AFRICA DATA PROTECTION

RAPPORT SEMESTRIEL - JANVIER 2026

AFRICA DATA PROTECTION REPORT

Protecting data, empowering Africa

OUGANDA

Mise en demeure de la PDPO : Google sommé de se mettre en conformité

NIGÉRIA

Meta et la NDPC trouvent un accord pour mettre fin à leur litige sur la protection des données

ANGOLA

Consultation publique sur le projet de loi sur la régulation de l'intelligence artificielle

www.africadataprotection.org

English version

SOMMAIRE

3 Édito

5 Algérie
La loi sur la protection des données renforcée par de nouvelles mesures

6 Nigéria
Ouverture d'une enquête visant près de 1300 organisations pour non-conformité

7 Maroc
Dark Web : la CNDP déploie un nouvel outil de surveillance

8 Mali
Entrave à la mission de contrôle : sanction pécuniaire de 5 millions de francs CFA

9 Égypte
Première application de la loi sur la protection des données : un opérateur télécom condamné par un tribunal

10 Angola
Failles de sécurité : sanctions prononcées contre des institutions publiques

4 Ouganda
Mise en demeure de la PDPO : Google sommé de se mettre en conformité

11 Angola
Consultation publique sur le projet de loi sur la régulation de l'intelligence artificielle

12 Nigéria
Meta et la NDPC trouvent un accord pour mettre fin à leur litige sur la protection des données

13 Tanzanie
Vie privée : la PDPC sanctionne la persistance d'une violation de données

14 Afrique du Sud
Lancement d'une plateforme pour signaler les violations de données

15 Sénégal
Deepfakes : la CDP alerte sur les dangers de l'IA et appelle à une utilisation responsable

16 Kenya
La Haute Cour tranche sur la constitutionnalité des attributions de l'autorité de protection des données

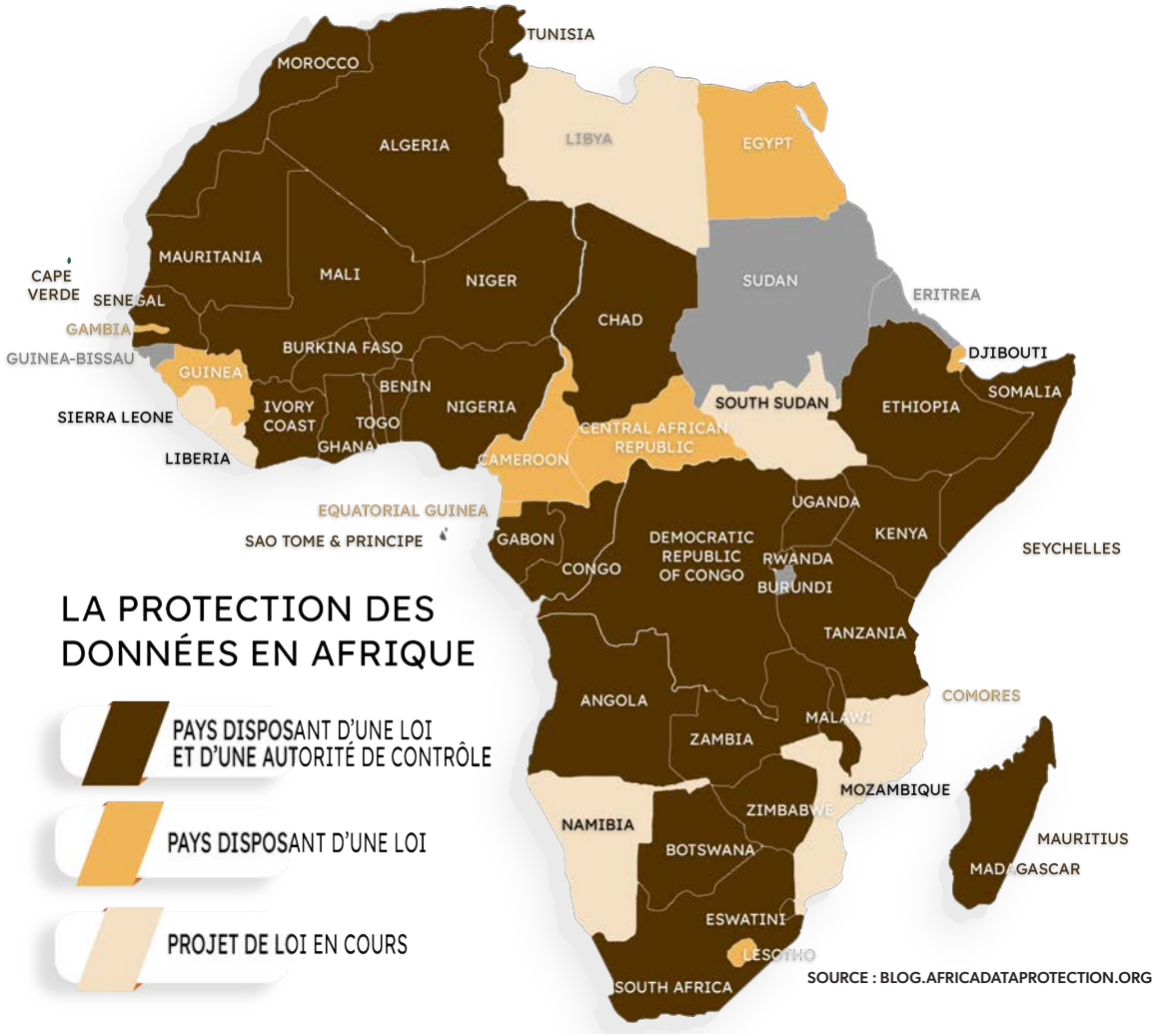
ÉDITO

Pour l'Afrique, l'année 2025 aura été le signe d'une accélération notable de la dynamique de protection des données personnelles et de la régulation de l'intelligence artificielle. L'entrée de Djibouti et de la Gambie dans le cercle des pays disposant d'une législation sur les données personnelles porte désormais à plus de quarante le nombre d'États africains dotés d'un cadre juridique en la matière. Cette évolution témoigne d'une maturité croissante face aux enjeux de la souveraineté numérique, de la protection des libertés et de la sécurité des citoyens dans un monde interconnecté.

Jules Hervé YIMEUMI
Président
d'Africa Data Protection

Sur le front de l'intelligence artificielle, 2025 a vu le continent abandonner son rôle de simple spectateur pour se saisir pleinement du sujet en tant qu'acteur. Des initiatives comme le projet de loi angolais reflètent l'ambition des États africains de tirer profit de cette avancée technologique majeure, tout en prévenant les risques inhérents et surtout l'imposition de standards extraterritoriaux. Bien qu'encore isolées, ces initiatives dessinent les contours d'un modèle de régulation qui se veut propre, alliant impératifs de développement socio-économique, protection des valeurs africaines ainsi que des libertés et droits fondamentaux des citoyens.

Pour autant, les défis restent immenses. L'effectivité des normes, l'harmonisation des législations, le renforcement des capacités locales à travers la formation des acteurs et l'accès équitable aux technologies demeurent des chantiers prioritaires. Le continent a certes démontré en 2025 qu'il pouvait innover dans la gouvernance des données et de l'IA ; l'enjeu post-2025 sera de traduire ces avancées en opportunités concrètes pour ses populations.



OUGANDA

MISE EN DEMEURE DE LA PDPO : GOOGLE SOMMÉ DE SE METTRE EN CONFORMITÉ

Par La rédaction

L'autorité ougandaise de protection des données (Personal Data Protection Office - PDPO) a rendu, le 18 juillet 2025, une décision à l'encontre Google LLC pour non-conformité à la législation relative à la protection des données. Cette décision fait suite à une plainte collective déposée par quatre citoyens ougandais, accusant le géant technologique de ne pas respecter les obligations légales locales. Elle s'appuie sur la Data Protection and Privacy Act, Cap 97 ainsi que sur les Data Protection and Privacy Regulations, qui encadrent la collecte, le traitement et le transfert des données à caractère personnel en Ouganda.

