AFRICA DATA PROTECTION

REPORT

Mai 2024

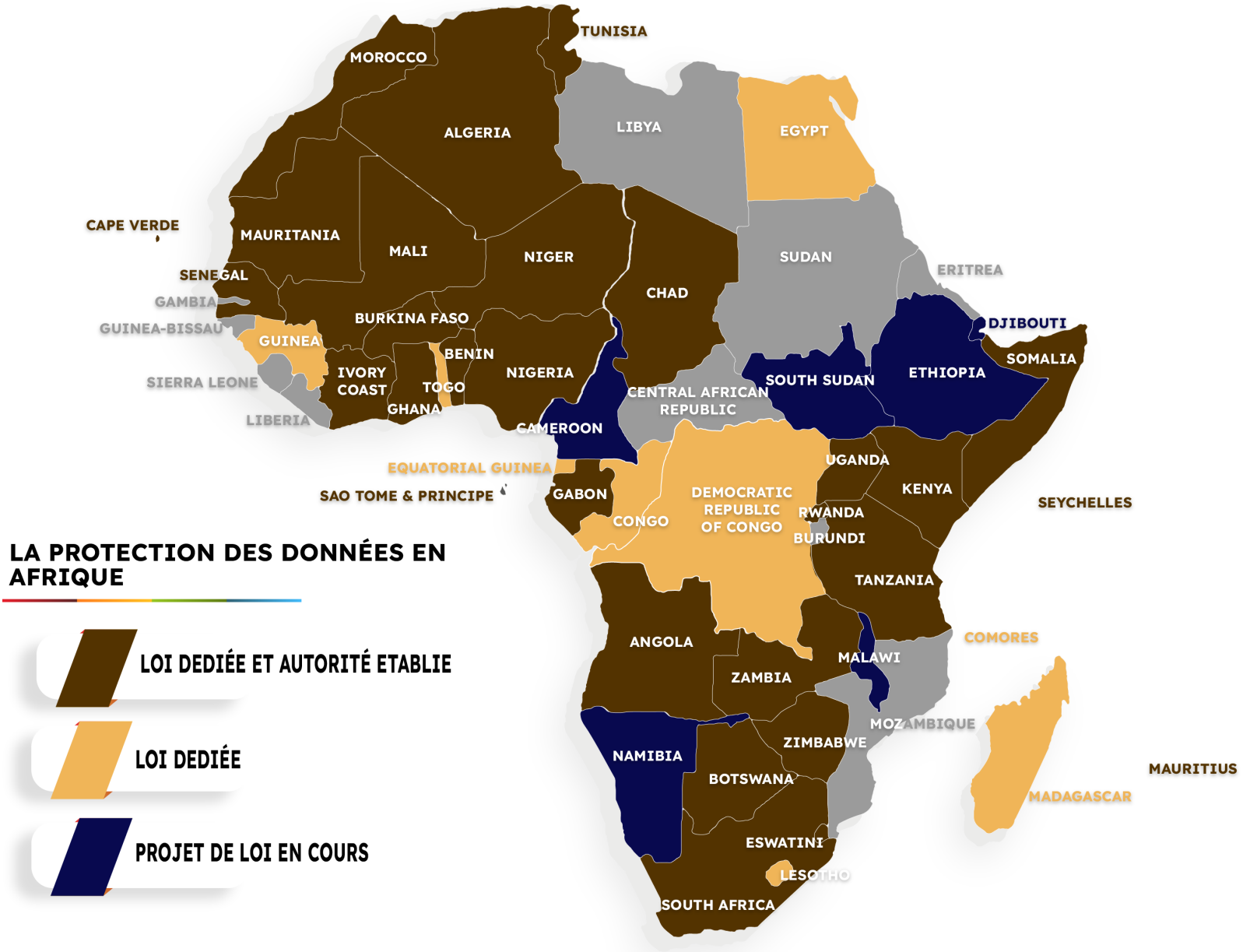
AFRICA DATA PROTECTION

Sommaire

AVANT-PROPOS DU PRÉSIDENT

Jules Hervé YIMEUMI
Président de l'association
Africa Data Protection

Le premier semestre de l'année 2024 a été marqué par l'inauguration de deux autorités de protection des données sur le continent africain. Il s'agit, en premier lieu, de l'autorité somalienne (Somali Data Protection Authority). La création de cette autorité fait suite à l'approbation de la Loi somalienne sur la Protection des Données (Loi n° 005 de 2023). Cela représente une avancée législative significative, ratifiée par les deux chambres parlementaires du pays, et signée par le Président Hassan Sheikh Mohamud en mars 2023. Cette Loi a ouvert la voie à une réglementation robuste en matière de protection des données en Somalie, alignant le pays sur les normes mondiales.



Dans un second temps, la création de l'autorité tanzanienne (Personal Data Protection Commission) a eu lieu. Son inauguration a été faite avec la présence de la Présidente de la République, ce qui marque un signal fort envers la protection des données à caractère personnel dans le pays. C'est ainsi que le 10 avril 2024, cette autorité a annoncé qu'elle avait commencé l'enregistrement des responsables de traitement et des sous-traitants de données, comme l'exige l'article 14(1) de la loi de 2022 sur la protection des données personnelles (PDPA). L'autorité a expliqué que les responsables de traitement et les sous-traitants de données disposent de six mois à compter de la date de l'annonce pour s'inscrire sur le système d'enregistrement disponible sur son site Web.

Dans les autres actualités, La Chambre des représentants éthiopien a adopté le projet de loi sur la protection des données personnelles, qui a été auparavant approuvé par le Conseil des ministres. De son côté, l'autorité de protection des données de la Côte d'Ivoire (ARTCI) a adressé une mise en demeure et un avertissement à un ministère et à une société pour non-respect de la loi sur la protection des données personnelles. Cette mise en demeure oblige ces organismes à designer respectivement leurs correspondants à la protection des données dans un délai de sept jours, et à entamer leur processus de mise en conformité avec la loi dans un délai de soixante jours.

