AFRICA DATA PROTECTION

REPORT

DEC. 2024

LE NIGÉRIA INFLIGE À META UNE AMENDE RECORD DE 220 MILLIONS DE DOLLARS US : DECRYPTAGE D'UNE SANCTION HISTORIQUE
PAGE 7

LES DONNÉES DE SANTÉ EN AFRIQUE SUB-SAHARIENNE : DÉFIS, RISQUES ET OPPORTUNITÉS
PAGE 11

ÉDITO : HARMONISATION DE L'ENCADREMENT DES DONNÉES PERSONNELLES EN AFRIQUE : DE LA STRATÉGIE CONTINENTALE AUX INITIATIVES SOUS-RÉGIONALES
PAGE 5

AFRICA DATA PROTECTION

SOMMAIRE

AVANT-PROPOS 03

ÉDITO 05

LE NIGÉRIA INFLIGE À META (EX FACEBOOK) UNE AMENDE RECORD DE 220 MILLIONS DE DOLLARS US : DÉCRYPTAGE D'UNE SANCTION HISTORIQUE ! 07

LES DONNÉES DE SANTÉ EN AFRIQUE SUB-SAHARIENNE : DÉFIS, RISQUES ET OPPORTUNITÉS 11

L'AUTORITÉ DE PROTECTION DES DONNÉES DU NIGER PUBLIE SON RAPPORT ANNUEL 2023 : QUE FAUT-IL RETENIR ? 15

ARPTIC/ARPTC INVESTIT DES MISSIONS DE L'AUTORITÉ DE PROTECTION DES DONNÉES EN RD-CONGO 17

AVANT-PROPOS

Jules Hervé YIMEUMI
President of Africa Data Protection association

Ces derniers mois, la protection des données à caractère personnel en Afrique connaît des avancées marquantes, témoignant de la prise de conscience croissante des gouvernements et des institutions locales quant à l'importance de garantir la sécurité et la confidentialité des données des citoyens.

En Éthiopie, l'entrée en vigueur de la nouvelle loi sur la protection des données marque un tournant significatif pour le pays, le plaçant parmi les États engagés dans la défense des droits des individus face aux usages des technologies de l'information. Au Botswana, la publication du projet de loi visant à remplacer la législation existante en matière de protection des données reflète une volonté d'adaptation aux évolutions rapides de l'environnement numérique mondial. Au Cameroun, le projet de loi sur la protection des données à caractère personnel a été présenté au Parlement, témoignant d'une dynamique similaire en faveur de la régulation des pratiques numériques.

Par ailleurs, la récente sanction imposée à Meta au Nigéria montre la vigilance accrue des régulateurs africains à l'égard des géants technologiques et illustre l'importance d'assurer un traitement responsable des données personnelles par les multinationales. Enfin, au Bénin, l'Autorité de Protection des Données Personnelles (APDP) a récemment précisé les exigences pour la certification des compétences du Délégué à la Protection des Données (DPD), soulignant la nécessité de compétences spécifiques et de qualifications pour les professionnels de ce domaine.

Ces mesures récentes témoignent de l'effort coordonné de nombreux pays africains pour développer un cadre solide et efficace de protection des données personnelles, en phase avec les préoccupations croissantes en matière de droit du numérique et de souveraineté numérique sur le continent.

AWARDS

APPEL À CONTRIBUTION OUVERT AUX ÉTUDIANT(E)S, CHERCHEUR(E)S, PROFESSIONNEL(LE)S, UNIVERSITAIRES, ENTREPRENEUR(E)S, ETC., SE DISTINGUANT PAR LEUR TRAVAIL INNOVANT SUR LES QUESTIONS D'INTELLIGENCE ARTIFICIELLE OU DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL EN AFRIQUE

DATE LIMITE DE SOUMISSION : 13 JANVIER 2025

PLUS D'INFORMATIONS : WWW.AFRICADATAPROTECTION.ORG

ÉDITO

DE L'ENCADREMENT DES DONNÉES PERSONNELLES EN AFRIQUE : DE LA STRATÉGIE CONTINENTALE AUX INITIATIVES SOUS-RÉGIONALES

Par Winnie Franck DONGBOU
Senior Data Protection Lawyer & PhD Candidate in Health Data Governance

Le 28 juillet 2022, l'Union Africaine (UA) a dévoilé sa politique sur la gouvernance des données à travers un guide stratégique à destination des États africains. Ce document vise notamment à harmoniser les politiques de gouvernance des données sur l'ensemble du continent et à faciliter la fluidité des échanges de données afin d'instaurer la confiance dans les systèmes numériques.