Les plaignants dénonçaient notamment l'absence d'enregistrement de Google auprès du PDPO, le transfert de leurs données personnelles vers des serveurs à l'étranger sans autorisation préalable, ainsi que l'impossibilité de contacter un représentant local de Google, ce qui les laissait sans recours face à leurs préoccupations.

Dans sa défense, Google avait soutenu que ses activités en Ouganda n'etaient pas soumises aux obligations légales locales, faute de présence physique dans le pays. Cependant, la PDPO a rejeté cet argument, rappelant que Google est un contribuable enregistré en Ouganda et tire des revenus substantiels des utilisateurs locaux. L'Autorité a estimé que le critère de présence économique suffisait à établir l'applicabilité de la loi ougandaise, même en l'absence d'établissement physique. Elle a donc conclu que Google agissait en tant que responsable de traitement, et qu'il était tenu de se conformer à la loi nationale.

La PDPO a ordonné à Google de s'enregistrer auprès de ses services dans un délai de 30 jours, de désigner un responsable de traitement pour l'Ouganda, et de fournir des preuves de conformité concernant ses transferts transfrontaliers de données. Bien qu'elle n'ait pas imposé de localisation des données, l'Autorité a rappelé que tout transfert international doit se conformer strictement aux dispositions de la loi ougandaise.

© ENVATO

ALGÉRIE

LA LOI SUR LA PROTECTION DES DONNÉES PERSONNELLES RENFORCÉE PAR DE NOUVELLES MESURES

Par La rédaction

L'algérie a adopté une nouvelle loi modifiant et complétant son cadre juridique en matière de protection des données personnelles, avec la publication au Journal officiel de la loi n° 25-11 du 24 juillet 2025. Ce texte, qui actualise la loi n° 18-07 de 2018, introduit des dispositions majeures pour répondre aux nouveaux défis numériques et sécuritaires, tout en renforçant les droits des citoyens et les obligations des acteurs publics et privés.

Des définitions modernisées pour mieux encadrer les technologies émergentes

La réforme apporte des précisions essentielles sur plusieurs définitions clés, intégrant désormais les données biométriques, le profilage, la pseudonymisation et la violation des données. Ces ajouts traduisent la volonté du législateur de s'adapter à l'évolution des technologies et aux risques associés, notamment ceux liés à l'usage croissant de la reconnaissance faciale ou à l'analyse comportementale.

Un renforcement institutionnel de l'Autorité nationale

Pour garantir un contrôle plus efficace, l'Autorité nationale de protection des données à caractère personnel (ANPDP) se voit dotée de pôles régionaux chargés d'effectuer des audits et des contrôles auprès des institutions et des organisations publiques et privées traitant des données à caractère personnel. Cette décentralisation vise à rapprocher l'action de l'Autorité sur le terrain, à assurer une meilleure couverture territoriale, et à améliorer la réactivité face aux incidents de sécurité.

Des obligations accrues pour les responsables de traitement

La loi rend désormais obligatoire la désignation d'un Délégué à la protection des données (DPD/DPO) par tout responsable de traitement et par les autorités compétentes. Ce dernier a pour mission d'informer, de conseiller et de former les équipes, tout en servant d'interlocuteur privilégié auprès de l'ANPDP. Les juridictions sont toutefois dispensées de cette obligation lorsqu'elles exercent leurs fonctions juridictionnelles.

Tenue de registres et études d'impact obligatoires

Les responsables de traitement devront désormais tenir un registre détaillé de leurs activités de traitement, incluant notamment les finalités poursuivies, les catégories de données collectées, les destinataires des informations, ainsi que les mesures de sécurité mises en place. Un carnet automatisé retraçant toutes les opérations effectuées sur les données (collecte, modification, effacement, etc.) devient également obligatoire. Par ailleurs, lorsqu'un traitement est susceptible d'engendrer des risques élevés pour les droits et libertés des personnes physiques, le responsable de traitement devra mener une étude d'impact.
Ces documents doivent pouvoir être présentés à tout moment à l'ANPDP, renforçant ainsi la transparence et la responsabilité.

Encadrement du transfert international des données

Le transfert de données vers un pays tiers ou une organisation internationale sera désormais soumis à une évaluation préalable du niveau de protection offert par le destinataire. En l'absence de garanties suffisantes, le transfert ne pourra avoir lieu que dans des cas exceptionnels, notamment pour la protection d'intérêts vitaux ou la prévention d'une menace grave à la sécurité publique.
Avec cette réforme, l'Algérie se dote d'un arsenal juridique plus robuste renforçant les droits des citoyens, et s'alignant progressivement sur les standards internationaux.

© ENVATO

NIGÉRIA

OUVERTURE D'UNE ENQUÊTE VISANT PRÈS DE 1300 ORGANISATIONS POUR NON-CONFORMITÉ

Par La rédaction

© ENVATO

L'autorité nigériane de protection des données (Nigeria Data Protection Commission - NDPC) a rendu publique, le 25 août 2025, la liste de près de 800 organisations visées par une enquête pour non-conformité à la législation sur la protection des données. Cette initiative s'inscrit dans le cadre de la mise en œuvre du Nigeria Data Protection Act (NDPA), adopté en juin 2023, qui a renforcé les pouvoirs d'enquête et de sanction de la NDPC.

Ces investigations visent à vérifier que les entités concernées peuvent fournir la preuve du dépôt de leur rapport d'audit de conformité pour 2024, qu'elles ont bien désigné un délégué à la protection des données (DPO) dont les coordonnées ont été communiquées à la NDPC, et qu'elles sont en mesure de présenter un résumé des mesures techniques et organisationnelles mises en œuvre pour protéger les données personnelles. Elles visent également à s'assurer que ces organisations sont dûment enregistrées en tant que responsables de traitement ou sous-traitants de données d'importance majeure, c'est à dire celles dont le volume ou la sensibilité présente un risque élevé pour les droits des personnes concernées.

Les organisations identifiées disposent d'un délai de 21 jours pour transmettre l'ensemble de ces informations. À défaut, elles s'exposent à des sanctions pouvant inclure des amendes administratives, des ordres d'exécution ou, dans certains cas, des poursuites pénales. Cette opération de contrôle massif illustre la volonté de la NDPC d'instaurer une culture de la conformité et de renforcer la confiance numérique au Nigeria.

MAROC

DARK WEB : LA CNDP DÉPLOIE UN NOUVEL OUTIL DE SURVEILLANCE

Par La rédaction

© ENVATO

L'autorité marocaine de protection des données (Commission Nationale de contrôle de la protection des Données à caractère Personnel - CNDP) a annoncé dans un communiqué de presse une avancée majeure dans sa lutte contre la diffusion illicite de données personnelles sur le darkweb. Grâce à un outil développé par une société spécialisée dans la cybersécurité, la CNDP peut désormais surveiller plus efficacement les publications non autorisées de données sensibles et agir en conséquence.

Cet outil permettra d'identifier rapidement les responsables de traitement concernés et de leur appliquer les dispositions prévues par la loi, notamment en cas de non-notification préalable de leurs traitements de données à la CNDP, conformément à la loi n°09-08. En effet, les traitements de données à caractère personnel doivent faire l'objet d'une déclaration préalable ou d'une demande d'autorisation préalable auprès de la CNDP. Aucun traitement ne peut être mis en œuvre sans la délivrance préalable d'un récépissé de la part de la CNDP.

La CNDP prévoit par ailleurs de renforcer son arsenal technologique en adoptant d'autres outils dans les mois à venir. Cette évolution témoigne de sa volonté de s'adapter aux défis croissants posés par la cybersécurité et de garantir une protection optimale des données personnelles.

MALI

ENTRAVE À LA MISSION DE CONTRÔLE : SANCTION PÉCUNIAIRE DE 5 MILLIONS DE FRANCS CFA

Par La rédaction

L'Autorité malienne de protection des données (Autorité de Protection des Données à Caractère Personnel - APDP) a infligé une amende administrative de 5 millions de francs CFA (environ 7500 euros) à une clinique privée. Cette sanction intervient après que l'établissement a entravé une mission de contrôle menée par l'APDP concernant un dispositif de vidéosurveillance installé illégalement, sans autorisation préalable. La décision s'appuie sur la Loi 2013-015 du 21 mai 2013 relative à la protection des données à caractère personnel.