Enfin, dans un autre registre, nous avons le plaisir de vous annoncer l'évènement de lancement de notre association au Maroc.
Depuis sa création en 2020 en tant que plateforme d'information sur la protection des données en Afrique, Africa Data Protection (ADP) a poursuivi sa mission avec dévouement et engagement. Depuis, l'organisation a franchi une étape majeure dans son parcours en devenant une association à but non lucratif, visant à façonner un avenir numérique sûr et éthique pour tous les citoyens africains.

ADP, étant devenue une association à part entière depuis septembre 2023, s'engage à jouer un rôle essentiel dans l'évolution de la société africaine vers une utilisation responsable des technologies de l'information. Son objectif premier est de garantir que les droits fondamentaux de chacun à la vie privée et à la protection des données soient respectés dans un monde de plus en plus connecté.
Afin de célébrer cette nouvelle étape et d'officialiser le démarrage des activités de l'association, ADP organise donc son évènement de lancement le 29 mai 2024 à l'École Nationale des Sciences Appliquées de Marrakech.
L'association y dévoilera ses initiatives futures, notamment une plateforme de e-learning sur la protection des données en Afrique, ainsi qu'un kit destiné à sensibiliser la jeunesse à la protection de leurs données en ligne.
Cet événement promet d'être une soirée riche en partage de connaissances et en réseautage, réunissant des parties prenantes engagées dans la construction d'un avenir numérique éthique pour l'Afrique. N'hésitez pas à nous y rejoindre !

Inscription :

J.H.Y

EDITO

Winnie Franck DONGBOU
Juriste en protection des données à caractère personnel

Wissem SEMMAR-BELGHAZI
Responsable évaluation de l'intégrité des tiers

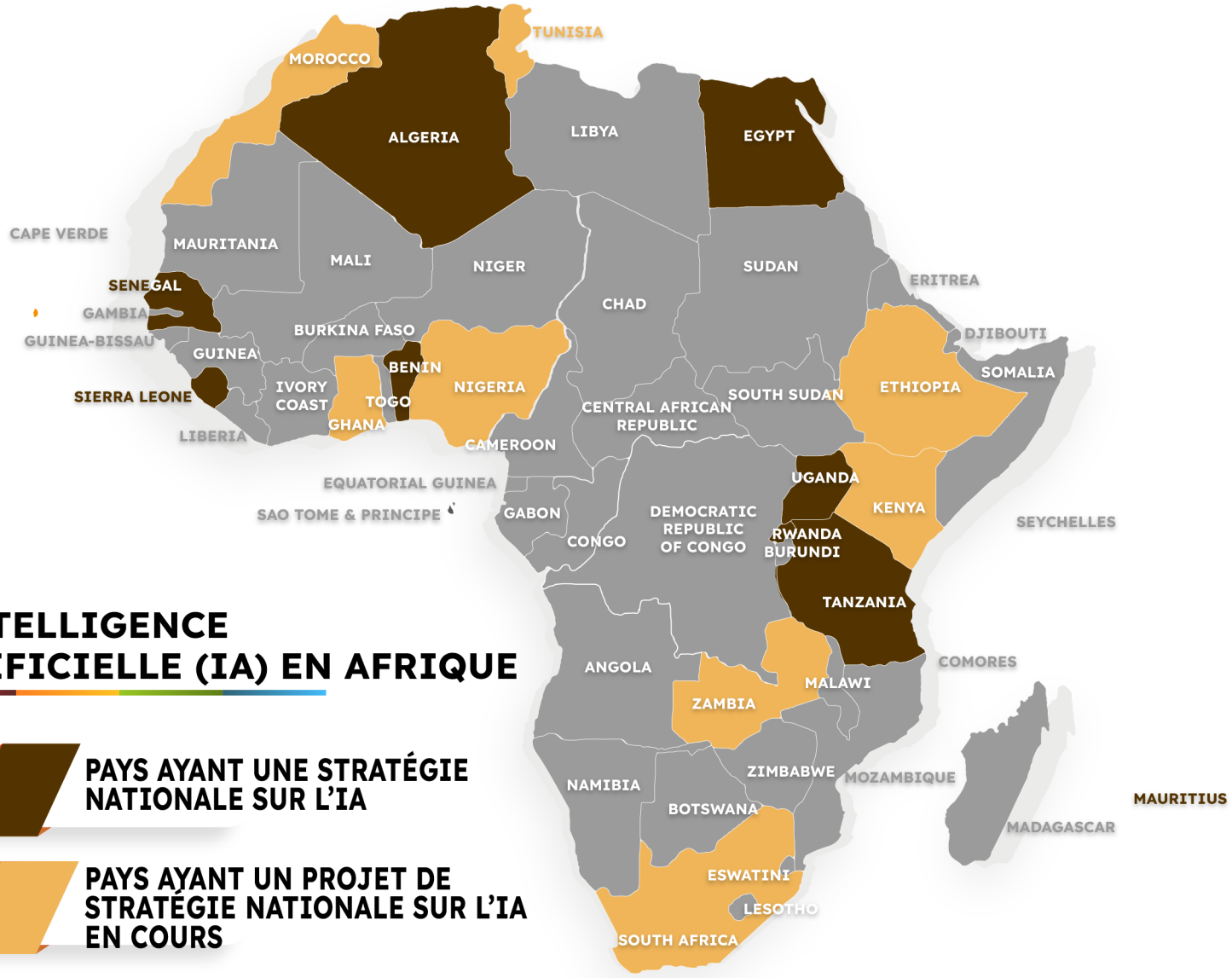
IMPACTS LIÉS À LA DÉPENDANCE DES TECHNOLOGIES D'IA SUR LA SOUVERAINETÉ DES DONNÉES DES PAYS AFRICAINS

L'encadrement de l'Intelligence Artificielle (IA) est bien plus qu'un effet de mode. Les récentes adoptions en Europe de la première réglementation en la matière, ainsi que les initiatives au niveau de l'Union Africaine pour une stratégie de réglementation continentale, en témoignent. L'utilisation des technologies d'IA est aujourd'hui perçue comme synonyme d'innovation et de compétitivité dans une ère où le marché numérique est dominé par des fournisseurs occidentaux. Fort de ce constat, il est crucial de s'interroger sur la capacité pour l'Afrique à tirer son épingle du jeu en matière d'IA et à rester souveraine face aux géants occidentaux.

