Absence de vision diplomatique numérique partagée** : Le défaut de politique commune de diplomatie numérique à l'échelle continentale prive l'Afrique d'une voix unifiée et d'un poids de négociation conséquent dans les instances internationales de gouvernance de l'internet, les forums de normalisation technique et les négociations bilatérales ou multilatérales portant sur les flux de données, la fiscalité numérique ou les transferts de technologies.

3. Enjeux stratégiques

L'affirmation de la puissance africaine à l'ère numérique passe par des choix stratégiques audacieux et une action collective coordonnée :

- **Construction d'une souveraineté numérique continentale** : L'établissement d'une véritable autonomie stratégique nécessite la maîtrise intégrale de la chaîne de valeur numérique : déploiement massif d'infrastructures d'hébergement sur le continent, développement de capacités cryptographiques endogènes garantissant la confidentialité des communications sensibles, et instauration de mécanismes de contrôle rigoureux des flux transfrontaliers de données pour préserver les intérêts économiques et sécuritaires des États africains.

- **Opérationnalisation de la Convention de Malabo** : La transformation de la Convention de l'Union Africaine sur la cybersécurité et la protection des données personnelles en cadre juridique continental contraignant et effectivement appliqué constitue un prérequis indispensable à l'harmonisation réglementaire. Son adoption universelle et sa mise en œuvre rigoureuse par l'ensemble des États membres créeront un espace juridique unifié, renforçant la crédibilité et le poids diplomatique du continent.

- **Institutionnalisation de la coopération régionale en cybersécurité** : La création de mécanismes permanents de partage d'informations sur les menaces, d'assistance technique mutuelle en cas d'incident majeur, et de coordination des réponses aux cyberattaques transfrontalières permettra de mutualiser les ressources limitées, d'accélérer les temps de réaction et de constituer progressivement une communauté africaine de cyberdéfense capable de faire face aux menaces les plus sophistiquées.

- **Affirmation d'un leadership africain dans la gouvernance numérique mondiale** : Le positionnement proactif du continent dans les instances internationales de régulation des données, les forums de normalisation technique et les négociations sur l'encadrement éthique et juridique de l'intelligence artificielle permettra à l'Afrique de défendre ses intérêts spécifiques, d'influencer

l'élaboration des normes mondiales et de s'imposer comme un acteur incontournable – et non plus un simple récipiendaire – de la gouvernance numérique globale.

Conclusion

La protection des données sensibles constitue bien plus qu'un enjeu technique ou réglementaire : elle représente un levier stratégique central du développement durable et de l'affirmation de la souveraineté africaine au XXIe siècle.

Les États, les institutions régionales et les acteurs économiques du continent doivent opérer un changement de paradigme en considérant la gouvernance des données non comme une contrainte administrative, mais comme un pilier fondamental de puissance géopolitique, de compétitivité économique et de cohésion sociale. C'est à cette condition que l'Afrique pourra transformer sa transition numérique en véritable levier d'émancipation et de prospérité partagée.

Cette ambition appelle une mobilisation collective articulée autour de trois priorités stratégiques indissociables :

- **Renforcer l'architecture continentale de gouvernance des données** : L'harmonisation et l'opérationnalisation des cadres juridiques et institutionnels à tous les niveaux – continental (Union Africaine), sous-régional (CEDEAO, CEMAC, SADC, etc.) et national – permettront de créer un espace numérique africain cohérent, prévisible et attractif, capable de rivaliser avec les grands blocs réglementaires mondiaux tout en préservant les spécificités et les intérêts du continent.

- **Investir massivement dans le capital humain et les infrastructures critiques** : Le développement de compétences locales de haut niveau en cybersécurité, en gouvernance des données et en technologies émergentes, combiné au déploiement d'infrastructures numériques souveraines et résilientes, constitue le socle indispensable sur lequel reposent l'autonomie stratégique, la capacité d'innovation et la création de valeur à long terme.