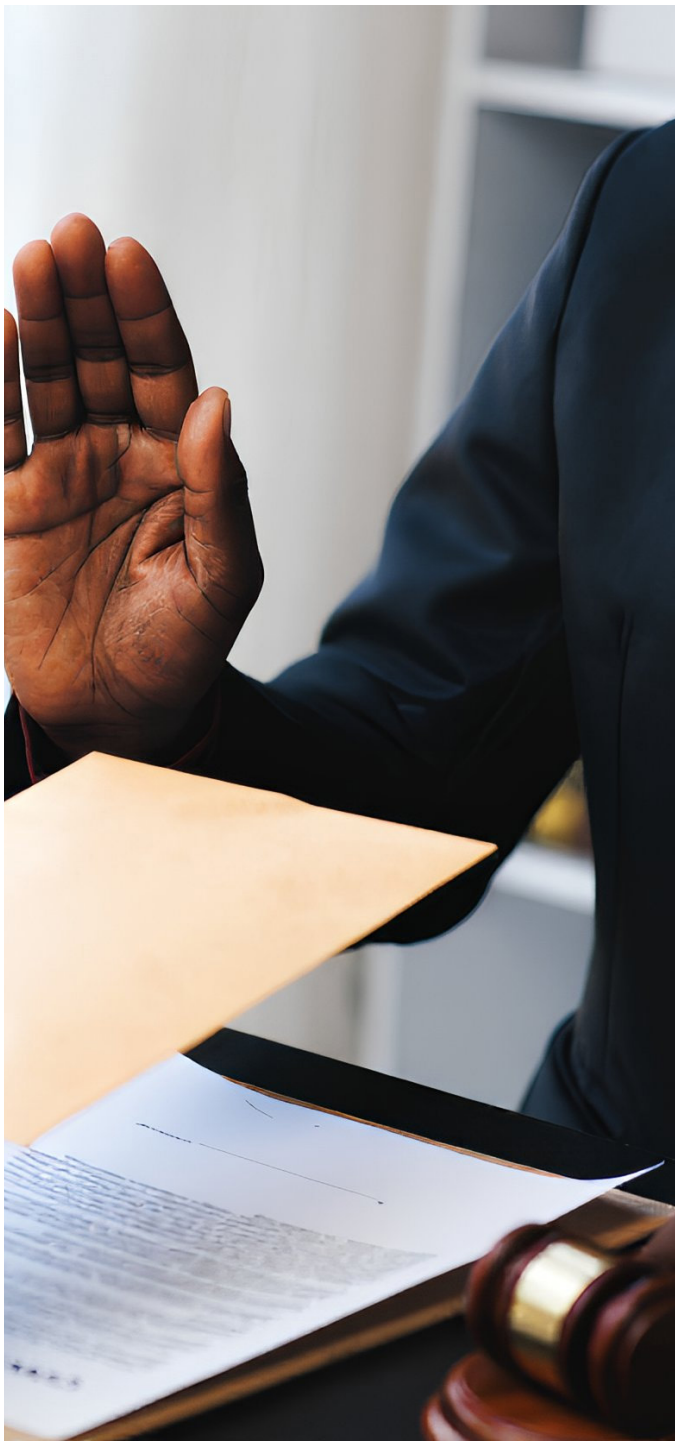
Un contrôle entravé, une sanction

Selon les informations communiquées par l'APDP, la clinique a fait obstacle à l'action des agents de l'autorité en refusant de coopérer lors d'une vérification sur place. L'article 65 de la Loi n°2013-015 du 21 mai 2013, telle que modifiée, prévoit des sanctions allant de 5 à 20 millions de francs CFA (environ 7 500 euros à 30 000 euros) pour toute entrave à l'action de l'APDP, notamment le refus de fournir des informations ou documents utiles à la mission, la dissimulation de preuves ou l'obstruction à un contrôle.
Dans ce cas précis, la clinique a été sanctionnée pour avoir empêché l'accès à un système de vidéosurveillance jugé non conforme à la réglementation en vigueur. L'APDP rappelle que toute installation de dispositifs de surveillance dans un espace public ou semi-public doit être, sous peine de sanctions, déclarée et autorisée conformément à la législation sur la protection des données personnelles.

Un rappel à l'ordre pour les établissements publics et privés

Cette décision s'inscrit dans une volonté de l'APDP d'affirmer son autorité et de renforcer le respect des règles relatives à la protection des données personnelles au Mali, en particulier dans le secteur de la santé où les traitements de données sensibles sont nombreux. Les établissements, qu'ils soient publics ou privés, sont tenus de se conformer aux exigences légales en matière de collecte, de traitement et de conservation des données.

L'APDP souligne que cette amende vise à rappeler aux acteurs concernés l'importance de la transparence et de la coopération avec les autorités compétentes.



© ENVATO

ÉGYPTE

PREMIÈRE APPLICATION DE LA LOI SUR LA PROTECTION DES DONNÉES : UN OPÉRATEUR TÉLÉCOM CONDAMNÉ PAR UN TRIBUNAL

Par La rédaction

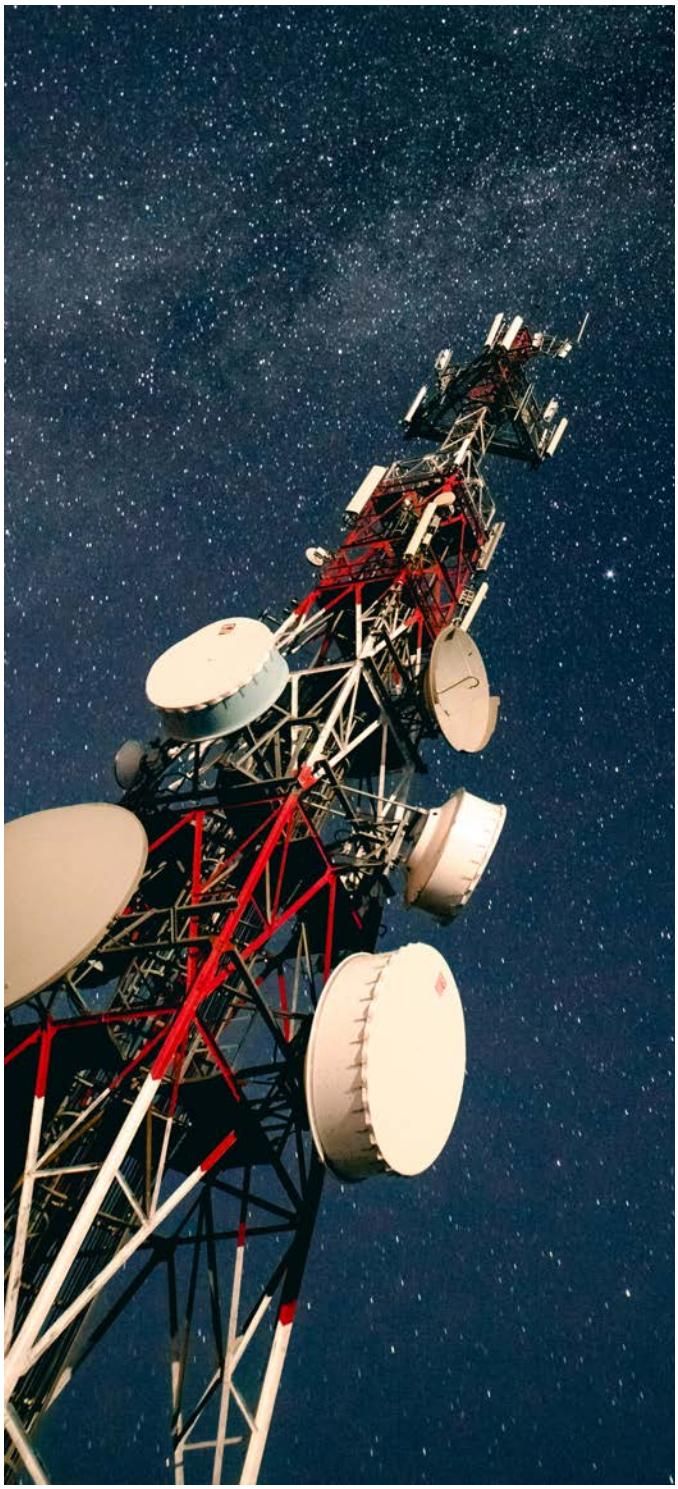
Pour la première fois depuis l'adoption de la loi sur la protection des données personnelles en 2020, un tribunal égyptien a condamné un opérateur télécom à verser une indemnisation record pour violation de la vie privée. Le 27 mai 2025, le Tribunal d'Alexandrie a ordonné à l'opérateur de payer environ 280 000 euros à une femme dont les données personnelles avaient été compromises après le remplacement frauduleux de sa carte SIM.