Une opportunité de développement indéniable pour le continent

En 2019, Google ouvrait son premier centre de recherche sur l'IA sur le continent africain, à Accra. Depuis lors, dans la capitale ghanéenne, les applications de l'IA au développement du pays sont multiples et touchent les domaines de l'agriculture, de la santé et de l'éducation.
L'IA se révèle particulièrement bénéfique pour les agriculteurs locaux. Un projet aide les producteurs ghanéens de noix de cajou à utiliser des véhicules aériens sans pilote dans le cadre d'une innovation en matière de détection des maladies basée sur l'IA. Un autre projet utilise l'IA pour aider les petits exploitants agricoles du Ghana à prévoir les pénuries et les excédents après la récolte, contribuant ainsi à accroitre la sécurité alimentaire de la région.

Bien qu'elle soit encore émergente, l'IA est sans aucun doute en train de transformer les secteurs de l'économie africaine. Selon un récent article d'Africa Renewal, un journal numérique local des Nations Unies, l'IA a le potentiel de contribuer à hauteur de 15 700 milliards de dollars à l'économie mondiale d'ici 2030, dont 1 200 milliards de dollars pourraient être générés en Afrique, ce qui représente une augmentation de 5,6 % du Produit intérieur brut du continent d'ici 2030.



Les risques d'une IA africaine « made by others »

Les données, en particulier les données personnelles, sont au cœur des systèmes d'intelligence artificielle (IA), jouant un rôle essentiel tant dans leur développement que dans leur utilisation. Dans le contexte du développement des systèmes d'IA, la représentativité des données africaines revêt une importance capitale pour garantir un progrès équitable et pertinent de ces technologies sur le continent. Actuellement, de nombreuses bases de données utilisées par les systèmes d'IA sont largement constituées de données provenant de régions occidentales, ce qui entraîne un déséquilibre et des biais dans les résultats et les décisions engendrés par ces systèmes.

En outre, la dépendance aux technologies d'IA occidentales dans le cadre des services publics peut conduire à une perte de contrôle et de souveraineté des gouvernements sur les données des Africains. Cette dépossession de souveraineté expose potentiellement les données sensibles et les infrastructures critiques à des risques de sécurité et de confidentialité accrus, ou même à une surveillance étrangère, mettant ainsi en péril la sécurité nationale et individuelle.

Vers le développement d'une IA africaine

Selon Seydina Ndiaye, enseig-

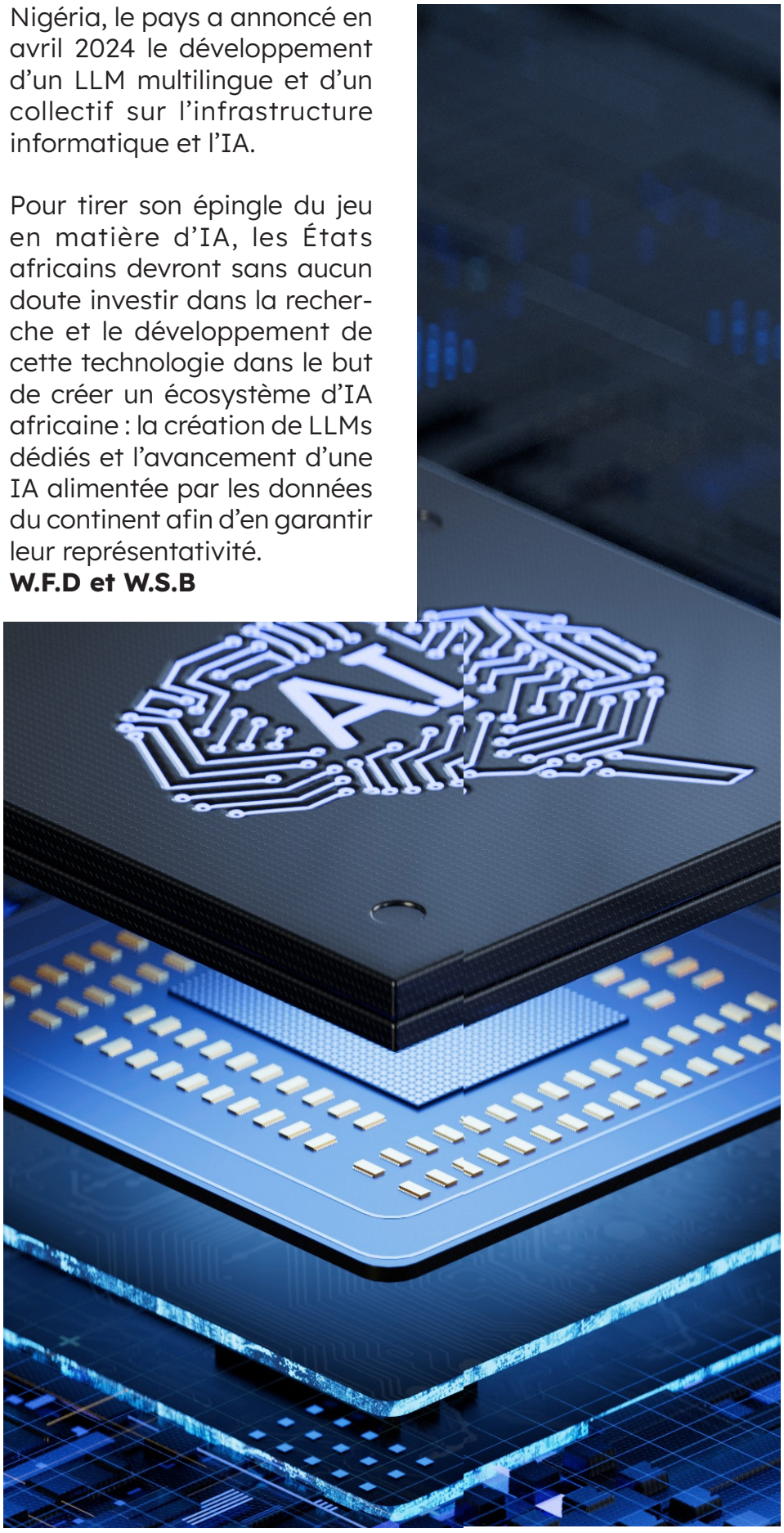
nant chercheur à l'Université numérique Cheikh Hamidou KANE au Sénégal et membre du Conseil consultatif de l'ONU sur l'IA, investir dans l'IA se traduit par deux aspects importants : la recherche pure et dure visant à développer de nouveaux modèles d'IA, et l'utilisation des avancées technologiques actuelles dans le domaine de l'IA pour tenter de résoudre les problématiques contemporaines.

