AFRICA DATA PROTECTION REPORT

JUIN 2025

AFRICA DATA PROTECTION

ÉDITO

PROTECTION DES DONNÉES EN AFRIQUE : LA DYNAMIQUE S'ACCÉLÈRE

Par Jules Hervé YIMEUMI
Président de l'association Africa Data Protection

Le paysage africain de la protection des données connaît un dynamisme sans précédent. Ces derniers mois ont été marqués par une série de décisions fortes, révélant une montée en puissance des autorités locales face aux enjeux de souveraineté numérique et de respect des droits fondamentaux.

Au Nigeria, un tournant majeur a été franchi avec la confirmation, par la justice, d'une amende record de 220 millions de dollars infligée à la Société Meta. Le Tribunal nigérian a, en effet, rejeté l'appel de la multinationale contre la décision de sanction rendue le 19 juillet 2024 par la Commission fédérale de la concurrence et de la protection des consommateurs (FCCPC), estimant que les violations constatées par la Commission – notamment dans les services WhatsApp et Facebook – avaient été correctement qualifiées. Une décision qui envoie un message clair : l'impunité des géants du numérique n'est plus une fatalité sur le continent.
Autre fait notable : au Mali, l'Autorité de Protection des Données Personnelles (APDP) a sanctionné une entreprise d'une amende de 5 millions de francs CFA (environ 8 300 dollars) pour entrave à une mission de contrôle. Une décision qui rappelle l'importance de la coopération des responsables de traitement avec les régulateurs, et fait écho à une situation similaire observée récemment au Gabon, où l'autorité de protection des données (APDPVP) n'a pas pu accéder aux documents administratifs d'une société lors d'un contrôle.
Le Mali renforce également son action sur le terrain : l'APDP a récemment mis en demeure successivement 84 puis 100 organismes pour non-respect de leurs obligations déclaratives. Ces structures se sont vu accorder un délai pour se mettre en conformité, sous peine de sanctions. Une vigilance qui traduit la volonté croissante des autorités africaines de bâtir des cadres robustes et crédibles.

Enfin, en Afrique du Sud, le régulateur de l'information (Information Regulator) a officialisé un amendement clé au Règlement de 2018 sur la protection des données personnelles. Ce texte clarifie des points essentiels tels que le droit d'opposition, l'effacement ou encore la rectification des données, en imposant un délai de 30 jours pour le traitement de ces demandes. Il renforce aussi les obligations en matière de marketing direct et encadre mieux le traitement des plaintes, tout en introduisant la possibilité de paiement échelonné pour les amendes administratives.

Ces signaux convergents témoignent d'une évolution profonde : l'Afrique affirme de plus en plus sa souveraineté numérique et attend une protection renforcée des données de ses citoyens. L'ère de l'inaction est révolue. Désormais, la protection des données personnelles n'est plus un luxe ou un simple enjeu technique ; elle devient un pilier essentiel de l'État de droit et du développement du numérique sur le continent. **JHY**

ÉTAT DES LIEUX DE LA PROTECTION DES DONNÉES EN AFRIQUE (JUIN 2025)

RÉSEAU DES AUTORITÉS AFRICAINES DE PROTECTION DES DONNÉES : VERS UNE CONVERGENCE STRATÉGIQUE POUR LA PROTECTION DES DONNÉES EN AFRIQUE

Par **Moussa SALL**, Senior Consultant en cybersécurité GRC

© ODPC

Du 6 au 8 mai 2025, Abuja a été le théâtre de la 8ème édition de la Conférence du Réseau des Autorités Africaines de Protection des Données (NADPA-RAPDP). Cet événement d'envergure internationale a rassemblé des représentants de plus de 30 pays africains, ainsi que d'Europe, d'Asie, du Moyen-Orient et des États-Unis, autour d'un objectif commun : concilier innovation technologique et respect des droits fondamentaux à l'ère numérique.

Un thème d'actualité : concilier innovation et protection des données

Placée sous le thème « Équilibrer l'innovation en Afrique : protection des données et vie privée dans les technologies émergentes », la conférence a alterné panels techniques, discours stratégiques, ateliers thématiques et rencontres de haut niveau. Les discussions ont mis en lumière des enjeux critiques : l'impact de l'intelligence artificielle, les défis liés à la FinTech, les identités numériques et la gouvernance des flux transfrontaliers de données. L'objectif affiché : renforcer la coopération interafricaine, identifier et combler les lacunes réglementaires, proposer des mécanismes concrets de conformité, et établir un socle commun de standards numériques adaptés aux réalités du continent.