Un précédent judiciaire inédit

L'affaire remonte à novembre 2022, lorsque la plaignante, alors à l'étranger, a vu sa carte SIM remplacée sans son consentement. Des individus ont ainsi pris le contrôle de son compte WhatsApp et l'ont soumise à du chantage, l'obligeant à renoncer à des poursuites judiciaires qu'elle avait engagées contre une société immobilière à l'étranger. Malgré ses sollicitations, l'opérateur télécom a refusé de lui fournir une copie de son contrat téléphonique, poussant la victime à saisir la justice.
Le tribunal a retenu la responsabilité de l'opérateur, estimant que celui-ci avait manqué à ses obligations légales en matière de protection des données. La décision s'appuie sur plusieurs textes, dont la loi sur la protection des données personnelles (n°151 de 2020), la loi contre la cybercriminalité (n°175 de 2018), et la loi sur la protection des consommateurs (n°181 de 2018). Selon les juges, l'opérateur a non seulement échoué à sécuriser les données de sa cliente, mais a également violé son droit constitutionnel à la vie privée, garanti par l'article 57 de la Constitution égyptienne.

Des obligations légales ignorées

Le tribunal a souligné que la loi contre la cybercriminalité impose aux opérateurs de conserver les données des utilisateurs pendant 180 jours et de les protéger contre tout accès non autorisé. Or, dans ce cas, l'opérateur n'a pas su empêcher le remplacement frauduleux de la carte SIM, ni fournir les preuves nécessaires permettant d'écarter sa responsabilité. Alors que l'Égypte s'apprête à finaliser les décrets d'application de la loi sur la protection des données, ce jugement marque le début d'une ère de responsabilité accrue pour les acteurs du numérique.



© ENVATO

ANGOLA

FAILLES DE SÉCURITÉ : SANCTIONS PRONONCÉES CONTRE DES INSTITUTIONS PUBLIQUES

Par La rédaction

L'autorité angolaise de protection des données (Agência de Protecção de Dados - APD) a rendu publiques, le 22 septembre 2025, deux délibérations majeures condamnant une compagnie aérienne et une banque à des amendes pour manquements graves à la législation sur la protection des données personnelles. Ces sanctions, prononcées sur le fondement de la loi n°22/11 du 17 juin 2011 relative à la protection des données personnelles, marquent un tournant dans la lutte contre les infractions liées à la cybersécurité et à la confidentialité des informations sensibles en Angola.

La compagnie aérienne : une double condamnation pour négligence

Dans ses délibérations n°001 et n°002 datées du 10 septembre 2025, l'APD a infligé à la compagnie aérienne deux amendes distinctes. La première, d'un montant de 100 000 USD (cent mille dollars américains), sanctionne le défaut de mise en œuvre de mesures techniques et organisationnelles appropriées pour protéger les données personnelles d'un passager et de ses proches. La compagnie est également sanctionnée pour avoir traité les données de ses clients et employés sans notification ni autorisation préalable de l'ADP, en violation des obligations prévues par la Loi n°22/11.

La seconde amende, s'élevant à 75 000 USD (soixante-quinze mille dollars américains), sanctionne la négligence de la compagnie face à une cyberattaque par ransomware survenue le 15 septembre 2024, ayant provoqué la perte temporaire, l'accès non autorisé et la divulgation illicite d'informations sensibles. L'APD a rappelé que les responsables de traitement sont tenus d'assurer la sécurité des données personnelles contre tout risque de violation ou d'accès non autorisé.

Une banque également dans la ligne de mire

Lors d'une réunion extraordinaire tenue le 30 avril 2025, l'APD avait déjà condamné une banque à une amende de 75 000 USD pour des manquements similaires. L'établissement bancaire était accusé de ne pas avoir déployé les mesures de sécurité nécessaires pour protéger les données de ses collaborateurs lors d'une cyberattaque par ransomware, survenue le 10 février 2023.

Une atténuation des peines justifiée par la coopération

Malgré la sévérité des sanctions, l'APD a souligné que les montants des amendes avaient été réduis en raison de la coopération exemplaire des deux entités. Celles-ci ont en effet collaboré activement avec l'autorité pour établir les faits, tout en démontrant un engagement sérieux à améliorer leurs processus internes de sécurité et de conformité. Par ailleurs, l'absence d'antécédents en matière d'infractions à la protection des données a également constitué un facteur atténuant.

Un signal fort pour la protection des données en Angola

Ces décisions interviennent dans un contexte de recrudescence des cyberattaques et rappellent l'urgence, pour les entreprises et institutions angolaises, de renforcer leurs dispositifs de sécurité et de conformité. Elles traduisent également la volonté de l'APD d'affirmer son autorité et de faire respecter la loi, y compris à l'encontre d'acteurs économiques majeurs.

© ENVATO

ANGOLA

CONSULTATION PUBLIQUE SUR LE PROJET DE LOI SUR LA RÉGULATION DE L'INTELLIGENCE ARTIFICIELLE

Par La rédaction

© ENVATO

En septembre 2025, le ministère des Télécommunications, des Technologies de l'Information et de la Communication Sociale d'Angola a présenté une proposition de loi sur l'intelligence artificielle (IA). Ce texte, élaboré dans un contexte de transformation numérique accélérée, vise à établir un cadre juridique complet pour réguler le développement, l'utilisation et la supervision de l'IA en Angola. L'objectif est double : stimuler l'innovation technologique tout en protégeant les droits fondamentaux des citoyens, conformément aux valeurs constitutionnelles du pays.

La proposition s'appuie sur les articles 40, 54, 55 et 210 de la Constitution angolaise, qui garantissent notamment la liberté d'expression, la protection des données personnelles et la dignité humaine. Elle répond également à la Déclaration africaine sur l'IA, signée à Kigali en avril 2025, laquelle promeut une IA éthique, inclusive et alignée sur les objectifs de développement durable.

Le texte s'articule autour de 9 chapitres et 86 articles, couvrant des aspects tels que les dispositions générales, le développement et la promotion de l'IA, la protection des droits des utilisateurs, les obligations des développeurs et des fournisseurs, ainsi que la gouvernance et la supervision de l'IA.

En Afrique, des pays comme l'Égypte, le Kenya, le Sénégal et le Rwanda ont déjà adopté des stratégies nationales dédiées à l'IA, mais l'Angola se distingue en proposant un projet de loi intégrant des mécanismes de responsabilité civile, pénale et administrative.

NIGÉRIA

META ET LA NDPC TROUVENT UN ACCORD POUR METTRE FIN À LEUR LITIGE SUR LA PROTECTION DES DONNÉES

Par La rédaction

Le 30 octobre dernier, un accord de règlement a été conclu entre Meta (Maison mère de Facebook, Instagram et WhatsApp) et la Commission nigériane de protection des données (NDPC), mettant fin à un litige judiciaire qui opposait les deux parties depuis près de deux ans. L'accord a été homologué le 3 novembre 2025 par la Haute Cour Fédérale du Nigéria à Abuja.