Si le deuxième aspect concerne davantage la bonne gouvernance et la maitrise de la technologie, le succès du premier nécessitera de la part des dirigeants africains un investissement conséquent dans la recherche et le développement liées à l'IA, ce qui peut s'avérer couteux. Cependant, le secteur privé s'engage d'ores et déjà dans le développement de nouveaux grands modèles de langages (LLM, de l'anglais "Large Language Models"). Nous notons notamment le projet 2A2I initié au Maroc, une initiative communautaire visant à exploiter les technologies de l'IA pour réduire la fracture technologique en développant les applications d'IA pour l'arabe en les alignant sur les avancées mondiales dans le paysage de l'IA en anglais.

Du côté des États, nous soulignons à titre illustratif, le lancement récent du processus d'élaboration d'une stratégie de l'IA au Kenya. À la suite d'un projet initial de stratégie nationale en matière d'IA au Nigéria, le pays a annoncé en avril 2024 le développement d'un LLM multilingue et d'un collectif sur l'infrastructure informatique et l'IA.

Pour tirer son épingle du jeu en matière d'IA, les États africains devront sans aucun doute investir dans la recherche et le développement de cette technologie dans le but de créer un écosystème d'IA africaine : la création de LLMs dédiés et l'avancement d'une IA alimentée par les données du continent afin d'en garantir leur représentativité.

W.F.D et W.S.B



GITEX AFRICA Morocco X NORTH STAR AFRICA Morocco

CO-LOCATED WITH WORLD FUTURE HEALTH AFRICA

29 - 31 MAY 2024 MARRAKECH

VISIT THE LARGEST TECH SHOW IN AFRICA

GITEXAFRICA.COM

GITEX AFRICA features every major technology player. Visit the vibrant landscape of the global tech that will shape Africa's future. Whetheryou are looking to source products, create valuable networks, gain industry knowledge, you'll encounter unparalleled opportunities.

VISIT GITEX AFRICA

UNDER THE AUTHORITY OF
Kingdom Of Morocco
Head Of Government
Ministry Of Digital Transition and Administration Reform

HOSTED BY
#ADD Digital Development Agency

ORGANISED BY
KAOUN INTERNATIONAL

FIND YOUR WORLD
GITEX AFRICA Morocco | GITEX GLOBAL DUBAI | GITEX EUROPE Berlin

INTERVIEW DE DRUDEISHA MADHUB, COMMISSAIRE À LA PROTECTION DES DONNÉES DE MAURICE

Maurice est devenu un leader africain dans le domaine de la protection des données, grâce à son engagement constant envers des normes élevées de confidentialité et de sécurité des données. En dotant le pays d'une législation dédiée à la protection des données et en ratifiant la convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, le travail accompli par la Data Protection Commissioner a joué un rôle crucial dans le renforcement de la confiance des entreprises et des investisseurs internationaux dans l'économie mauricienne.

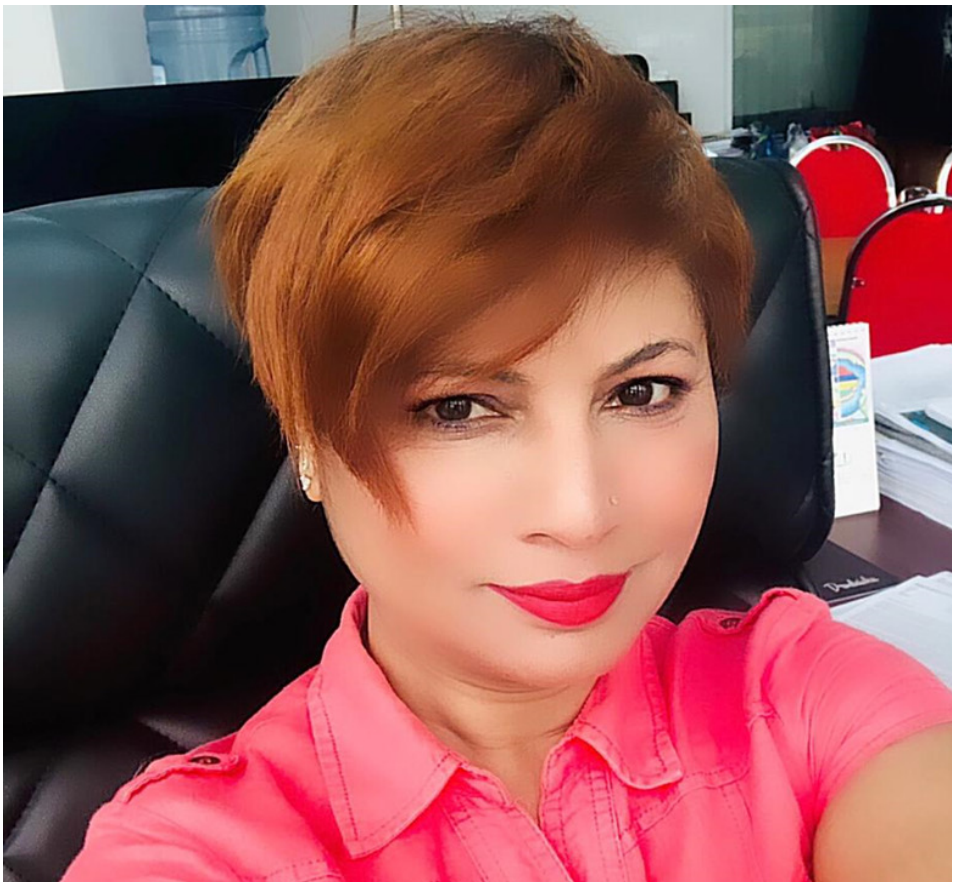
Comment la loi sur la protection des données de 2017 se compare-t-elle aux normes internationales en matière de protection des données ?