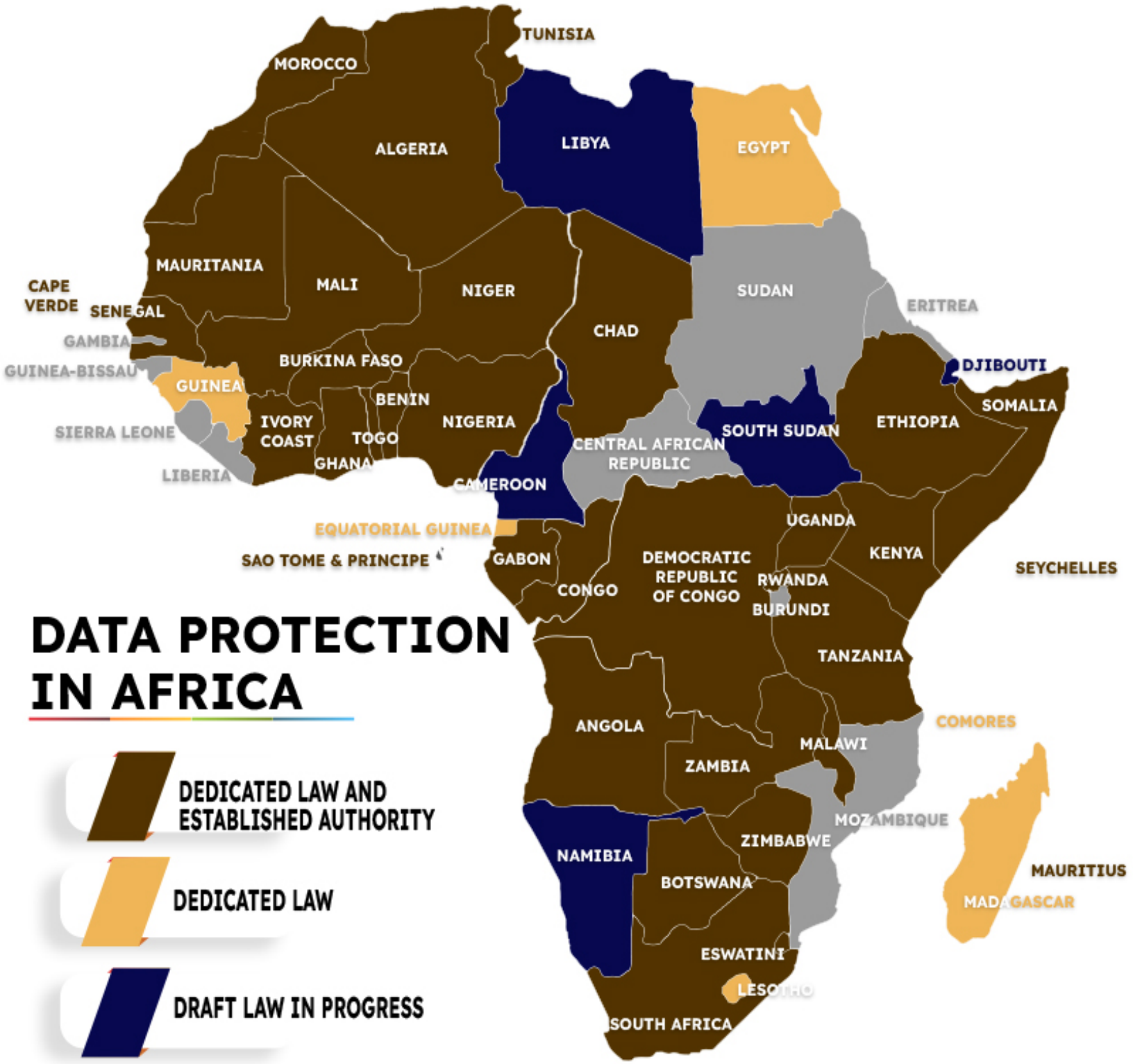
Pour y parvenir l'UA formule de multiples recommandations soulignant l'importance de protéger les données personnelles et d'en faciliter le transfert à travers le continent.

A titre illustratif, il est recommandé que les États membres « coopèrent pour permettre aux données de circuler dans le continent tout en préservant les droits de l'Homme, la protection des données, la sécurité et le partage équitable des bénéfices ». Conscient de la nécessité d'impliquer les communautés économiques régionales (CER), l'Union formule également à leur égard des recommandations visant à encourager la création « d'un cadre commun de catégorisation et de partage des données qui tient compte des grands types de données et les niveaux de confidentialité et de sécurité associés ». C'est donc à juste titre que l'UA encourage la collaboration avec les autorités nationales de protection des données personnelles des États membres de l'UA, en ce compris le Réseau africain des autorités de protection des données personnelles.

Ces recommandations de l'UA font écho aux initiatives de la Communauté Economique des Etats de l'Afrique de l'Ouest (CEDEAO) et de la Communauté Est-Africaine (EAC). En effet, du 16 au 18 octobre 2024, le Rwanda a accueilli 70 délégués représentant les 8 États membres de l'EAC, en vue de promouvoir l'harmonisation des cadres de gouvernance des données à l'échelle régionale et de renforcer la coopération juridique en matière de protection des données. Immaculate Kassait, Commissaire kenyane à la protection des données, a rappelé à cette occasion que l'harmonisation des législations en matière de protection des données en Afrique permettra aux autorités nationales d'adopter une approche cohérente et concertée dans la gestion des litiges liés à la protection des données, en particulier lorsqu'ils impliquent des multinationales.

La Commission de la CEDEAO, quant à elle, a organisé au Nigeria un atelier centré sur la révision de l'Acte additionnel sur la protection des données personnelles et le renforcement des capacités pour l'harmonisation des cadres de protection et les flux transfrontaliers de données. À partir d'un avant-projet d'environ quatre-vingts pages, la CEDEAO vise à supprimer les obstacles au libre transfert des données entre ses États membres, tout en fixant des conditions communes pour les transferts de données en dehors de la région.

Ces initiatives régionales illustrent sans conteste une partie de l'objectif d'harmonisation continentale recherché, qui nécessitera d'être coordonné et aligné. En l'absence d'une harmonisation complète, l'interopérabilité des cadres juridiques régionaux constituera la clé de voûte pour garantir une gouvernance efficace des données en Afrique. **W.F.D**



Source : blog.africadataprotection.org/en/legislation

LE NIGÉRIA INFLIGE À META (EX FACEBOOK) UNE AMENDE RECORD DE 220 MILLIONS DE DOLLARS US : DÉCRYPTAGE D'UNE SANCTION HISTORIQUE !

Par Franck ADOPO, PhD Candidate in digital law and data protection

© iStock

Les actes et initiatives tant institutionnels qu'individuels en faveur d'une meilleure protection de la vie privée sur le continent se multiplient. L'espace africain, longtemps considéré comme un « désert règlementaire » en la matière, est aujourd'hui le théâtre de pas de géants. Le Nigéria n'a pas attendu l'entrée en vigueur de sa dernière loi sur la protection des données de 2023 pour s'intéresser aux activités du groupe Méta, anciennement dénommé Facebook sur son territoire.

De quoi s'agit-il ?