Un litige distinct des autres sanctions

Il est important de souligner que cet accord concerne uniquement le différend entre Meta et la NDPC et n'a aucun lien avec la sanction infligée par la Commission fédérale de la concurrence et de la protection des consommateurs nigériane (FCCPC) en juillet 2024. On se souviens en effet que la FCCPC avait infligé à Meta une amende de 220 millions de dollars pour violation des législations sur la protection des données personnelles et la protection des consommateurs à travers la mise à jour en 2021 de la politique de confidentialité de WhatsApp. Les deux affaires, bien que liées à la régulation des activités de Meta au Nigeria, restent indépendantes sur le plan juridique et procédural.

Un litige né d'une enquête approfondie

Tout a commencé en septembre 2023, lorsque la NDPC a lancé une enquête sur les pratiques de Meta en matière de traitement des données personnelles au Nigeria. Les conclusions de cette enquête, publiées en février 2025, étaient accablantes : la Commission reprochait à Meta de ne pas obtenir le consentement explicite des utilisateurs nigérians pour le ciblage publicitaire comportemental, de transférer des données hors du pays sans autorisation, et de collecter les données de non-utilisateurs via ses plateformes. Parmi les mesures imposées figuraient une amende de 32,8 millions de dollars, ainsi que des obligations strictes, comme la réalisation d'une évaluation d'impact sur la protection des données et la mise à jour de sa politique de confidentialité.

Un compromis aux enjeux majeurs

Plutôt que de poursuivre les procédures judiciaires, les deux parties ont choisi la voie du dialogue. Meta a accepté de retirer sa plainte et de se conformer à plusieurs exigences, notamment, renforcer la transparence dans le traitement des données, collaborer avec des institutions éducatives, améliorer ses mesures techniques et organisationnelles pour protéger la vie privée.

En échange, la NDPC a annulé ses ordres initiaux et renoncé à les appliquer, tout en conservant son droit de surveiller le respect de la loi nigériane sur la protection des données.

© ENVATO

TANZANIE

VIE PRIVÉE : LA PDPC SANCTIONNE LA PERSISTANCE DE LA VIOLATION DE DONNÉES

Par La rédaction

L'autorité tanzanienne de protection des données (Personal Data Protection Commission - PDPC) a rendu une décision le 10 juillet 2025 en faveur d'un citoyen dont les photos et vidéos, publiées sans son consentement, continuaient de circuler sur les réseaux sociaux d'une entreprise. Une affaire qui soulève des questions sur la protection de la vie privée à l'ère numérique.

Un cas emblématique de violation de la vie privée

Un employé d'un cabinet d'avocats a porté plainte contre une entreprise accusée d'avoir publié des photos et vidéos de lui, prises dans un contexte privé, sur son compte Instagram entre février et avril 2023. Ces images, montrant le plaignant en état d'ébriété, ont été publiées sans son autorisation et ont eu des répercussions professionnelles : il a été suspendu de son emploi en août 2024, avant d'être réintégré après une enquête interne prouvant que les faits dataient d'avant son embauche.

Un débat juridique sur la rétroactivité de la loi

La Personal Data Protection Act (Cap. 44), entrée en vigueur le 1er mai 2023, protège les données personnelles des Tanzaniens. Cependant, les faits reprochés à l'entreprise remontent à une période antérieure à cette date. La PDPC a dû trancher : peut-on sanctionner une entreprise pour des actes commis avant l'adoption de la loi ?
Dans sa décision, la PDPC a rappelé que la loi ne s'applique pas rétroactivement, mais que la persistance d'une violation après son entrée en vigueur relève de son champ d'application. Elle invoque ainsi le principe de violation continue : bien que les publications initiales aient eu lieu avant mai 2023, leur maintien en ligne après l'entrée en vigueur de la loi constitue une atteinte persistante à la vie privée du plaignant. Elle a donc estimé que la plainte était recevable et que l'entreprise devait répondre de ses actes.

Une décision saluée, mais des limites persistantes

La PDPC a ordonné à l'entreprise de :
- Supprimer immédiatement toutes les photos et vidéos du plaignant de ses plateformes en ligne ;
- Verser une compensation financière de 20 millions de shillings tanzaniens (environ 7 500 euros) pour préjudice moral.

Cette décision marque une avancée dans la protection des données personnelles en Tanzanie, mais elle révèle aussi les défis posés par l'application rétroactive des lois. Pour les experts, elle envoie un signal fort aux entreprises : la protection de la vie privée ne peut être ignorée, même pour des faits anciens, si leurs conséquences perdurent.

Un appel à la vigilance collective

La PDPC a souligné que cette affaire n'était qu'un exemple parmi d'autres de pratiques abusives dans les bars et lieux de divertissement, où des clients sont filmés ou photographiés à leur insu. Une prise de conscience collective s'impose, tant pour les professionnels que pour le grand public.

© ENVATO

AFRIQUE DU SUD

LANCEMENT D'UNE PLATEFORME POUR SIGNALER LES VIOLATIONS DE DONNÉES

Par La rédaction

L'autorité sud-africaine de protection des données (Information Regulator) a lancé une plateforme en ligne dédiée au signalement des violations de données. Cette initiative, annoncée par un communiqué publié le 7 avril 2025, vise à moderniser et simplifier le processus de déclaration des violations de données à caractère personnel. Désormais, toutes les organisations publiques comme privées, sont tenues d'utiliser le portail eServices pour notifier toute violation de données, mettant ainsi fin à l'ancien système de signalement par courrier électronique. Cette réforme s'inscrit dans une volonté de renforcer la transparence, la traçabilité et l'efficacité dans la gestion des violations affectant les données à caractère personnel, conformément aux exigences de la loi sur la protection des données (Protection of Personal Information Act - POPIA).

Une obligation légale pour les responsables de traitement

La POPIA impose aux responsables de traitement de notifier immédiatement l'Information Regulator en cas d'accès non autorisé, de perte ou de divulgation illicite de données à caractère personnel. Jusqu'à présent, ces signalements pouvaient être transmis par courriel, mais depuis le 1er avril 2025, l'usage exclusif du portail eServices est devenu obligatoire pour toute notification de violation. Cette plateforme, accessible via le site officiel de l'autorité,permet aux organisations de déclarer les incidents de manière structurée et sécurisée. En plus de notifier l'autorité, les organisations doivent également informer les personnes concernées par la violation, sauf si leur identité ne peut être établie.

Un accompagnement renforcé pour faciliter la transition

Afin d'assurer une mise en œuvre fluide de ce nouveau dispositif, l'Information Regulator a publié un guide pratique détaillant la procédure d'inscription sur le portail, la soumission des rapports d'incidents et les bonnes pratiques en matière de notification. L'autorité a également mis en place des canaux d'assistance dédiés afin d'accompagner les responsables de traitement dans leurs démarches. Ces outils visent à soutenir les organisations dans leur conformité et à garantir une application homogène de la POPIA sur l'ensemble du territoire.

Une avancée majeure pour la protection des données

La mise en place de cette nouvelle plateforme représente une avancée significative dans la consolidation du cadre sud-africain de protection des données. En centralisant les signalements de violations, l'Information Regulator espère améliorer la surveillance et la détection des violations des données, analyser les tendances en matière de cybersécurité et renforcer la protection des droits des individus ainsi que la prévention des incidents futurs. Cette centralisation favorisera une meilleure coordination entre les organisations et l'autorité, permettant une réponse plus rapide, plus cohérente et plus efficace face aux compromissions de données personnelles.

© ENVATO

SÉNÉGAL

DEEPFAKES : LA CDP ALERTE SUR LES DANGERS DE L'INTELLIGENCE ARTIFICIELLE ET APPELLE À UNE UTILISATION RESPONSABLE

Par La rédaction

Dans un communiqué publié en octobre 2025, l'autorité sénégalaise de protection des données (Commission de Protection des Données Personnelles - CDP) a exprimé sa vive préoccupation face à la prolifération, sur les réseaux sociaux, de vidéos et d'images générées par intelligence artificielle (IA). Ces contenus, souvent destinés à manipuler l'opinion publique ou à porter atteinte à la réputation de personnalités publiques, de guides religieux ou de simples citoyens, constituent selon la CDP une menace sérieuse pour la dignité humaine et la cohésion sociale. L'autorité rappelle que de telles pratiques sont susceptibles d'entraîner des sanctions pénales et administratives, et qu'elles portent gravement atteinte aux droits fondamentaux, notamment à la vie privée et à la protection des données personnelles.