Maurice a promulgué la loi sur la protection des données 2017 (DPA), qui est entrée en vigueur le 15 janvier 2018, pour s'aligner sur les normes internationales à savoir : le Règlement général sur la protection des données de l'Union européenne, la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) et le Protocole portant amendement à la Convention pour la protection des personnes à l' égard du traitement automatisé des données à caractère personnel (Convention 108+).

Maurice a pris divers engagements internationaux en matière de protection des données :

a) Maurice a été le premier État africain à ratifier la Convention 108 du Conseil de l'Europe, depuis le 1er octobre 2016.

b) Maurice a également été le premier État non européen à



ratifier la Convention 108+, le 4 septembre 2020.

c) Enfin, la ratification par Maurice de la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles (Convention de Malabo) a eu lieu le 14 mars 2018.

Notre pays adhère également à la Déclaration des droits de l'homme des Nations unies, au Pacte international relatif aux droits civils et politiques et à la Convention sur la cybercriminalité (Convention de Budapest), ce qui a conduit à la promulgation de la loi sur la cybersécurité et la cybercriminalité en 2021 à Maurice.

Ainsi, le 7 décembre 2023, le rapporteur spécial des Nations Unies sur le droit à la vie privée a cité notre pays comme modèle : "Maurice est un exemple à suivre dans la régi-

on africaine car elle s'est alignée sur le cadre de l'UE...". Malgré cela, des défis subsistent.
Le DPD a préparé et soumis un rapport complet en 2022, conformément aux exigences d'adéquation établies par l'UE, afin que la Commission européenne procède à une évaluation objective de la protection des données à Maurice.
En 2023, la Commission européenne a donné le coup d'envoi d'une série de réunions de discussion avec le Bureau sur des éléments thématiques de la loi sur la protection des données, afin de proposer d'éventuelles modifications à apporter au DPA. Le Bureau attend le rapport final de la Commission européenne.
Enfin, Maurice a également participé au projet Prida de l'Union Africaine (UA) et est actuellement engagée avec celle-ci dans d'autres initiatives au niveau africain.

Quels sont les principaux défis auxquels votre autorité est confrontée pour protéger les données des citoyens mauriciens ?

Les principaux défis auxquels le Bureau de protection des données doit faire face pour protéger les données des citoyens mauriciens sont les suivants :
a) Indépendance financière
Le Bureau de la protection des données opère sous l'égide du ministère des Technologies de l'information, de la Communication et de l'Innovation. En vertu de la loi de 2017 sur la protection des données, le commissaire à la protection des données jouit d'une indépendance fonctionnelle. Par conséquent, il n'y a pas d'interférence du ministère ou de toute autre autorité concernant les fonctions du commissaire. Cependant, le Bureau de la protection des données n'a pas d'indépendance financière et son budget est centralisé au sein de son ministère de tutelle. Ce manque d'autonomie financière limite la capacité du Bureau à garantir efficacement les droits des personnes en matière de protection des données.
b) Manque de ressources humaines
Le Bureau manque cruellement de personnel technique, alors que la complexité du travail exige un haut niveau de compétence et d'expertise pour mener des audits, des évaluations d'impact sur la protection des données, des certifications et remplir d'autres fonctions.
c) Application de la loi
Le Bureau manque d'officiers de police, ce qui entrave sa capacité à exécuter efficacement les mesures d'application, telles que l'émission de sanctions, la mise en place d'enquêtes sur les plaintes et les poursuites pénales.

Quels sont les domaines spécifiques dans lesquels la protection des données est particulièrement importante à Maurice, et quelles sont les mesures prises par votre autorité sur ces questions ?

Bien que la protection des données soit cruciale dans tous les secteurs, elle revêt une importance particulière dans diverses industries et domaines à Maurice, notamment les services financiers, les soins de santé et les services gouvernementaux. Dans le secteur des services financiers, par exemple, il est impératif de garantir la protection des données pour maintenir la confiance, étant donné la nature sensible des informations financières, telles que les coordonnées bancaires et les transactions.

Le Bureau de la protection des données a adopté une approche proactive en fournissant des guides essentiels dans ces domaines.
a) Par exemple, le Bureau a rédigé un guide intitulé "Protection des données dans le secteur financier mauricien", qui sera bientôt publié. Dans ce guide, le Bureau se penche sur l'importance critique de la protection des données dans le secteur financier au milieu des violations de données et des cyber-menaces, qui peuvent avoir des conséquences financièrement dévastatrices et catastrophiques pour la réputation. Ce guide transmet également des connaissances, des bonnes pratiques et des idées sur la protection des données pour les institutions (publiques et privées) du secteur financier. Il vise à fournir des conseils sur le traitement des données personnelles eff-

ectué par les entités financières, afin d'assurer la conformité avec les principes de protection des données en vertu de la loi mauricienne sur la protection des données. Le guide a été rédigé après consultation des parties prenantes du secteur financier.