Le 19 juillet 2024, la commission fédérale de la concurrence et de la protection des consommateurs (FCCPC) a prononcé contre Méta une sanction record de 220 millions de dollars américains. Faisant partie des plus lourdes sanctions jamais prononcées sur le contient contre un géant du numérique, elle constitue le début d'un bras de fer entre le Nigéria et Méta. L'une des particularités de cette affaire résulte de la parfaite collaboration entre la FCCPC et la commission nigériane de protection des données (NDPC), une grande première en Afrique. L'ambition affichée par la FCCPC était claire : montrer comment la problématique de la protection des données pouvait servir de support pour résoudre les questions de protection des consommateurs mais aussi à régler des questions de concurrence. Afin de faciliter la compréhension de cette affaire, ces deux entités seront désignées par le terme « Commission ».

Le point de départ de cette affaire a été la mise à jour, le 15 mai 2021, de la politique de confidentialité de l'application WhatsApp, une entité du groupe Méta. Pour faciliter la compréhension et à la suite de la Commission, aucune différence ne sera faite entre WhatsApp et l'entité mère Méta, dans la mesure où la sanction les implique de manière indifférenciée. La politique de confidenti-

alité est le document juridique permettant d'expliquer aux utilisateurs les différentes données traitées par une entité, les formes de traitement et leur impact sur eux. Elle précise notamment les mesures de sécurité mises en place afin de protéger de manière optimale la vie privée des utilisateurs. Cependant, celles récemment mises en place par WhatsApp ont suscité une vague de réactions au Nigéria. Selon la Commission, les politiques étaient imposées aux consommateurs donc contraires aux règles d'équité applicables en matière de traitement de données. C'est le début d'une enquête préliminaire contre Méta pour d'éventuelles violations de la loi fédérale sur la concurrence et la protection des consommateurs (FCCPA) et le règlement du Nigeria sur la protection des données (NDPR) à présent remplacé par la loi nigériane sur la protection des données de 2023 (NDPA).

La procédure et la réaction de Méta

À la suite de ces évènements, une enquête préliminaire a été ouverte par la commission afin d'évaluer le caractère volontaire de son acceptation. Une demande a alors été adressée à Méta le 10 juin 2021 sous la forme d'un ordre de justification (OSC) conformément aux missions de la FCCPC prévues à l'Article 17 du FCCPA, afin de lui présenter l'accusation et lui laisser l'initiative de répondre. Au bout d'une procédure de 38 mois, les interventions de Méta lors des confrontations avec les autorités ont consisté à affirmer que « l'intervention règlementaire de la Commission était injustifiée et fondée sur une mauvaise compréhension de l'objectif et de l'effet de sa politique de confidentialité », en dépit des nombreuses preuves détaillées par celle-ci. Cette longue procédure démontre la complexité de l'affaire dans la mesure où les autorités nigérianes ont retenu contre Méta des infractions tant sur des questions de concurrence mais aussi de protection des données, à savoir : la méconnaissance du droit à l'auto-détermination, le transfert et le partage non autorisés de données, la discrimination par le traitement disparate des données, l'abus de position dominante et les ventes liées de produits et services.

Que dit la règlementation nigériane ?

En vertu de la section 1.2, le règlement concerne les « personnes physiques résidant au Nigeria ou résidant en dehors du Nigeria et qui sont citoyennes du Nigeria ». En l'espèce, selon les caractéristiques de son activité, WhatsApp est un service de messagerie instantanée. Il utilise les données des Nigérians via leurs contacts afin de leur fournir ses services. En plus des informations partagées par l'utilisateur, WhatsApp collecte des données sur l'activité et les habitudes de ces derniers. Cette activité est donc soumise au règlement dans la mesure où elle correspond aux critères établis à la section 1.2. Cependant, ce champ d'application reste assez flou, notamment sur le volet territorial. Il ne fournit aucune information sur le responsable de traitement ou le sous-traitant. Doit-il résider ou non sur le territoire du Nigéria ? Cette situation pourrait favoriser la violation du règlement. Cependant, le NDPA offre une protection plus étendue et vient clarifier ce cadre. En effet, son champ d'application est beaucoup plus clair. Il prend en compte le critère du ciblage, mettant en avant l'offre de biens et de services destinée aux personnes concernées indépendamment de la localisation du responsable de traitement.

En vertu du NDPR, le droit à l'autodétermination implique le respect des principes généraux de traitement des données, en l'occurrence la licéité, le consentement, la publicité et la clarté des politiques de confidentialité. Ces principes sont prévus aux sections 2.1, 2.2, 2.3, 2.5 et 3.1 du règlement. Selon ces principes, tout traitement doit être licite et transparent. Il requiert surtout le consentement de la personne concernée. Le règlement a la particularité de fournir des détails et des conditions clairs en ce qui concerne le consentement, de sorte qu'il devient une condition incontournable dans l'activité de traitement des données. En effet, le consentement doit être libre, éclairé et sans équivoque. Or, selon les informations recueillies par la commission, toutes les caractéristiques d'un consentement libre, éclairé et sans équivoque n'étaient pas présentes dans le traitement effectué par WhatsApp. L'introduction de la mise à jour des politiques semble avoir été réalisée en méconnaissance de ce principe. Selon elle, les politiques étaient opaques et ne permettaient pas aux consommateurs de donner un consentement libre et éclairé. Pour la commission, cette pratique constitue un abus de la part de WhatsApp.

En plus de reconnaître les principes fondamentaux de traitement des données, le règlement organise les transferts de données sous la supervision conjointe du Procureur général fédéral (HAGF) et de

l'Agence nationale de développement des technologies de l'information (NITDA) sous les sections 2.11 et 2.12. Plusieurs conditions sont posées, notamment le transfert vers des pays adéquats. En ce sens, la NITDA a publié en novembre 2020, une liste blanche des pays adéquats pour des transferts de données en toute sécurité. Or, les pays de l'UE, Singapour et les USA, destinations vers lesquelles sont transférées les données y figurent. A priori, WhatsApp serait donc fondé à rejeter l'argumentaire de la commission visant à sanctionner son transfert de données. Cependant, il est important de retenir que ce qui est reproché à WhatsApp, c'est plutôt la manière dont les données ont été collectées. C'est le non-respect du droit à l'autodétermination qui transcende toute cette décision. Son non-respect rend illégal le transfert. En effet, aucun transfert de données ne peut être effectué sans que les personnes concernées soient informées, encore moins sans leur consentement. Or, c'est ce qui ressort de la pratique de WhatsApp. Les utilisateurs n'avaient pas conscience et n'avaient pas consenti au transfert de leurs données vers ces pays. La commission a jugé alors ces transferts illégaux.