Deepfakes et collecte abusive : des risques multiples pour les citoyens

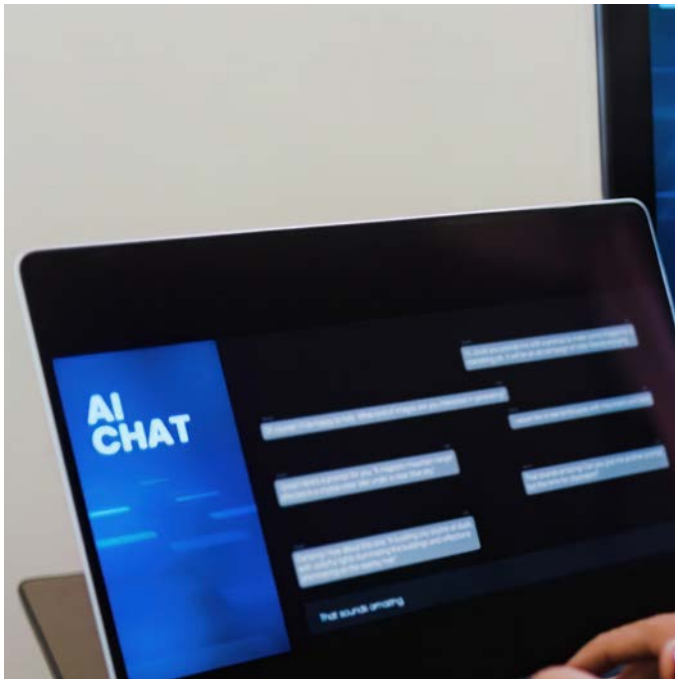
Parmi les dangers mis en avant par la CDP figurent la collecte et l'exploitation massive de données personnelles sans consentement, ainsi que les risques d'usurpation d'identité, de manipulation de l'information et d'atteinte irréversible à la réputation. L'émergence des deepfakes, ces contenus hyperréalistes mais falsifiés et trompeurs générés par IA, accentue le danger en brouillant la frontière entre réalité et fiction et en sapant la confiance au sein de la société. Selon la CDP, ces dérives technologiques, si elles demeurent non encadrées, risquent de fragiliser le vivre-ensemble, en favorisant la manipulation et la propagation de fausses informations à grande échelle.

Appel à une utilisation éthique et responsable de l'intelligence artificielle

Face à ces enjeux, la CDP appelle à une utilisation éthique, responsable et transparente des outils d'IA. Elle invite les citoyens à redoubler de vigilance avant de partager des contenus générés par IA, en vérifiant leur authenticité et leur provenance. Les créateurs de contenus, quant à eux, sont exhortés à éviter toute manipulation susceptible de porter atteinte aux valeurs religieuses, culturelles ou personnelles d'autrui. Les plateformes numériques, pour leur part, doivent renforcer leurs mécanismes de détection et de signalement des contenus illicites, trompeurs ou nuisibles, afin d'en limiter la diffusion et l'impact.

La CDP réaffirme son rôle de régulateur et de sensibilisation

Dans son communiqué, la CDP réaffirme son engagement à la mise en œuvre de la loi n°2008-12 du 25 janvier 2008 sur la protection des données personnelles et rappelle qu'elle poursuivra ses efforts de sensibilisation auprès du public, des institutions et des entreprises. L'autorité entend également adapter son cadre d'action aux nouveaux défis posés par l'IA générative, afin d'assurer un équilibre entre innovation technologique, respect de la vie privée et préservation des valeurs sociales et culturelles sénégalaises.



© ENVATO

KENYA

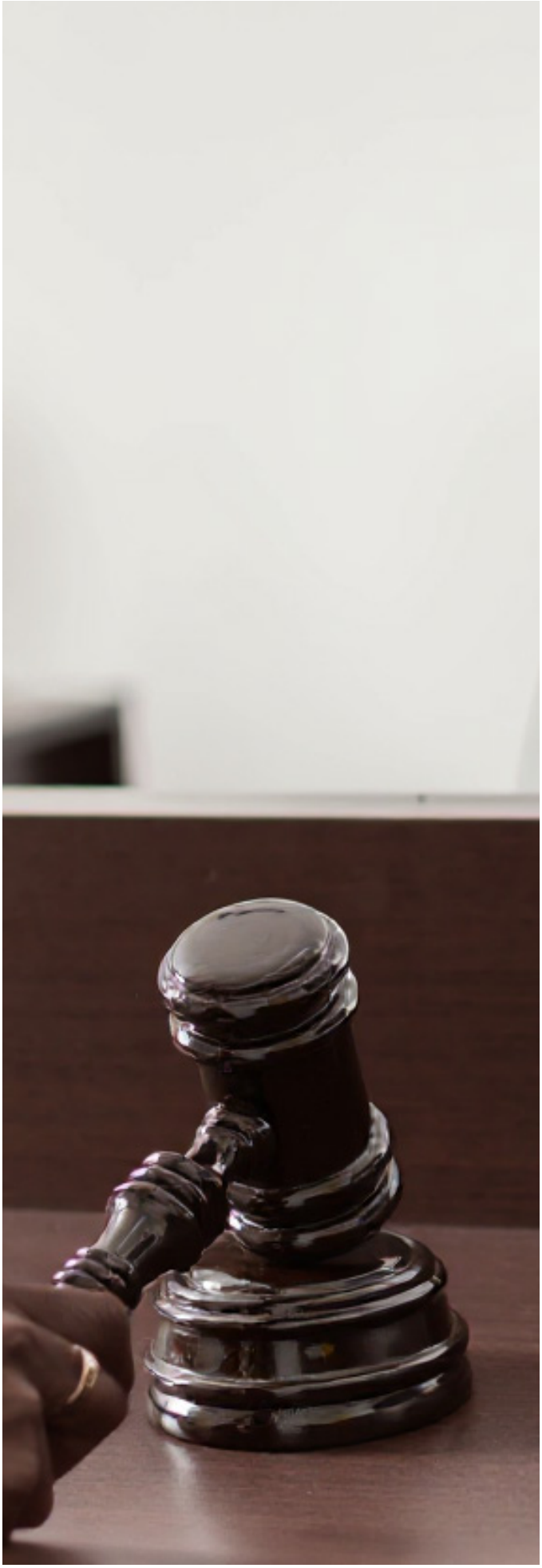
LA HAUTE COUR TRANCHE SUR LA CONSTITUTIONNALITÉ DES ATTRIBUTIONS DE L'AUTORITÉ DE PROTECTION DES DONNÉES

Par **Arnaud NADINGA,** Docteur en droit privé

Les autorités de protection constituent un rouage essentiel du mécanisme de protection des personnes à l'égard des traitements de données à caractère personnel. Chargées de donner plein effet à la législation dédiée, le choix de leur statut est crucial : elles doivent disposer de tous les moyens juridiques et présenter les garanties nécessaires de compétence, d'indépendance et d'impartialité. Véritables autorités de régulation, elles se distinguent des autres autorités administratives par l'absence de subordination hiérarchique ou de tutelle, sans pour autant être érigées en juridictions. Ce positionnement hybride est essentiel. Outre les assurances d'impartialité et d'indépendance vis-à-vis de l'exécutif, il présente le double mérite de préserver l'intégrité des compétences juridictionnelles en évitant tout empiètement et de prévenir la reproduction des lenteurs de la justice, dans une matière qui requiert une grande célérité. Ce statut s'est matérialisé par la figure de l'autorité administrative ou publique indépendante, un modèle qui s'est imposé malgré le débat qu'il suscite quant à sa légitimité, particulièrement au sujet de sa compatibilité avec la stricte séparation des pouvoirs judiciaire et exécutif.