b) Pendant la pandémie de COVID-19, le Bureau a également publié un guide intitulé "Data Protection for Health Data and Artificial Intelligence Solutions in the context of the COVID-19 pandemic" (Protection des données de santé et des solutions d'intelligence artificielle dans le contexte de la pandémie de COVID-19). Ce guide détaille une approche recommandée pour assurer la conformité avec le DPA pendant la pandémie. En outre, le Bureau a formulé des recommandations sur l'intelligence artificielle et les applications mobiles.

c)Le Bureau a également publié un guide sur la sécurité nationale et la vie privée, qui examine les implications des projets de sécurité nationale sur la vie privée, notamment les dispositions relatives à la sécurité nationale dans le DPA. Le guide contient également plusieurs recommandations à l'attention des responsables du traitement et des sous-traitants. Ces recommandations comprennent l'adoption de pratiques conseillées en matière de respect de la vie privée dans le cadre des projets de sécurité nationale.

d) Enfin, le Bureau a publié un code de pratique pour l'exploitation des systèmes de villes sûres exploités par la police mauricienne. Il définit les conditions de base pour l'utilisation de ces systèmes, conformément aux dispositions de la loi sur la protection des données de 2017 (DPA).

Le Bureau entreprend une panoplie d'actions de conformité et d'application, publiées dans nos rapports annuels.

La Convention de Malabo sur la cybersécurité et la protection des données est devenue effective en juin 2023, neuf ans après son adoption par l'Union africaine en 2014. Comment allez-vous la mettre en œuvre ?

Maurice a déjà établi son cadre juridique avec la loi sur la protection des données, en vigueur depuis janvier 2018. En outre, le Bureau de la protection des données est opérationnel depuis 2009.

La mise en œuvre de la Convention de Malabo sur la cybersécurité et la protection des données nécessitera en outre la collaboration des États membres pour faciliter :

a) Le renforcement des capacités : Les États membres doivent investir dans des initiatives de renforcement des capacités afin de s'assurer qu'ils disposent de l'expertise et des ressources nécessaires pour mettre en œuvre efficacement la convention. Il peut s'agir de programmes de formation, d'ateliers et d'une assistance technique de la part d'organisations internationales.

b) La coopération internationale : La collaboration et le partage d'informations entre les États membres de l'UA sont essentiels. Les États membres doivent rester souples et adaptables dans leur approche de la protection des données.

Plusieurs discussions sur l'intelligence artificielle (IA) sont en cours en Afrique. Comment votre autorité traite-t-elle les préoccupations éthiques liées à l'utilisation de l'IA ?

En tant que commissaire à la protection des données, j'ai participé à divers panels et je suis intervenue lors de nombreuses conférences pour partager les meilleures pratiques concernant les préoccupations éthiques liées à l'utilisation de l'IA. J'ai également publié un article intitulé "AI : a future-proof force or undermining power" (L'IA : une force d'avenir ou une puissance de destruction) à la suite d'une demande reçue par le Bureau de la part d'une entreprise privée. En outre, le Bureau prévoit d'élaborer cette année un guide sur la protection des données et l'IA générative.

Propos recueillis par Jules Hervé Yimeumi

L'AUTORITÉ DE PROTECTION DES DONNÉES INFORMÉE DE LA COMPROMISSION DE LA SÉCURITÉ INFORMATIQUE DE LA COMMISSION ÉLECTORALE INDÉPENDANTE

Par Franck ADOPO

La sécurité des systèmes informatiques en Afrique : faut-il attendre le pire avant de réagir ? Après la compromission du système informatique du ministère de la Justice en Afrique du Sud, c'est au tour de la Commission électorale indépendante (CEI) de subir une violation de données. Cependant, il s'agit cette fois de données beaucoup plus sensibles : des données électorales.
À la veille de la tenue des élections générales, prévues pour le 29 mai 2024 prochain, une nouvelle affaire vient fragiliser le dispositif électoral sud-africain déjà tendu en raison de tensions sociales et politiques grandissantes dans le pays.

De quoi s'agit-il ?

Le 11 mars 2024, la CEI, organe créé par la constitution chargée d'organiser les élections en Afrique du Sud, a informé l'autorité de protection des données (le Régulateur) de la compromission de son système informatique. Cette attaque a conduit à la publication non autorisée des noms de certains candidats de deux partis politiques en lice, et non des moindres, pour les élections législatives imminentes. Il s'agit du parti historique l'African National Congres (le parti ANC) et le parti uMkhonto we Sizwe (le parti MK), deux partis politiques rivaux qui ont pour ambition de remporter les élections et sont au cœur de toutes les polémiques en ce moment. Cette violation de données électorales soulève des questions non seulement en termes d'enjeux juridiques, mais aussi d'enjeux sociopolitiques.

La réaction de la CEI et la réponse du Régulateur

Après avoir pris connaissance de la violation des données électorales sous son contrôle, la CEI a notifié la fuite de données au Régulateur, comme exigé par l'article 22 de la loi sud-africaine sur la protection des renseignements personnels (POPIA).
De son côté, le Régulateur a bien reçu la notification de la CEI, mais l'a jugée incomplète. En effet, à la suite d'une fuite de données, la notification de violation de données est censée respecter un certain formalisme et contenir des informations prévues par la POPIA. Selon le communiqué publié par le Régulateur, la CEI aurait enfreint les règles prévues dans la procédure de notification. Le Régulateur a alors renvoyé une note d'information à la CEI afin qu'elle lui fournisse dans sa notification des informations complémentaires sur la violation concernée. Cette note d'information supplémentaire n'ayant pas été rendue publique, il est donc difficile de connaître le délai dont dispose la CEI pour r-

© iStock

éagir. Cependant, dans sa communication, le Régulateur rappelle les informations à fournir afin de vérifier si la CEI a bien respecté ses obligations de responsable de traitement.

Que dit la loi sud-africaine en matière de violation de données ?