- **Forger une diplomatie numérique africaine assertive et solidaire** : L'émergence d'une voix africaine unifiée et influente dans les forums internationaux de gouvernance numérique, fondée sur les principes de solidarité continentale, de confiance partagée et de défense collective des intérêts stratégiques communs, permettra au continent de peser dans la définition des règles du jeu numérique mondial et de négocier en position de force les partenariats technologiques de demain.

L'heure n'est plus à la simple prise de conscience, mais à l'action résolue et coordonnée. La fenêtre d'opportunité pour bâtir une Afrique numérique souveraine, prospère et résiliente est ouverte, mais elle ne le restera pas indéfiniment. C'est maintenant que se jouent l'indépendance stratégique et la place du continent dans l'ordre numérique mondial des décennies à venir.

4. Recommandations

Recommandations techniques

Les infrastructures critiques (ICs) présentent quelques défis spécifiques dans le cadre de leur utilisation :

- Une disponibilité prioritaire : les systèmes ne peuvent souvent pas être arrêtés pour maintenance
- Des systèmes hérités de période où leur sécurité informatique n'avait pas encore cette importance
- Des environnements hybrides IT/OT complexifiant leur sécurisation

La directive Européenne NIS2 1 donne quelques axes de mesures techniques. (Réf. https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fr)

Ce document se focalisant sur la protection des données, les paragraphes suivant proposent quelques suggestions sur ce sujet.

Recommandations organisationnelles

Les mesures techniques ne peuvent être totalement efficaces sans une gouvernance appropriée. La protection des données sensibles au sein des infrastructures critiques repose donc également sur des mesures organisationnelles robustes et appliquée avec rigueur.

Dans le cadre de ce document, la partie Gestion des Incidents n'est pas couverte. Le CAC reste à disposition pour des recommandations associées à ce sujet.

Mise en place d'une gouvernance

La première étape consiste à établir une gouvernance claire avec la nomination de responsables clés disposant de l'autorité et des ressources nécessaires : un/e Responsable de la Sécurité des Systèmes d'Information (RSSI), un/e Délégué(e) à la Protection des Données (DPD), et un/e responsable de la sécurité opérationnelle.

Ces acteurs doivent formaliser une politique de sécurité globale, déclinée en politiques thématiques et procédures opérationnelles couvrant tous les aspects de la protection des

données. Ces rôles doivent dépendre directement du management (CEO/COO) et avoir le soutien du Conseil d'administration.

Note : le CAC propose la mise à disposition de ressources expertes capables d'assurer les missions de RSSI et/ou DPO au sein de votre organisation

Documentation et traçabilité

La documentation exhaustive de toutes les mesures, politiques, procédures, incidents et actions correctives doit être assurée de manière rigoureuse. Cette documentation répond à plusieurs objectifs : garantir la traçabilité des décisions et actions de sécurité, faciliter les audits de conformité internes et externes, permettre la formation et l'intégration de nouveaux collaborateurs, et capitaliser sur les retours d'expérience pour l'amélioration continue.

Audits et contrôles

Un programme d'audits de sécurité réguliers doit être instauré pour évaluer l'efficacité des mesures déployées, identifier les écarts de conformité réglementaire et les vulnérabilités organisationnelles. Ces audits, réalisés au minimum annuellement (idéalement semestriellement pour les systèmes les plus critiques), doivent couvrir tant les aspects techniques qu'organisationnels.

Chaque audit doit donner lieu à un plan d'action priorisé, avec des responsables clairement identifiés et des échéances de mise en œuvre définies. Le suivi de la réalisation de ces plans d'action doit être assuré au plus haut niveau de l'organisation pour garantir leur exécution effective.

Certifications

ISO

Les certifications ou à minima la gouvernance associée à des certifications ISO et/ou de type SOC2 devraient être mise en place :

- ISO/IEC 27001 - La certification fondamentale pour le management de la sécurité de l'information. Indispensable pour toute infrastructure critique.
- ISO/IEC 27017 - Extension spécifique pour la sécurité du cloud computing.
- ISO/IEC 27018 - Protection des données personnelles dans le cloud.
- ISO/IEC 27701 - Système de management de la protection de la vie privé
- (extension de l'ISO 27001 pour le RGPD).