Le Nigeria en position de leadership

Pays hôte de cette édition, le Nigeria s'est affirmé comme un acteur central dans la structuration de la gouvernance des données personnelles en Afrique. La Nigeria Data Protection Commission (NDPC) a présenté des résultats significatifs : plus de 5 000 audits de conformité réalisés et 1,2 million USD de revenus générés. Deux annonces majeures ont marqué l'événement :
- le lancement de la Nigeria Virtual Privacy Academy ;
- la signature d'un protocole d'accord stratégique avec Mastercard, réunissant plus de 150 acteurs du secteur public et privé.

Technologies émergentes : entre opportunités et vigilance

Les technologies émergentes ont été au cœur des échanges. Dans le secteur de la FinTech, les experts ont souligné l'urgence de réguler sans brider l'innovation. La croissance rapide des paiements mobiles et de la blockchain en Afrique nécessite un cadre réglementaire robuste pour prévenir les dérives telles que le profilage abusif, la collecte excessive de données ou l'opacité algorithmique. En matière d'intelligence artificielle, la notion de régulation par le design a été mise en avant. Intégrer la protection de la vie privée dès la conception des systèmes, recourir aux technologies de préservation de la confidentialité (PETs), et lutter contre les biais algorithmiques dans les jeux de données sont désormais des impératifs techniques autant que politiques.

Identité numérique et confiance citoyenne

L'identité numérique, considérée comme une pierre angulaire de l'infrastructure numérique africaine, a fait l'objet d'un consensus : sans confiance, aucune transformation digitale ne sera pérenne. Protéger les données personnelles est la condition sine qua non pour garantir l'adhésion des citoyens aux systèmes numériques.

Inégalités persistantes et urgence des moyens

La conférence a également mis en lumière les disparités qui subsistent à travers le continent. Si certains pays ont adopté des législations avancées, leur mise en œuvre est souvent entravée par un manque de ressources humaines, financières et techniques. Le témoignage poignant d'une intervenante somalienne a mis en exergue l'ampleur des violations graves en l'absence de protections minimales, rappelant que la protection des données touche à la dignité humaine et à la sécurité des individus.

Souveraineté numérique VS commerce transfrontalier

Un point de tension majeur a été soulevé : la souveraineté des données face aux impératifs du commerce numérique. Alors que les flux transfrontaliers s'intensifient via des services cloud internationaux, les données africaines circulent souvent sans garanties suffisantes. Ce paradoxe appelle à une infrastructure locale renforcée, à des centres de données souverains, et à une application effective des législations existantes.

Renforcement institutionnel et cadre juridique commun

Lors de l'Assemblée générale du réseau NADPA, la Tanzanie et la Somalie ont officiellement rejoint le réseau. Un processus de modernisation du secrétariat a été lancé pour renforcer sa capacité de coordination. La commissaire kenyane a souligné l'urgence d'une gouvernance numérique cohérente, inclusive et résiliente, plaidant pour :
- une coopération renforcée entre les secteurs public et privé,
- un investissement massif dans le capital humain,
- une harmonisation concrète des cadres juridiques, via la mise en œuvre de la Convention de Malabo.

Cette convention représente aujourd'hui un socle commun pour l'alignement des cadres réglementaires africains. Il ne s'agit pas d'imposer une uniformisation, mais de promouvoir une convergence stratégique autour de principes partagés, respectueux des spécificités nationales, tout en assurant l'interopérabilité continentale.

Vers une souveraineté numérique africaine

Parmi les enseignements clés de ces trois journées, plusieurs principes fondamentaux se sont imposés :
- la nécessité d'une innovation responsable ;
- l'importance d'une coopération pérenne entre autorités de protection des données ;
- le rôle fondamental de la transparence et de la redevabilité ;
- l'impératif de renforcer durablement les capacités humaines et institutionnelles.

En conclusion, cette conférence d'Abuja a démontré que l'Afrique n'est pas condamnée à suivre les modèles existants, mais qu'elle est capable de tracer sa propre voie numérique. Une voie qui conjugue souveraineté, innovation et respect des droits humains. Réussir ce pari nécessite une action coordonnée, un investissement soutenu dans les compétences et une mise en valeur des talents africains. La souveraineté numérique ne se décrète pas : elle se construit, collectivement, dans la durée , par des choix lucides et des partenariats durables. **M.S**