Il faut tout d'abord se poser la question de l'applicabilité de la POPIA à l'activité de la CEI. C'est l'article 3 de la POPIA qui établit les conditions de son application. Cette loi s'applique entre autres aux activités de traitement de données réalisées sur le territoire sud-africain. Puis, au titre des exclusions, il faut préciser que la loi ne s'applique pas aux traitements effectués par un organisme public ou pour le compte de celui-ci dans des cas bien déterminés par la loi : il peut s'agir de la sécurité nationale ou encore de la lutte contre les activités illégales. Cependant, le processus électoral ne fait pas partie des exclusions prévues par la POPIA. La CEI est donc une institution soumise à cette loi. C'est à juste titre qu'elle a entamé la procédure de notification conformément à la loi. Mais c'est aussi à bon droit que le Régulateur poursuit cette affaire afin de situer les responsabilités.

En ce qui concerne l'obligation de confidentialité et de sécurité des données, elle est prévue par l'article 19 de la POPIA. En vertu de cette obligation, le responsable de traitement doit garantir l'intégrité et la confidentialité des données qu'il traite. Cette obligation se matérialise par la mise en place de mesures techniques et organisationnelles appropriées pour empêcher la perte, l'accès illicite ou encore la destruction non autorisée des données. En l'espèce, la CEI avait l'obligation de prendre ces mesures techniques et organisationnelles selon l'état de l'art afin d'empêcher que les données personnelles des candidats, mais aussi des électeurs, soient divulguées avant les publications officielles par les autorités et instances compétentes. Néanmoins, les données des candidats de l'ANC et du parti MK ont été dévoilées illicitement. La CEI a donc manqué à son obligation de confidentialité et de sécurité des données.

Après la survenance d'une violation de données, l'article 22 de la POPIA rappelle la procédure obligatoire à suivre. Le responsable de traitement doit procéder, dès qu'il a connaissance de cette situation, à une notification au Régulateur et aux personnes concernées. Dans ce dernier cas, cette notification peut être retardée en cas de procédure criminelle en cours. Les supports de cette notification peuvent être divers : il peut s'agir d'un envoi postal ou de courriel, d'une notification de manière publique sur le site internet du responsable de traitement ou dans les médias publics. En l'espèce, la CEI a entamé une procédure similaire. Toutefois, c'est la complétude de cette démarche qui est remise en cause par le Régulateur. Il estime que les informations fournies sont insuffisantes pour établir clairement les causes et les implications de cette fuite de données. Les sanctions encourues par les organismes de traitement de données en vertu de la loi sud-africaine ont été détaillées dans notre rapport de janvier dernier. Cependant, il est important de se demander, dans le cas où l'autorité parviendrait à établir la responsabilité de la CEI, si celle-ci restera constante dans ses décisions.
En effet, ira-t-elle aussi loin qu'elle l'a récemment fait dans l'affaire de la violation de données du ministère de la Justice? Elle avait alors enjoint à la CEI de prononcer des sanctions disciplinaires contre les fonctionnaires responsables de cette fuite de données électorales en raison de la gravité de l'affaire et le caractère sensible des données ? La réponse à cette question ne sera connue que lors de la décision finale du Régulateur dans cette affaire.

Cette deuxième affaire concernant la violation de données traitées par les institutions doit servir à tirer la sonnette d'alarme. Elle est la triste preuve que la sécurisation des infrastructures informatiques, des entreprises, et des institutions en Afrique n'est pas un choix, mais un impératif. Cette question a une importance capitale non seulement pour l'économie, mais aussi pour le bon fonctionnement des États et de la démocratie. Elle doit occuper l'agenda des politiques.
La protection des données doit être un sujet de politique nationale, car les menaces pour la stabilité des États ne sont plus seulement physiques, mais aussi informatiques.
Il est temps de renforcer les frontières informatiques des États et des institutions en Afrique.
F.A

LA COMMISSION NIGÉRIANE DE PROTECTION DES DONNÉES PUBLIE UNE NOTE SUR L'ENREGISTREMENT DES RESPONSABLES DE TRAITEMENT ET DES SOUS-TRAITANTS

Par Justin Yao KOUMAKO

© iStock

Conformément à l'article 5 (d) de la nigerian data protection act de juin 2023 (NDPA, ci-après la loi nigériane sur la protection des données), l'une des missions principales de l'autorité de contrôle, la NDPC (ci-après la Commission), est de désigner les responsables de traitement et les sous-traitants (ci-après RT/ST) dits d'importance majeure qui doivent être soumis à l'obligation d'enregistrement auprès de la Commission. Dans une note en date du 14 février 2024, la Commission a publié ses orientations relatives à l'enregistrement.

Notion de RT/ST d'importance majeure et obligations d'enregistrement.

La notion de RT/ST d'importance majeure est définie à l'article 65 de la loi nigériane sur la protection des données comme un RT/ST « domicilié, résidant ou opérant au Nigeria et traitant ou ayant l'intention de traiter les données à caractère personnel d'un nombre de personnes concernées supérieur à celui fixé par la Commission, ou toute autre catégorie de RT/ST traitant des données à caractère personnel d'une valeur ou d'une importance particulière pour l'économie, la société ou la sécurité du Nigeria, telle que désignée par la Commission ». Cet article crée deux critères susceptibles d'être retenus par la Commission pour la désignation des RT/ST d'importance majeure : le critère principal du territoire (domiciliation, résidence ou activité au Nigéria), qui doit être cumulé avec un critère accessoire du nombre de personnes concernées, ou celui de la sensibilité du traitement pour l'économie, la société ou la sécurité nigériane. Dans sa note d'orientation, la Commission a

établi qu'un RT/ST domicilié, résidant ou exerçant une activité au Nigéria est considéré comme d'importance majeure dès lors qu'il traite des données de plus de 200 personnes concernées en 6 mois (article 1§a de la note d'orientation), ou s'il est un fournisseur de services TIC sur des appareils dotés de capacité de stockage (par exemple les entreprises de téléphonie mobile). La Commission a fait évoluer ces critères en dégageant un nouveau critère lié au secteur d'activité. Ainsi, les organisations ou les fournisseurs de services dans les domaines suivants sont des RT/ST d'importance majeure : finance, communication, santé, éducation, assurance, import, export, aviation, tourisme, pétrole et gaz, électricité.