L'argument inédit dans cette affaire est le traitement disparate des données des consommateurs nigérians et européens, nonobstant un cadre règlementaire similaire. Il ressort du rapport de la commission et des pièces fournies par WhatsApp, que ce dernier n'accorde pas le même traitement aux utilisateurs nigérians qu'à ceux de l'Union européenne. Il était difficile de contester cet argument dans la mesure où cette « discrimination » est clairement disponible sur le site internet de WhatsApp. Cela pourrait s'expliquer par les spécificités règlementaires locales et la rigidité du Règlement Général sur la Protection des Données (RGPD) en ce qui concerne la protection des données en Europe. Bien qu'il existe des similarités entre des principes généraux ou encore les droits reconnus aux individus, cela ne suffit pas à affirmer que la législation européenne est identique à celle du Nigéria. En effet, plusieurs autres facteurs prévus à l'article 45 du RGPD entrent en ligne de compte, notamment l'état de droit, le respect des droits de l'homme, la législation pertinente, les recours dont disposent les personnes concernées. De plus, le Nigéria ne fait pas encore partie des pays jugés adéquats par la Commission européenne. Pouvons-nous produire la même analyse à propos de la nouvelle loi de 2023 ? Per-

© iStock

mettrait-elle au Nigéria d'être un potentiel candidat à la très sélective liste des pays adéquats ? En l'état actuel des choses, des éléments concrets permettent de l'envisager sérieusement. En effet, depuis l'entrée en vigueur de la loi de 2023, les cadres règlementaires et institutionnels ont fortement évolué. De plus, les actions et les initiatives de la NDPC ne font que se multiplier, au point où la problématique de la protection de la vie privée est devenue un enjeu d'intérêt national majeur.

En ce qui concerne les infractions propres à la règlementation liée au droit de la concurrence, elles concernent l'abus de position dominante et les ventes liées. Sur la base de la section 70 du FCCPA, l'enquête de la Commission a révélé avec détails que Méta était en position dominante et abusait de cette position. Cette situation résulte de son pouvoir de marché estimé à 93% du marché nigérian. L'abus émane du déséquilibre à l'égard des consommateurs et le non-respect de leur droit à l'autodétermination dans le traitement de leurs données, tout en niant leur consentement à l'utilisation de ces données. WhatsApp s'est contenté de rejeter en bloc ces arguments et la définition du marché retenue par la Commission sous prétexte qu'elle avait des concurrents de taille. Mais la Commission a estimé que les preuves et arguments fournis par WhatsApp étaient insuffisants pour démontrer le contraire.

La section 72, 2, d, iii de la FCCPA interdit les pratiques qui s'apparentent aux ventes liées. Dans ce cas de figure, c'est le détournement de finalité qui est pris en compte. En effet, WhatsApp partage des données avec Facebook ou d'autres partenaires à des fins de profilage et de marketing. Ce partage est réalisé sans possibilité pour les consommateurs de refuser. Or, pendant la collecte, WhatsApp ne fournit pas aux utilisateurs l'information de ce partage. Pour la Commission, le fait que cette finalité s'éloigne de la finalité initiale et que cette nouvelle finalité ne procure aucun bénéfice aux utilisateurs nigérians, cela constitue une vente liée.

À la lecture de cette analyse, les pratiques de WhatsApp portent préjudice aux consommateurs nigérians. Or, sur la base du respect au droit à l'autodétermination dans le traitement des données, le responsable de traitement doit s'assurer que le traitement ne porte pas préjudice aux personnes concernées. Pour la Commission, le fait que les politiques de confidentialité aient été imposées aux utilisateurs, cela constitue un préjudice pour ces derniers. C'est en ce sens qu'elle justifie sa sanction. La démarche de la FCCPC n'est pas loin de celle des régulateurs en Europe. Il s'agit de contraindre le groupe Méta, sur la base de l'absence de consentement à se conformer à la législation par de lourdes sanctions pécuniaires. Même s'il s'agit d'une première sanction record en Afrique, les autorités nigérianes envoient un message fort aux géants du numérique. Le respect des droits fondamentaux des africains demeure une priorité. La souveraineté numérique tant convoitée n'est pas une utopie. Cependant, la question qu'il faudrait se poser serait de savoir si le Nigéria seul pourra atteindre cet objectif. La protection des données sur le fondement du droit de la concurrence peut-elle constituer une nouvelle approche solide de protection de la vie privée en Afrique ? **F.A**

© iStock

LES DONNÉES DE SANTÉ EN AFRIQUE SUB-SAHARIENNE : DÉFIS, RISQUES ET OPPORTUNITÉS

Par Prof. Benjamin C. GUINHOUYA, Prof. of Epidemiology & Program. leader of Health Data Science

© iStock

L'Afrique Sub-Saharienne (ASS) porte une lourde charge sanitaire, représentant 20 % des maladies mondiales tout en ne disposant que de 1 % des scientifiques et d'un ratio alarmant de 20 médecins pour 100 000 habitants. Ce déficit critique en ressources humaines et matérielles est exacerbé par une concentration des services dans les zones urbaines, laissant les populations rurales dans une précarité sanitaire inquiétante. L'ASS est également confrontée à une double transition épidémiologique. Alors que des maladies transmissibles comme le VIH/SIDA, le paludisme et la tuberculose continuent de ravager la région, on observe une augmentation rapide des maladies non transmissibles, telles que le diabète et les maladies cardiovasculaires. Ce profil impose une révision des priorités de santé publique, ainsi qu'une allocation plus stratégique et rationnelle des ressources. Dans ce contexte, les données de santé se révèlent essentielles pour une planification ciblée et des interventions efficaces, permettant de surmonter en partie ces inégalités.