L'AUTORITÉ DE PROTECTION DES DONNÉES INSTITUE UNE CERTIFICATION DES COMPÉTENCES DES DPO

Par **Arnaud NADINGA**, Doctorant en droit privé du numérique

© ENVATO

Avec l'essor des traitements de données et l'importance croissante du droit des données personnelles en Afrique, le besoin de professionnels qualifiés dans ce domaine s'accentue. Un nombre croissant de pays impose désormais aux responsables de traitement répondant à des critères spécifiques la désignation d'un délégué à la protection des données (DPO). En réponse à cette exigence, des structures et individus sans compétences spécifiques s'autoproclament ou sont parfois parachutés DPO. Par ailleurs, la multiplication des offres de formation ne garantit pas toujours un niveau de qualité suffisant. Or, le DPO doit posséder des compétences professionnelles solides pour remplir ses missions d'information et de conseil auprès du responsable de traitement, ainsi que de contrôle de la conformité des opérations. Au Bénin, l'article 430, alinéa 5 du Code du numérique (CBN) précise d'ailleurs que sa désignation repose sur ses qualités professionnelles, lesquelles sont évaluées à l'aune de ses connaissances spécialisées en droit et pratiques de protection des données, ainsi que de sa capacité à exercer les missions définies à l'article 432 du CBN. Aussi, pour garantir au marché la disponibilité de compétences fiables, l'Autorité de protection des données (APDP) — après avoir instauré le label « APDP Approuvé » pour les formations — s'est attelée à certifier les compétences des DPO. Elle a adopté, le 13 juin 2024, la décision n° 2024-008/APDP/Pt/AP/CA/CTJ/SA destinée aux personnes physiques et morales de droit privé souhaitant exercer cette fonction. Cette décision a été légèrement modifiée en mars dernier (décision n° 2025-004/APDP/Pt/AP/CA/CTJ/SA du 31 mars 2025), rendant ainsi utile le retour sur les conditions de cette certification.

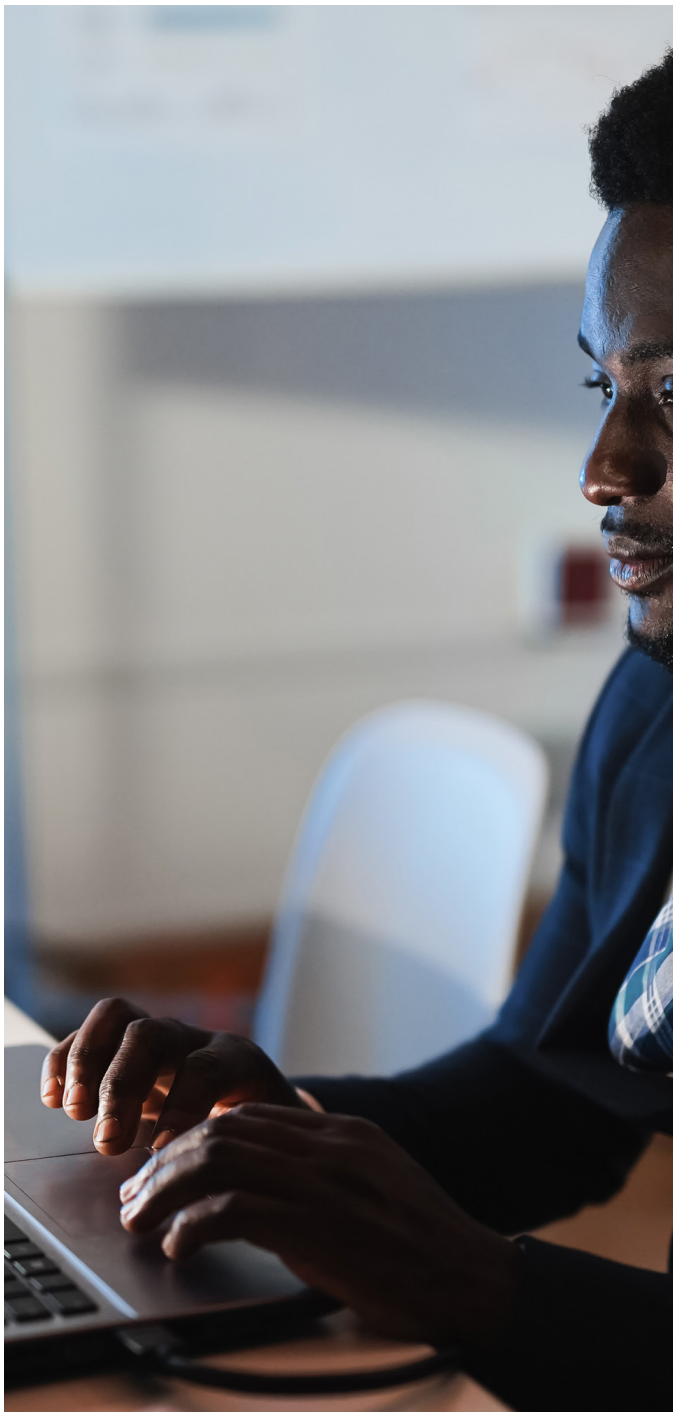
Une bataille rangée entre juristes et informaticiens : BAC + 5 en informatique ou en droit + une formation en droit des données personnelles