SOC2 Type II

Un rapport SOC 2 Type II est clé car il :

- les contrôles FONCTIONNENT sur 6-12 mois
- Teste l'efficacité opérationnelle réelle
- Détecte les défaillances, interruptions, exceptions
- Prouve la constance et la discipline de sécurité

*Certifications associées aux domaines**

Selon le type d'activités, d'autres certifications devraient être mise en place :

- Santé : par ex. HDS (Hébergement Données de Santé)
- Finance : par ex. PCI-DSS
- Energie : par ex. IEC 62443

Amélioration continue et veille

L'organisation doit mettre en place une démarche d'amélioration continue s'appuyant sur un système de management de la sécurité de l'information, tel que préconisé par les normes ISO/IEC 27001 (pour la sécurité des systèmes d'information) et ISO/IEC27701 (pour la protection de la vie privée). Ce système structure la gouvernance dans la durée et facilite la démonstration de la conformité réglementaire.

Veille des menaces

Une veille active doit être maintenue sur l'évolution des menaces, des techniques d'attaque, des vulnérabilités affectant les technologies utilisées, et des exigences réglementaires. Cette veille alimente l'adaptation permanente des mesures de protection et la priorisation des investissements de sécurité.

Une analyse et surveillance des risques

La gouvernance doit s'appuyer obligatoirement sur une analyse de risques approfondie permettant d'identifier ses Points d'Importance Vitale (PIV), d'évaluer les menaces spécifiques (cyberattaques, menaces internes, défaillances techniques), et de définir les mesures de protection proportionnées aux enjeux.

L'élaboration d'un Plan de Sécurité d'Opérateur d'Importance Vitale (PSO) doit formaliser cette démarche. Pour chacun de ces PIV, le Plan de sécurité d'Opérateur d'Importance Vitale (PSO) doit prévoir la rédaction d'un Plan Particulier de Protection (PPP).

Gestion du personnel

La sécurité des données repose largement sur le facteur humain. L'organisation doit définir les catégories de personnel et mettre en place des vérifications d'antécédents appropriées pour tous les postes, en particulier pour le personnel exerçant des fonctions critiques sensibles ou ayant accès aux infrastructures ou données les plus critiques.

Des procédures claires doivent définir les responsabilités de chaque acteur en matière de protection des données, avec des conséquences formalisées en cas de non-respect.

Classification des données

L'organisation doit mettre en œuvre une classification systématique des données selon leur niveau de sensibilité et mettre en place des mesures de protection adéquates.

Gestion des accès

Les procédures strictes de gestion du cycle de vie des accès doivent couvrir l'attribution initiale des droits, leur révision régulière (au minimum trimestrielle), et leur révocation immédiate en cas de changement de fonction ou de départ. Un système de contrôle d'accès basé sur les rôles (RBAC) doit être déployé, appliquant rigoureusement le principe du moindre privilège pour limiter l'exposition des données sensibles.

Gestion des sous-traitants

Les sous-traitants accédant aux infrastructures critiques doivent faire l'objet d'une qualification sécuritaire stricte (audits, certifications ISO 27001) et de clauses contractuelles contraignantes, avec traçabilité complète de leurs accès, limitation au principe du moindre privilège, et révocation immédiate en fin de mission.

Un suivi continu de leur posture de sécurité et de leurs propres sous-traitants est indispensable pour maîtriser les risques de la chaîne d'approvisionnement (supply chain), principale source de compromission des infrastructures sensibles.

Sensibilisation à la sécurité

Un programme continu de sensibilisation et de formation à la sécurité doit être déployé, couvrant les menaces actuelles (hameçonnage/phishing, ingénierie sociale, ransomware, hypertrucage/deepfake, risques liés à l'intelligence artificielle), les bonnes pratiques de protection des données, et les procédures internes à respecter. Ces formations doivent être actualisées régulièrement face à l'évolution des menaces.