Ces données de santé proviennent de multiples sources, allant des écrits des professionnels de soins de santé à des bases complexes de données génétiques en passant par des dossiers médicaux simples plus ou moins structurés et les données médico-administratives. Selon le Règlement général sur la protection des données (RGPD) européen, elles incluent toute information relative à l'état de santé physique ou mentale d'une personne, qu'elle soit collectée directement, via des dossiers médicaux, ou indirectement, par le biais de dispositifs connectés. Dans la Digital Bill du Kenya, les données de santé concernent les données relatives à l'état de santé physique ou mentale de la personne concernée et incluent les dossiers concernant l'état de santé passé, présent ou futur, les données collectées lors de l'accueil en vue de la prestation de services de santé ou les

données qui associent la personne concernée à la prestation de services de santé spécifiques. Malheureusement, il existe une inefficacité persistante dans la gestion des données. De nombreux systèmes de santé s'appuient encore sur des documents papier, ralentissant les processus diagnostiques et compromettant les prises de décision rapides, particulièrement en période de crise.

Avec l'essor des outils numériques et de l'intelligence artificielle (IA), ces données deviennent des leviers incontournables pour améliorer la surveillance épidémiologique, personnaliser les soins de santé et optimiser l'allocation et/ou l'utilisation des ressources limitées. Certains programmes innovants sont déjà fonctionnels, particulièrement en ASS d'expression anglaise, y compris la Tanzanie, le Kenya, ou encore le Nigeria. Cependant, ces innovations, bien que prometteuses, s'accompagnent aussi de défis majeurs, notamment en matière de protection des données personnelles et d'équité dans l'accès aux technologies. Enfin, des progrès substantiels en matière de traitement et de valorisation des données de santé sont encore requis en ASS d'expression française.

Opportunités offertes par la digitalisation : des exemples fonctionnels en Afrique Sub-Saharienne d'expression anglaise

La transformation numérique des systèmes de santé en ASS offre une réponse prometteuse aux défis structurels et épidémiologiques de la région. Les données de santé digitalisées constituent une ressource stratégique pour optimiser l'efficacité des systèmes tout en améliorant l'accès et la qualité des soins. Ces outils numériques ont déjà commencé à transformer certains domaines clés. En Tanzanie, par exemple, l'initiative Wazazi Nipendeni donne à voir de quelle manière des technologies simples comme les SMS peuvent produire un impact considérable. Ce programme utilise des messages personnalisés pour fournir des informations essentielles sur les soins prénatals, la nutrition et les vaccinations aux mères et aux familles. Cette approche a conduit à une augmentation significative des consultations prénatales et des taux de vaccination, contribuant à une meilleure santé maternelle et infantile.

Au Kenya, les hôpitaux comme « Kenyatta National Hospital » ont adopté des dossiers médicaux électroniques (EMR), simplifiant ainsi la gestion des informations des patients. Grâce à ces systè-

© iStock

mes, la communication entre les professionnels de santé s'améliore, les erreurs médicales diminuent et la continuité des soins devient plus fluide. En parallèle, des outils plus sophistiqués, comme l'analyse assistée par IA, sont employés pour identifier des pathologies complexes. Par exemple, des images de frottis sanguins analysées par des algorithmes permettent de détecter le paludisme avec une précision accrue, accélérant les diagnostics dans les zones où les spécialistes sont rares.
Au Nigeria, le système SORMAS illustre comment les données numériques peuvent renforcer la réponse aux crises sanitaires. Initialement conçu pour surveiller les maladies infectieuses, ce système a été adapté pour gérer les réponses au COVID-19, élargissant sa portée à l'ensemble des 36 États du pays en un temps record. Cette flexibilité montre le potentiel des solutions numériques pour répondre rapidement à des besoins de santé publique en constante évolution.
Ces exemples montrent que la digitalisation peut non seulement rendre les systèmes de santé plus efficaces, mais aussi plus résilients face aux crises, en réduisant les délais de réaction et en améliorant la coordination entre les acteurs. Cependant, pour que ces opportunités se réalisent pleinement, des efforts doivent être faits pour garantir une adoption à grande échelle et des infrastructures adaptées.

Risques et enjeux liés aux données de santé

Malgré leur immense potentiel, les données de santé digitalisées présentent des risques importants qu'il est impératif d'anticiper et de gérer. L'un des principaux défis réside dans la vulnérabilité de ces données face aux cyberattaques et aux violations de sécurité. En l'absence de mesures robustes, les systèmes de santé peuvent devenir des cibles pour des acteurs malveillants, exposant ainsi des informations sensibles et compromettant la confiance du public.
Un autre enjeu majeur est lié à la ré-identification des personnes. Même lorsque des informations sont anonymisées, les avancées en IA permettent parfois de croiser des données et de retrouver l'identité des individus. Ce phénomène soulève des inquiétudes non seulement pour la confidentialité des patients, mais aussi pour les conséquences sociales ou économiques qui pourraient découler de la divulgation de ces informations.
En parallèle, la question éthique du consentement éclairé demeure cruciale. De nombreuses plateformes numériques de santé collectent et utilisent des données sans que les utilisateurs soient pleinement conscients de leurs finalités. Pour répondre à ce défi, certains projets adoptent des modèles de consentement dynamique, permettant aux individus d'ajuster à tout moment leur autorisation d'utilisation des données. Cette approche favorise une plus grande transparence et renforce la confiance des populations.
Enfin, l'inégalité d'accès aux outils numériques constitue un obstacle supplémentaire. Dans les zones rurales ou parmi les populations marginalisées, le manque de connectivité ou d'alphabétisation numérique empêche une adoption équitable de ces technologies. Il est essentiel que les systèmes de santé veillent à inclure ces populations afin d'éviter d'amplifier les inégalités déjà existantes.
Pour exploiter tout le potentiel des données de santé, il est impératif de mettre en place des cadres de gouvernance éthiques et sécurisés, garantissant à la fois la protection des individus et l'utilisation efficace des données pour le bien commun.