C'est précisément cette tension autour de la légitimité de l'autorité de protection des données du Kenya (Office of the Data Protection Commissioner – ODPC) qu'a dû trancher la Division constitutionnelle et des droits de l'Homme de la Haute Cour du Kenya à Milimani, le 12 août 2025. Par requête n° E010 du 02 février 2025, il lui a été demandé, d'une part de déclarer inconstitutionnels l'article 56 de la loi sur la protection des données (Data Protection Act – DPA) et l'article 14 (5) du Règlement sur les procédures de traitement des plaintes et d'exécution (Data Protection [complaints handling and enforcement procedures] Regulations, 2021). Deux moyens sont avancés au soutien de cette prétention. Le requérant a soutenu en premier lieu que seule la Haute Cour serait habilitée, en vertu des articles 23 (1) et 165 (3) (b) de la Constitution, à statuer sur les questions relatives à la violation de la Déclaration des droits et à ordonner des mesures de réparations pour violation de la vie privée. Reconnaitre à l'ODPC le pouvoir de trancher des litiges relatifs à la vie privée reviendrait donc à empiéter sur les attributions de la Haute Cour. En second lieu, accorder à l'ODPC le pouvoir de prendre des décisions contraignantes et exécutoires, incluant la possibilité d'ordonner des mesures correctives et d'accorder une indemnisation, contreviendrait, selon lui, au principe de la séparation des pouvoirs. D'autre part, la Cour était invitée à déclarer que le mandant de l'ODPC chevauche celui de la Commission nationale des droits de l'homme et de l'égalité du Kenya (Kenya National Human Rights and Equality Commission – KNHREC), expressément habilitée en vertu de l'article 59 de la Constitution à enquêter sur les violations des droits de l'Homme.

En réplique, l'ODPC, première défenderesse, a fait valoir qu'elle est un organe statutaire spécialisé créé pour donner effet au droit fondamental à la vie privée, particulièrement pour contrôler les traitements de données personnelles. De plus, ses attributions et pouvoirs résultant des articles 5, 8 (1) (f), 56, 58 et 65 de la DPA et qui lui permettent de recevoir et de traiter les plaintes, de prendre des décisions et de délivrer des notices d'exécution, seraient de nature administrative et quasi-juridictionnelle, mais non juridictionnelle. Par ailleurs, en vertu de l'article 64 du DPA, ses décisions sont soumises au contrôle de la Haute Cour par voie d'appel, garantissant ainsi leur conformité à la constitution. Le modèle ne serait du reste pas inédit, puisque c'est la même configuration qui est retenue pour les autorités de régulation du secteur des communications et de la concurrence.



© ENVATO

Le ministère public, second défendeur, s'est aligné sur cette position, précisant au passage que les fonctions de l'ODPC seraient également admises à la lumière du principe de l'épuisement des voies de recours et du principe de la retenue constitutionnelle. La partie intervenante, la Data Privacy and Governance Society of Kenya, a quant à elle insisté sur la légitimité technique de l'ODPC en raison de son expertise technique et sur la nécessité de disposer de recours spécialisés et accessibles en matière de protection de données.

La question posée à la Haute Cour portait donc sur la constitutionnalité des attributions de l'ODPC en matière de protection du droit à la vie privée, avec en filigrane la tension avec le principe constitutionnel de la séparation des pouvoirs. Dans son jugement (en premier ressort), la Haute Cour a conclu que le cadre juridique fourni par la DPA, tel qu'actuellement formulé, est suffisamment constitutionnel, fonctionnel et nécessaire pour garantir effectivement le droit à la vie privée (pt. 60). Le modèle de l'ODPC a donc été validé, le juge ayant considéré que ses attributions quasi-juridictionnelles sont constitutionnelles, car elles sont celles d'un organe spécialisé, dont les décisions restent soumises au contrôle du juge. Cette décision légitime les attributions de l'ODPC (I) et clarifie sa position au sein du dispositif constitutionnel kényan (II).

I - La consécration de la légitimité des attributions de l'ODPC

Le juge a reconnu que les attributions de l'autorité de protection sont celles d'une autorité administrative aux pouvoirs quasi-juridictionnels (A) et dont les missions sont justifiées par son expertise technique (B).

A - Une autorité administrative aux pouvoirs quasi-juridictionnels

La Haute Cour a tout d'abord rejeté l'argument selon lequel l'ODPC empiète sur son domaine exclusif de compétence. Selon elle, l'ODPC « constitue plutôt un mécanisme important et conforme à la Constitution pour la mise en œuvre du droit à la vie privée [...], sous

réserve de la compétence de contrôle de la Haute Cour, telle que préservée par l'article 64 de la DPA. » (pt. 25). Ainsi, bien que l'article 23 (1) de la Constitution confère à la Haute Cour le pouvoir de statuer sur les violations de la Déclaration des droits, cela ne signifie pas que tout litige impliquant un droit fondamental doive nécessairement être initié devant elle. Pour elle, le fait que les décisions de l'ODPC soient susceptibles d'appel devant la Haute Cour garantit le respect des attributions de cette dernière. L'existence de l'ODPC n'offrirait que des recours administratifs pour donner effet au droit fondamental, à côté du contrôle juridictionnel prévu à l'article 64 de la DPA qui garantit le respect de la suprématie de la Haute Cour. Par ailleurs, l'ODPC ne rendrait pas de décisions définitives en matière de violations de la vie privée et ses décisions ne seraient pas des jugements. Elle agit plutôt, selon la Cour, comme un régulateur ou un organisme quasi-juridictionnel remplissant un rôle complémentaire au sein du cadre global institué par la Constitution. Les articles 56 de la DPA et 14(5) du Règlement « ne confèrent pas de pouvoir juridictionnel à l'ODPC, mais autorisent des fonctions administratives et règlementaires en application de l'article 31 de la Constitution. [Ils] fournissent les attributions nécessaires à une agence spécialisée tout en maintenant des garanties judiciaires par le biais du contrôle en appel par la Haute Cour » (pts. 26 et s.). La Cour souligne que, même si l'ODPC est habilité à prendre des décisions contraignantes, toute décision contraignante n'implique pas nécessairement l'exercice d'un pouvoir juridictionnel : le critère déterminant est l'interprétation et l'application concluantes de la Constitution (pt. 35). Or, les pouvoirs de l'ODPC n'atteignent pas ce seuil. Ils sont de nature investigatoire et régulatoire, visant à assurer le respect de la DPA. Les décisions de l'autorité de protection ne sont pas des « jugements » au sens strict, mais des actes administratifs. Du reste, bien que l'ODPC puisse prescrire des mesures correctives et ordonner le versement d'une indemnisation au profit du plaignant, ces mesures ne constituent pas des déclarations de droits au sens de l'article 23 (3) (a) de la Constitution, mais des mesures administratives prévues par la loi contre un

© ENVATO

© ENVATO

droit d'appel. Lequel droit d'appel préserve le contrôle constitutionnel de la Haute Cour et garantit la suprématie de la fonction judiciaire. Le jugement s'appuie par ailleurs sur la jurisprudence sud-africaine relative à l'information Regulator établi par le Protection of Personal Information Act (POPIA), pour rappeler qu'un organe administratif spécialisé peut détenir des pouvoirs quasi-juridictionnels sous réserve d'un contrôle judiciaire, sans violer la séparation des pouvoirs. Enfin, les attributions de l'ODPC s'inscriraient dans le sens de l'article 159 (2) (c) de la Constitution qui, pour réaliser l'objectif constitutionnel d'une justice rapide et abordable, encourage les mécanismes alternatifs de règlement des différends, lesquels incluraient les organes statutaires dotés de mandats quasi-juridictionnels. Pour autant, il faut signaler que ce pouvoir reconnu à l'ODPC d'accorder une indemnisation des préjudices individuels ne se rencontre pas dans tous les systèmes. Il est souvent réservé au juge, notamment dans les pays francophones ; l'autorité de protection statuant dans l'intérêt de la loi et ne pouvant alors infliger que des sanctions administratives.