Pour l'exercice du métier de DPO, l'article 430, alinéa 5 du CBN semble privilégier les juristes en

précisant qu'il est évalué suivant sa connaissance du droit. Toutefois, il doit s'agir d'un « juriste augmenté », car il doit connaitre les « pratiques en matière de protection des données ». Cumulée aux exigences de ses missions, cette condition implique que le DPO doit aussi posséder des aptitudes en informatique. L'article 2 de la décision de 2024 avait amorcé cette orientation en mettant l'accent sur la formation en droit et en mentionnant la formation en informatique comme un simple « atout ». La nouvelle décision change cette approche. Le nouvel article 2 place les informaticiens et les juristes sur un pied d'égalité s'agissant des conditions préalables à la certification. La demande doit inclure « un diplôme ou une attestation BAC+5 en droit ou en informatique délivrés par un établissement d'enseignement reconnu par l'État ». Cette précision lève l'ambiguïté liée à la notion de « Master en droit » présente dans l'ancienne version. Pour les juristes, la spécialisation (droit privé, public, numérique ou droits humains) est secondaire, probablement en raison de la diversité des structures publiques et privées soumises à l'obligation de désigner un DPO (art. 430, al. 1 du CBN). Cependant, la seule maîtrise du droit ou de l'informatique ne suffit pas. Le candidat doit aussi justifier d'une formation en protection des données attestée par un diplôme ou une attestation. Aucune exigence n'est formulée quant à l'organisme formateur (public, privé, national ou étranger). Néanmoins, pour renforcer l'expertise locale, l'APDP valorise les formations labellisées « APDP Approuvé » (label instauré par décision n° 2022-001/APDP/Pt/SA du 27 avril 2022 modifiée par la décision n° 2025-005/APDP/Pt/AP/CA/CTJ/SA). Ainsi, la production d'un document délivré par un formateur labellisé, en activité au Bénin et disposant d'un label valide, constitue un atout pour l'obtention de la certification. Pour le reste, le dossier doit inclure un document d'identité, un casier judiciaire datant de moins de trois mois, un curriculum vitae et une preuve du paiement des frais d'étude du dossier (25 000 francs CFA).

Un sésame à 250 000 francs CFA pour une durée de deux (2) ans

L'examen de certification se déroule en présentiel, ce qui facilite le contrôle et limite les risques de fraude. L'épreuve, sous forme de questions à choix multiples et sélectionnée par le Président de l'APDP ou toute personne de son choix, est réalisée sur une application web permettant au candidat d'obtenir sa note instantanément. Elle est réussie si le candidat obtient au minimum 70 % de bonnes réponses. Le certificat, délivré après réussite à l'examen et paiement de 250 000 francs CFA, a une durée de validité limitée à deux ans. Ce délai permet de tenir compte de l'évolution des technologies et du droit du numérique, et oblige les DPO à actualiser régulièrement leurs connaissances. Il est renouvelable dans les mêmes conditions que celles précitées. À vos marques donc pour saisir ce sésame, gage de confiance tant pour votre entreprise que pour ses clients et partenaires. **A.N**



© ENVATO

L'AUTORITÉ DE PROTECTION DES DONNÉES MET EN DEMEURE 84 ORGANISATIONS POUR NON-RESPECT DES OBLIGATIONS DÉCLARATIVES

Par **Samiratou ISSA H.** Chargée Conformité - Protection des données

© ENVATO

Lors de sa première session ordinaire en février dernier, l'Autorité de Protection des Données Personnelles malienne (APDP) a prononcé des sanctions de mise en demeure contre un certain nombre de structures pour défaut d'accomplissement de formalité déclarative.

La formalité déclarative : De quoi s'agit-il ?

Contrairement à l'accountability prévue par le Règlement européen sur la protection des données et pareillement à certaines lois ouest-africaine (béninoise, nigérienne, sénégalaise, togolaise, etc.), la loi malienne N°2013-015 du 21 Mai 2013, modifié portant sur la protection des données à caractère personnel, consacre la déclaration des traitements de données personnelles auprès de l'APDP.
D'après le texte susvisé, par cette formalité, les responsables de traitement déclarent à l'Autorité de Protection des Données à caractère Personnel (ou « APDP »), les opérations qu'ils comptent mettre en œuvre, pour une finalité donnée. En outre, l'article 33 prévoit que la création de traitements informatiques doit faire l'objet de déclaration. Une question se pose dès lors : est-ce les seuls traitements concernés par cette formalité ? La réponse n'est pas évidente à la lecture du texte législatif.