Recommandations pour tirer les meilleurs avantages de la digitalisation des données de santé

Pour que l'ASS puisse tirer pleinement parti des avantages des données de santé tout en minimisant les risques, des actions concertées sont nécessaire s'imposent. L'harmonisation des politiques nationales et régionales constitue un premier levier. Par exemple, l'adoption de cadres comme la loi type sur la gouvernance des données de santé peut fournir une base commune pour garantir que la collecte, le stockage et l'utilisation des données respectent des principes d'éthique et des normes sécuritaires. Ces politiques doivent intégrer des mécanismes de transparence, de consentement et de supervision qui inspirent confiance aux populations.
Un deuxième pilier réside dans le développement des compétences locales. La formation d'experts en gestion et analyse de données de santé, combinée à des investissements dans des infrastructures robustes, est essentielle pour garantir l'autonomie et la souveraineté des systèmes de santé africains. Sans cela, la dépendance vis-à-vis de solutions importées pourrait freiner l'innovation locale et augmenter les coûts à long terme.
Enfin, il est crucial de mettre l'accent sur des solu-

tions adaptées aux besoins et aux contextes des populations. Les outils numériques doivent être conçus avec une approche centrée sur l'utilisateur, en intégrant les retours des patients et des professionnels de soins de santé. De plus, des partenariats entre gouvernements, entreprises privées et organisations internationales peuvent permettre de mobiliser les ressources nécessaires pour accélérer l'adoption des technologies numériques.
À long terme, ces efforts doivent viser à établir une équité dans l'accès aux soins, à renforcer la résilience des systèmes de santé et à transformer les défis structurels en opportunités durables. Les données de santé ne sont pas seulement des outils techniques : elles sont au cœur de la transformation des systèmes de santé pour un avenir plus juste et plus inclusif.

En rigueur de terme, pour maximiser les bénéfices des données de santé tout en limitant les risques, il est essentiel de mettre en place des politiques harmonisées et des infrastructures adaptées. Les axes prioritaires devraient intégrer :
1. **Une harmonisation régionale** : Adopter des cadres communs comme la loi type sur la gouvernance des données de santé pour garantir une gestion éthique et sécurisée des données.
2. **Un développement des compétences locales** : Former des experts en données de santé et promouvoir l'innovation locale pour éviter la dépendance envers les solutions étrangères.
3. **Des investissements dans l'infrastructure** : Moderniser les systèmes de santé avec des outils robustes et interopérables, adaptés aux contextes locaux.
4. **Des approches centrées sur l'utilisateur** : Concevoir des solutions adaptées aux besoins des populations et garantir leur engagement actif dans les décisions relatives à leurs données. **B.C.G**

L'AUTORITÉ DE PROTECTION DES DONNÉES DU NIGER PUBLIE SON RAPPORT ANNUEL 2023 : QUE FAUT-IL RETENIR ?

Par Mahadi MAIFADA MAGOUDANI, PhD in digital law

Depuis juillet 2023, le Niger connaît une transformation politique significative qui a influencé les priorités des institutions nationales, y compris la Haute Autorité de Protection des Données à caractère Personnel (HAPDP). Dans ce cadre, l'Autorité a démontré sa capacité à adapter ses activités pour répondre aux exigences du moment tout en s'inscrivant dans une démarche de régulation conforme aux standards internationaux.
La loi n°2022-59, saluée comme l'un des cadres juridiques les plus complets en Afrique de l'Ouest francophone, a permis de renforcer les outils et les missions de la HAPDP. Ce rapport d'activité constitue une opportunité pour évaluer les premières étapes de sa mise en œuvre et dessiner les contours d'une régulation plus robuste à l'avenir.

Actions de régulation de la HAPDP

Le rapport 2023 innove par l'introduction d'une rubrique consacrée aux « missions de contrôle », symbolisant la volonté de la HAPDP de garantir la conformité aux exigences légales. Deux types de contrôles sont mis en avant :
- Le contrôle par audition, axé sur l'examen des dossiers pour des secteurs tels que les télécommunications, les banques et les ONG. Ces contrôles offrent une opportunité d'assurer la conformité administrative tout en accompagnant les responsables de traitement dans la régularisation de leurs pratiques.
- Le contrôle sur place, qui s'est concentré sur des secteurs variés (santé, assurances, transport, télécommunications, ONG). Ce type de contrôle a permis de formuler des recommandations utiles, soulignant l'approche constructive de la HAPDP en matière de sensibilisation et d'amélioration continue des pratiques des acteurs concernés.

Recommandations et mise en demeure

Avec 30 mises en demeure notifiées en 2023, la respect de la législation en vigueur. Si le rapport ne détaille pas l'ensemble des résultats de ces actions, cela reflète le caractère évolutif de l'institution, qui continue à structurer ses outils pour une transparence accrue à l'avenir.

L'introduction du registre des opérations par la loi n°2022-59 est une avancée majeure qui distingue la législation nigérienne dans la région. En tant qu'outil de conformité clé, ce registre pourrait devenir un pilier des futures inspections et audits.
La HAPDP, dans un esprit d'accompagnement, pourrait renforcer son rôle en proposant des modèles standardisés et en offrant des formations adaptées pour faciliter l'adoption de cet outil par les responsables de traitement.
Bien que son déploiement soit encore en cours, cette étape témoigne de la modernité et de l'ambition du cadre juridique nigérien, offrant des perspectives prometteuses à long terme.

Perspectives et recommandations

Dans le contexte sécuritaire et politique actuel, la HAPDP dispose d'un rôle stratégique à jouer dans la souveraineté numérique du Niger. Par exemple, son implication dans la gestion des données sensibles, telles que celles liées au fichier de gestion des individus et entités concernées par le terrorisme, pourrait renforcer son positionnement comme acteur clé de la protection des données personnelles.