B - Une autorité administrative aux compétences spécialisées

La Cour a insisté sur la nécessité d'institutions spécialisées dotées de l'expertise technique nécessaire pour gérer des plaintes d'une nature particulière. La légitimité de l'ODPC découle principalement de son efficacité et de sa capacité à agir là où les structures traditionnelles sont moins adaptées. La Cour a ainsi repris à son compte l'idée, soulevée par la partie intervenante, selon laquelle la complexité des litiges en matière de données personnelles justifie l'intervention d'un organe doté d'une compétence technique pointue. Est rappelée à ce titre, la jurisprudence Rich Productions Ltd v Kenya Pipeline Co.[2014] eKLR selon laquelle « La raison pour laquelle la Constitution et la loi établissent différentes institutions et différents mécanismes pour le règlement des litiges dans divers secteurs est de garantir que les litiges qui pourraient survenir soient résolus par ceux qui possè-

dent l'expertise technique et la compétence pour les traiter ». L'intervention de l'autorité spécialisée permet, outre ses compétences techniques, d'éviter des lenteurs procédurales dans des domaines qui requièrent célérité (l'article 56 [5] de la DPA impose à l'ODPC de traiter les plaintes dans un délai maximal de 90 jours).

II - La délimitation du rôle de l'ODPC au sein du dispositif constitutionnel

Le juge s'est ensuite attaché à définir la place de l'ODPC dans le paysage institutionnel en montrant que son action est encadrée par le contrôle du juge (A) et s'articule de manière cohérente avec les autres organes de protection des droits (B).

A - Un pouvoir encadré par le contrôle du juge

L'argument central de la constitutionnalité du modèle est la possibilité d'exercer un appel contre les décisions de l'ODPC telle que prévue à l'article 64 de la DPA. Pour la Cour, les missions de l'ODPC se justifient, sous réserve du contrôle de la Haute Cour. Le droit d'appel préserve ce contrôle et garantit la suprématie de la fonction juridictionnelle. Le contrôle juridictionnel est également renforcé par l'application des principes « d'épuisement des voies de recours » et de « retenue constitutionnelle ». Le principe d'épuisement des voies de recours, fondé notamment sur l'article 159 (2)(c) de la Constitution et la section 9 (2) du Fair Administrative Action Act (FAAA) impose aux tribunaux de s'abstenir d'examiner les litiges à moins que les procédures administratives prescrites aient été suivies (pt. 40). Autrement dit, une personne ne peut demander un contrôle juridictionnel tant que les mécanismes légaux disponibles n'ont pas été épuisés, sauf si le tribunal l'en exempte dans des circonstances exceptionnelles (recours inefficace, traitement partial ou manifestement injuste). C'est un principe qui impose un règlement ordonné des litiges et garantit que les organismes spécialisés aient la possibilité d'exercer leurs mandats. Une saisine préalable de l'autorité de protection est donc imposée

© ENVATO

avant tout recours au juge en matière de protection des données. Quant au principe de la « retenue constitutionnelle », il implique que la Haute Cour ne doit examiner une question constitutionnelle que si le litige ne peut être résolu par d'autres moyens. Cette articulation, conforme à la jurisprudence Kirimi & Another v Mobi Changa Ltd (2023), souligne la complémentarité entre recours administratif et contrôle judiciaire. Il faut tout de même noter que l'application de ces principes dans le cadre d'une requête en constitutionnalité est étonnante.

B - Une compétence complémentaire à celles des autres institutions de protection des droits de l'Homme

Pour le requérant, compte tenu du fait que l'article 59 (2) (e) de la Constitution crée déjà la KNHREC et lui reconnait le pouvoir d'enquêter sur les plaintes de violations des droits de l'Homme, le mandat de l'ODPC chevaucherait ou entrerait en conflit avec les attributions de cette Commission. Endossant la position des défendeurs et de la partie intervenante, la Cour reconnait tout d'abord que l'ODPC est une autorité spéciale attributaire d'un mandat spécial de veiller au respect des législations sur la protection des données, lesquelles ont été adoptées en application de l'article 31 (c) et (d) de la Constitution, alors que la KNHREC a une fonction plus large de surveillance des droits de l'Homme. Ensuite, conformément à l'article 21 (3) de la Constitution, qui exige de tous les organes de l'État qu'ils répondent aux besoins des groupes vulnérables et développent des cadres qui favorisent la réalisation des droits, la création de l'ODPC est non seulement constitutionnelle, mais nécessaire pour assurer un mécanisme d'application ciblé et expert pour la protection des données. Les mandats des deux commissions seraient donc plutôt complémentaires. Pour la Cour, bien que les deux institutions puissent incidemment traiter du même droit fondamental, leurs mandats ne sont pas en conflit. La KNHREC fonctionne comme un organe constitutionnel responsable de la surveillance générale, du plaidoyer et des enquêtes sur les violations des droits de l'Homme, alors que l'ODPC est un régulateur

© ENVATO

© ENVATO

statutaire spécialisé assurant une surveillance technique sur la protection des données et les questions de confidentialité numérique. Et, la jurisprudence a déjà reconnu que la mise en œuvre du droit à la vie privée nécessite des institutions d'application à la fois générales et sectorielles et surtout que pour ce faire, il y a nécessité d'établir un cadre qui inclut une surveillance spécialisée sur les questions de plus en plus complexes entourant la gouvernance des données, y compris la collecte, le stockage et l'utilisation des informations personnelles. Elle a ajouté que la Constitution elle-même permet la décentralisation et la délégation fonctionnelles. L'article 186 (2) et la quatrième annexe de la Constitution envisagent le partage des responsabilités entre les institutions à différents niveaux de gouvernement et entre différents organes. Par conséquent, le chevauchement fonctionnel seul n'est pas inconstitutionnel à moins qu'il n'entraîne une contradiction juridique ou une paralysie juridictionnelle. Or, le requérant n'a montré aucun cas de conflit direct entre l'ODPC et la KNHREC et il n'a pas non plus produit de preuve d'une plainte traitée par les deux organes simultanément ou de manière incohérente. « Par conséquent, la [Haute] Cour estime que le mandat de l'ODPC n'entre pas illégalement en conflit ou ne chevauche pas celui de la KNHREC. Au contraire, les deux institutions sont conçues pour se compléter au sein de l'architecture constitutionnelle et statutaire du Kenya pour l'application des droits de l'Homme » (pt. 58). L'existence de l'ODPC « ne déroge pas à l'autorité ou au mandat de la KNHREC, mais fournit une voie nécessaire, experte et ciblée pour traiter les plaintes relatives à la vie privée dans un contexte numérique en rapide évolution » (pt. 59).

Conclusion

C'est une décision qui devrait rassurer les autorités de protection quant à la légitimité de leurs attributions. La leçon principale est que le modèle de l'autorité administrative indépendante dotée de pouvoirs règlementaires et de sanction n'est pas intrinsèquement contraire au principe de la séparation des pouvoirs. Sa légitimité découle du fait qu'avec ses

KENYA

garanties de compétence, d'indépendance et d'impartialité, il contribue à donner un effet concret à un droit fondamental (le droit à la vie privée) dans le domaine technique et complexe de la protection des données tout en restant sous le contrôle d'une haute juridiction. Cette jurisprudence kényane s'inscrit dans une tendance africaine plus large vers la reconnaissance d'autorités de régulation dotées de compétences spécialisées et quasi-juridictionnelles, à l'instar de l'Information Regulator d'Afrique du Sud, et renforce la solidité du cadre institutionnel de la protection des données sur le continent. Elle tranche une autre question cruciale : le rapport entre autorités de protection et Commissions Nationales des Droits de l'Homme que beaucoup d'États africains connaissent. La précision quant à la complémentarité de leurs mandants permet d'éviter les conflits de compétence et de créer un écosystème de protection où chaque institution a un rôle défini.

© ENVATO

WWW.AFRICADATAPROTECTION.ORG
INFO@AFRICADATAPROTECTION.ORG
© COPYRIGHT JANVIER 2026 - AFRICA DATA PROTECTION - TOUS DROITS RÉSERVÉS