Des exercices de campagnes doivent être menés régulièrement et les personnes ayant failli de façon récurrente doivent suivre une formation dédiée. Une solution de notification de phishing devra être mise en place afin d'informer le plus rapidement possible les équipes du Centre Opérationnel de Sécurité (SOC) pour une remédiation de la menace si confirmée, notamment dans le cadre d'une attaque en masse du personnel.

Résilience et continuité opérationnelle

Analyse des incidences sur les activités

Dans le contexte réglementaire des infrastructures critiques, le BIA (Business Impact Analysis) établit le socle factuel justifiant les investissements de résilience et lesexigences du PCA (Plan de Continuité des Activités). Le BIA quantifie précisément les impacts d'indisponibilité de chaque fonction (conséquences sur la sécurité publique, l'économie, la souveraineté nationale), identifie les dépendances et points de défaillance uniques, et définit les objectifs de temps de reprise (RTO) et de perte de données acceptable (RPO) contraignants pour les processus vitaux.

Plans de Continuité d'Activité (PCA)

L'organisation doit élaborer et maintenir à jour des Plans de Continuité d'Activité (PCA) et des Plans de Reprise après Sinistre (PRA) garantissant la résilience face aux incidents majeurs. Ces plans doivent identifier les fonctions vitales, définir les objectifs de temps de reprise (RTO) et de perte de données acceptable (RPO), et prévoir les moyens humains, techniques et organisationnels nécessaires à la restauration des services critiques.

Validation des plans

Des tests réguliers de ces plans (au minimum annuel, idéalement semestriels) doivent être réalisés pour valider leur efficacité et identifier les points d'amélioration.

Ces exercices peuvent prendre différentes formes : simulations sur table (exercice 1 sur table / tabletop exercises), tests partiels ou tests en conditions réelles selon la criticité des systèmes.

Coopération et partage d'informations

L'efficacité de la protection des infrastructures critiques repose également sur lacoopération avec l'écosystème de sécurité. L'organisation doit favoriser le partage d'informations sur les menaces émergentes et les incidents avec les autorités nationales de cybersécurité, les partenaires sectoriels, et les réseaux de partage d'informations (AfricaCERT 2 , CESIA 3 , CERT nationaux, etc.).

Cette coopération permet de bénéficier d'une vision élargie des menaces, d'alertes précoces sur les campagnes d'attaque en cours, et de retours d'expérience d'autres organisations confrontées à des incidents similaires. La participation active à ces réseaux de confiance constitue un élément différenciant dans la capacité à anticiper et contrer les cybermenaces sophistiquées.

5. Conclusion et Pistes d'Action

Conclusion : Importance de l'adoption et de l'amélioration des dispositifs

Les exemples sénégalais et ouest-africains montrent que l'existence de cadres juridiques adaptés et d'autorités de contrôle actives contribue à améliorer la protection des citoyens, à limiter les risques d'usurpation d'identité et à restaurer la confiance dans les institutions publiques. Toutefois, l'efficacité de la réponse dépend de la volonté politique, des ressources allouées et de l'harmonisation des législations à l'échelle continentale. Il est donc essentiel que l'ensemble des États africains s'engagent dans une dynamique d'adoption, de mise en œuvre et d'amélioration continue de leurs dispositifs pour anticiper les menaces et garantir la sécurité des données, pilier fondamental de la confiance numérique.

En définitive, la protection des infrastructures critiques exige une démarche proactive, intégrant des exercices réguliers, une coopération étroite avec l'ensemble des acteurs du secteur et une adaptation continue face à l'évolution des menaces. L'engagement dans le partage d'informations et la mutualisation des connaissances renforcent significativement la résilience collective face aux cyberattaques. Pour progresser, il est essentiel d'investir dans la formation, d'actualiser les plans de réponse et de valoriser l'innovation au sein des dispositifs de sécurité. Ces pistes d'action permettront aux organisations de mieux anticiper, détecter et contrer les menaces, tout en assurant la continuité et la sécurité des services essentiels.