Les recommandations suivantes pourraient contribuer à renforcer son efficacité :
Transparence accrue : Détails plus approfondis des actions entreprises dans les rapports futurs.
Accompagnement des acteurs : Renforcement des outils pratiques et pédagogiques, notamment pour le registre des opérations.
Renforcement des capacités : Formation continue des équipes pour relever les défis technologiques et sécuritaires.

Le rapport de la HAPDP met en lumière les bases solides jetées pour renforcer la régulation des données personnelles au Niger. Dans un contexte en évolution, l'Autorité a démontré sa capacité d'adaptation et son engagement en faveur de la protection des données. Avec un cadre juridique novateur et une approche progressive de la conformité, la HAPDP est bien positionnée pour devenir un acteur clé de la souveraineté numérique nationale, tout en gagnant la confiance des citoyens et des partenaires économiques. Cette dynamique positive contribuera à asseoir le Niger en tant que modèle de protection des données en Afrique de l'Ouest. **M.M.M**

© iStock

ARPTIC/ARPTC INVESTIT DES MISSIONS DE L'AUTORITÉ DE PROTECTION DES DONNÉES EN RD-CONGO

Par Brozeck KANDOLO, PhD Candidate in digital law

© iStock

L' année 2023 marque une étape majeure pour le cadre juridique du numérique en République Démocratique du Congo (ci-après « RD Congo ») avec l'entrée en vigueur de l'ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique. Ce texte ambitieux s'inscrit dans une volonté de modernisation et de régulation accrue des technologies numériques et de leurs usages en RD Congo. Il prévoit notamment la création de plusieurs autorités administratives chargées de superviser les différents segments du secteur numérique, comme disposent les articles 7 à 12, 275 à 280 et 41. Parmi ces autorités, on y trouve également l'Autorité de Protection des Données (ci-après « APD »), dont la création est prévue aux articles 262 à 270 (pour en savoir plus sur le fonctionnement de l'APD, voir Brozeck Kandolo, « RD-Congo : perspectives de l'autorité de protection des données », Rapport Africa Data Protection – Janvier 2024, p.18). Cette autorité indépendante s'inscrit dans la volonté de réguler les traitements de données personnelles, répondant ainsi aux défis croissants d'un monde de plus en plus digitalisé.

Cependant, malgré ces aspirations prometteuses, une évolution réglementaire inattendue est intervenue le 17 août 2024 avec l'Arrêté ministériel n°cab/min/pt&n/akim/kl/kbs/051/2024. Contrairement aux dispositions prévues par le Code du numérique pour la création de l'APD, cet arrêté a provisoirement transféré les prérogatives de cette dernière à l'Autorité de Régulation des Postes, des Télécommunications et des Technologies de l'Information et de la Communication (ci-après « ARPTIC »).

Cette décision suscite des interrogations majeures, tant sur le plan juridique que stratégique. Sur le plan juridique, on s'interroge sur la conformité de l'arrêté ministériel avec les prescriptions du Code du numérique. D'autre part, l'attribution tempora-

ire des prérogatives de l'APD à l'ARPTIC ne pourrait-elle pas être perçue comme une mesure pragmatique visant à surmonter les contraintes financières, administratives ou politiques entravant la mise en place effective de l'APD ?

I. La légalité de l'arrêté attribuant à l'ARPTIC les missions de l'APD

L'ARPTIC trouve son fondement juridique dans la loi de 2020 sur les télécommunications et les TIC. Cependant, ce n'est qu'en 2023, à la suite d'un décret pris par le Premier ministre, qu'elle a été officiellement créée. Il est important de noter que l'ARPTIC succède à l'ancienne Autorité de Régulation des Postes et Télécommunications du Congo (ARPTC), qui a été remplacée par cette nouvelle entité.
L'attribution des missions de l'APD à l'ARPTIC soulève des interrogations majeures quant à sa légalité. D'une part, elle interroge la conformité de cette extension des compétences avec les principes juridiques fondamentaux, notamment ceux de légalité et de spécialité (A). D'autre part, elle met en lumière des questions liées au transfert de compétences entre entités et au respect du principe de séparation des pouvoirs (B).

A. Extension des compétences de l'ARPTIC : Une entorse au principe de légalité et de spécialité ?

L'attribution des missions de l'APD à l'ARPTIC soulève une question juridique essentielle, celle de savoir si un décret peut légitimement étendre les compétences d'une autorité administrative au-delà des limites définies par la loi qui l'a créée. Cette question interroge directement le respect du principe de légalité et du principe de spécialité, deux principes fondamentaux en droit administratif.

Le principe de hiérarchie des normes selon la théorie de Hans Kelsen, impose que les normes juridiques sont organisées selon un ordre de priorité, où chaque norme doit respecter celles qui lui sont supérieures. En vertu de ce principe, toute norme inférieure, telle qu'un décret ou un règlement, doit être conforme à la loi qui lui sert de fondement. Ainsi, le pouvoir réglementaire, exercé par voie de décret, ne peut ni étendre ni restreindre les compétences d'une autorité créée par une loi, sauf si la loi d'origine prévoit explicitement une telle extension. Or, dans le cas présent, l'arrêté en question, qui vise à étendre les compétences de l'ARPTIC, lui accorde des prérogatives qui ne sont pas prévues par la loi créant cette autorité. En effet, seule une loi peut modifier ou compléter les compétences d'une autorité administrative, conformément au principe de la hiérarchie des normes.

Par ailleurs, le principe de spécialité limite les compétences des personnes morales publiques aux missions explicitement définies lors de leur création. Ce principe impose que toute action entreprise par une autorité publique reste dans le cadre strict des prérogatives qui lui ont été attribuées par la loi. Pour l'ARPTIC, cela signifie que, bien que cette autorité ait vu ses responsabilités élargies au domaine de la protection des données, ces nouvelles prérogatives doivent être accompagnées d'une modification préalable du cadre légal d'origine.