Toutefois, le formulaire de déclaration normale disponible sur le site de l'APDP semble répondre par l'affirmative. En effet, il est destiné aux traitements portant sur les Systèmes d'information (géolocalisation, contrôle d'accès etc.), les fichiers et les bases de données (personnel, clients, visiteurs, élèves, etc.). En revanche, une demande d'autorisation est requise dans l'hypothèse où ces traitements concernent des données sensibles telles que des données de santé, biométriques , lorsque ces traitements font l'objet d'un transfert de données ou encore d'une interconnexion.

En outre, la loi malienne en son article 55, exclut du champ de la déclaration : les traitements des juridictions, des autorités publiques agissant dans le

cadre de leurs attributions légales, des organismes publics personnalisés et des collectivités territoriales.

La sanction attachée au défaut d'accomplissement de formalité déclarative

Pour rappel, ce n'est qu'après des années de sensibilisation auprès du public et des professionnels et au bout d'au moins cinq ans de fonctionnement que l'APDP a commencé à sanctionner des responsables de traitement. Cette stratégie, compte tenu du terrain, peut s'observer chez d'autres autorités de protection de la sous-région.

Tout d'abord, il est important de noter que la formalité déclarative permet d'avoir une vue globale des activités d'une structure donnée en ce qu'elle informe sur : le responsable de traitement et son éventuel représentant, la désignation du correspondant à la protection des données, les finalités du traitement, les données traitées (catégories de données, types de données, origine, durée de conservation, destinataires), la loyauté du traitement (à travers l'information des personnes concernées ou la collecte du consentement), la sécurité et la confidentialité des données ; ainsi que sur la mise en œuvre d'un traitement automatisé. C'est donc à juste titre que l'article 57 de la loi malienne prévoit que les responsables de traitement qui omettent, de mauvaise foi, d'accomplir cette formalité encourent une sanction administrative que l'APDP apprécie, en fonction de la gravité de la faute. Quels sont donc les critères qui permettent de caractériser cette mauvaise foi ? Cela reste vraisemblablement à l'appréciation de l'autorité.

Au chapitre des 84 structures sanctionnées, figurent des établissements de santé et même des ONG internationales. Il convient de souligner que les traitements de données mis en œuvre par ce type de structures sont pour la plupart sensibles ; sans oublier la problématique du transfert des données, vers un pays tiers, fort probable dans le cas des ONG internationales ; pouvant également relever du régime de la demande d'autorisation.

L'APDP a fait le choix de publier la liste des structures mises en demeure sur son site internet. Les responsables de traitement concernés sont tenus d'exécuter les dispositions de la mise en demeure dans le délai indiqué sous peine de sanction allant de 5 000 000 FCFA à 20 000 000 FCFA sans préjudice de la saisine du Procureur de la République du Pôle National de Lutte contre la Cybercriminalité pour l'application de sanctions pénales. Notons qu'aucune précision sur le délai n'est donnée dans la publication.

Cependant, très récemment, le 12 mai 2025 a été lancée la deuxième session extraordinaire de l'APDP au titre de l'année 2025. Il faut retenir que plus de 300 dossiers seront étudiés, notamment, des demandes de mise en conformité et des mises en demeure prononcées à l'encontre de structures pour défaut d'accomplissement des formalités déclaratives.

Enfin, la publication de la liste des structures sanctionnées témoigne de la volonté de l'Autorité de Protection malienne d'encourager les responsables de traitement qui sont conformes à rester sur cette voie et de rappeler à l'ordre ceux qui ne le sont pas.

Soulignons également que les réticences à l'accomplissement de cette formalité déclarative tiennent non seulement aux coûts qu'elle peut engendrer ; mais aussi à la faible prise de conscience quant à l'importance de la protection des données personnelles, qui loin d'être un sujet théorique et au vu de la prolifération des cybermenaces, nous touche chaque jour de plus près.

Des efforts de sensibilisation, de vulgarisation et de mise en conformité des structures, par l'APDP, sont à noter. Cependant, les défis quant à la formation et au renforcement des compétences des acteurs et correspondants en la matière sont à relever ; de sorte à pouvoir faire de la protection des données, un levier de confiance sur le marché national, régional voire international, mais d'abord et surtout auprès des citoyens. **S.I.H**

WWW.AFRICADATAPROTECTION.ORG
INFO@AFRICADATAPROTECTION.ORG