Dans le cas de l'arrêté du 17 août 2024, l'ARPTIC se voit attribuer des missions qui ne figuraient pas dans la loi de 2020 sur les télécommunications et les NTIC. Par conséquent, cette extension de compétences excède les prérogatives fixées par la loi de 2020 et pourrait être juridiquement contestée pour non-conformité au principe de légalité.
Ainsi, la conformité de cette réforme avec les principes de légalité et de spécialité demeure incertaine, et son respect doit être examiné de manière approfondie pour garantir que les missions de l'ARPTIC, notamment en matière de protection des données personnelles, s'inscrivent dans un cadre juridique valide et respectueux de l'État de droit.

B. Transfert de compétences et séparation des pouvoirs

Conformément au Code du numérique, l'établissement de l'APD doit se faire par l'adoption d'un décret pris par le Premier ministre. Contre toute attente, c'est finalement par un arrêté ministériel que les compétences de l'APD ont été transférées à l'ARPTIC.

Il est légitime de s'interroger, sur le plan juridique, pour savoir si une entité qui devrait être créée par un décret du Premier ministre peut voir ses compétences transférées par un arrêté du ministre des Postes, Télécommunications et Numérique (PTN) ? En effet, cette situation soulève une problématique de respect des compétences et de l'autono-

mie des institutions publiques.

En vertu du principe de la séparation des pouvoirs, inscrit dans la Constitution congolaise (Article 68 de la Constitution de la RD Congo), chaque entité doit agir dans le cadre des compétences qui lui sont définies. Par conséquent, le transfert de compétences d'une entité dont la création est conditionnée par un acte du Premier ministre, si cela est fait par une autre autorité, sans base légale claire, pourrait constituer une violation au principe de séparation des pouvoirs.

II. Les défis posés par l'élargissement des compétences de l'ARPTIC

L'attribution temporaire des missions de l'APD à l'ARPTIC peut être perçue comme une démarche salutaire, témoignant de la volonté de l'État congolais de réguler les enjeux numériques tout en limitant les dépenses considérables qu'implique la création d'une nouvelle autorité. Ce choix semble d'autant plus pertinent dans un contexte où le Congo compte déjà de nombreuses institutions, telles que l'Autorité de Régulation du Numérique et l'Autorité Nationale de Certification Électronique, dont certaines compétences ont également été transférées à l'ARPTIC.

Cependant, la question de la protection des données personnelles revêt une dimension particulière. En touchant aux droits fondamentaux, elle appelle une vigilance accrue. Dès lors, confier les missions de l'APD à l'ARPTIC soulève plusieurs interrogations : l'ARPTIC dispose-t-elle de l'indépendance nécessaire pour exercer ces nouvelles missions en toute impartialité (A) ? Et quelle est la pertinence d'associer les objectifs économiques assignés à l'ARPTIC à une mission aussi sensible que celle de la protection des données personnelles (B) ?

A. L'indépendance de l'ARPTIC

L'ARPTIC est placée sous la tutelle du ministre des PTN, ce qui soulève des interrogations sur sa capacité à agir de manière totalement autonome. La dépendance hiérarchique de l'ARPTIC vis-à-vis du ministère risque de nuire à son impartialité et de générer des conflits d'intérêts, particulièrement en présence d'enjeux politiques. En effet, cette subordination administrative pourrait affecter l'autonomie de ses décisions, au détriment de la transparence et de l'impartialité nécessaire pour

© iStock

assurer une protection efficace des données personnelles.

Une autre problématique majeure réside dans la nomination des responsables de l'ARPTIC, en particulier ceux du conseil d'administration et de la Direction générale. Conformément aux articles 15 et 21 du Décret n° 23/13 du 3 mars 2023, ces responsables sont nommés, relevés de leurs fonctions, et révoqués par ordonnance du Président de la République. De plus, l'article 24 du même décret prévoit que les commissaires aux comptes sont nommés par décret du Premier ministre. Ce rapport de dépendance entre l'autorité de nomination et les personnes nommées soulève une question essentielle : l'indépendance des responsables de l'ARPTIC dans leurs décisions, notamment en matière de protection des données personnelles, peut-elle réellement être assurée dans un tel cadre ?

Ainsi, l'indépendance de l'ARPTIC est cruciale pour assurer une régulation impartiale et efficace de la protection des données personnelles en RD Congo. Les enjeux liés à la protection des données sont trop importants pour être soumis à des pressions politiques. Il est donc impératif de prendre des mesures concrètes afin d'assurer que l'ARPTIC puisse exercer ses missions de manière autonome et sans ingérence extérieure, en attendant la mise en place de l'APD.

B. ARPTIC : entre régulation économique et protection des données

L'ARPTIC, qui a pour principales missions la régulation du marché des télécommunications et des technologies de l'information et de la communication (TIC), se concentre principalement sur des objectifs économiques tels que la promotion de la concurrence, l'optimisation des infrastructures et l'amélioration de la qualité des services dans ces secteurs. Ces missions, bien qu'essentielles pour le développement du secteur numérique, ne s'alignent pas toujours avec les exigences inhérentes à une autorité de contrôle dédiée à la protection des données personnelles.

La régulation économique requiert souvent une approche plus flexible et pragmatique, visant à favoriser l'efficacité du marché et à encourager l'innovation. En revanche, la protection des données personnelles impose des obligations strictes en termes de confidentialité, de sécurité et de transparence. Cela nécessite une vigilance constante, une indépendance dans le contrôle et une capacité à s'opposer aux pratiques abusives, même si cela peut engendrer des répercussions économiques pour les acteurs du secteur.

Enfin, l'ARPTIC est appelée à arbitrer des intérêts parfois contradictoires, notamment en conciliant la promotion de la concurrence avec les besoins de sécurité et de confidentialité des données. Cependant, ces objectifs peuvent entrer en conflit, car les initiatives visant à stimuler la compétitivité sur le marché peuvent parfois nuire à la protection des données personnelles. **B.K**

© iStock

WWW.AFRICADATAPROTECTION.ORG
INFO@AFRICADATAPROTECTION.ORG