L'article 44 oblige les RT/ST d'importance majeure à procéder à leur enregistrement dans les six mois suivant l'entrée en vigueur de la loi, ou dès leur désignation comme tels. L'enregistrement se fait par notification à la Commission des informations précises fixées par l'article 44§2 de la loi nigériane sur la protection des données. A titre comparatif, la liste d'informations à notifier à la Commission ressemble aux dispositions de l'article 30 du RGPD qui prévoit le registre des activités de traitement. Ainsi, l'article 44 semble mettre à la charge des RT/ST d'importance majeure l'obligation de rédiger une sorte « fiche de registre » focalisé sur le RT/ST et une description succincte de ses traitements.

Le RT/ST d'importance majeure a l'obligation de notifier tout changement significatif à la Commission dans un délai de 60 jours, soit deux mois. La liste des RT/ST d'importance majeure constitue un registre, une sorte de document administratif communicable, que la Commission doit publier sur son site internet.

Classification des responsables de traitement et des sous-traitants d'importance majeure.

La Commission classe les RT/ST d'importance majeure en trois catégories de traitement des données : Major Data Processing-Ultra High Level (MDP-UHL), Major Data Processing-Extra High Level (MDP-EHL), Major Data Processing-Ordinary High Level (MDP-OHL). Sans nous embarrasser de traduction des termes retenus, il convient de noter que les MDP-UHL sont tenus, entre autres obligations, de respecter les standards les plus élevés en matière de protection des données alors que les MDP-EHL et les MDP-OHL doivent se soumettre aux bonnes pratiques classiques en la matière. Pour chaque catégorie, un faisceau d'indices permet de déterminer la catégorie dans laquelle une organisation pourrait s'inscrire.

Concrètement, les banques commerciales, les sociétés de télécommunications, les compagnies d'assurance, les entreprises multinationales, les sociétés de distribution d'électricité, les sociétés pétrolières… rentrent dans la catégorie des MDP-UHL. Les MDP-EHL sont les services publics (ministères, départements, agences gouvernementales), les structures hospitalières fournissant des services médicaux tertiaires et secondaires, les hautes institutions, les microfinances… ainsi que tout RT/ST d'importance majeure traitant semestriellement des données de plus de 1000 personnes concernées. Enfin, la dernière catégorie, les MDP-OHL, correspond aux PME/TPE, aux écoles primaires et secondaires, … et tout RT/ST d'importance majeure traitant semestriellement des données de plus de 200 personnes concernées.
L'enregistrement auprès de la Commission est payant, et les frais associés varient selon la catégorie de RT/ST d'importance majeure.

Régime financier applicable aux RT/ST d'importance majeure selon leur classification.

Les frais d'enregistrement sont fixés à 250 000 Naira pour les MDP-UHL (200€), 100 000 Naira (80€) pour les MPD-EHL et 10 000 Naira (8€) pour les MPD-OHL.

Impératif de délai.

Les RT/ST existants qui rentrent dans la catégorie d'importance majeure ont l'obligation de se faire enregistrer entre janvier et juin 2024. En effet, le défaut d'enregistrement peut être sanctionné par la Commission.

En somme, la note d'orientation sur l'enregistrement des RT/ST d'importance majeure vient renforcer l'effectivité de la loi et situer les acteurs sur les premières formalités que la loi leur impose.
J.Y.K

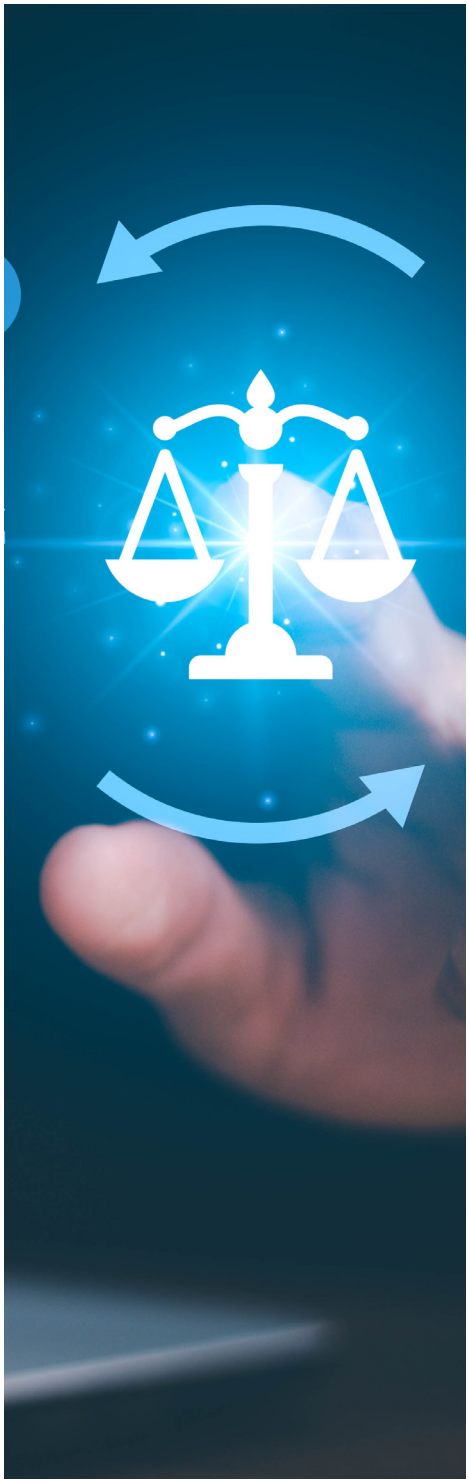
L'AUTORITÉ DE PROTECTION DES DONNÉES RAPPELLE AUX RESPONSABLES DE TRAITEMENT ET AUX CORRESPONDANTS À LA PROTECTION DES DONNÉES LEURS OBLIGATIONS EN TERMES DE COMMUNICATION D'INFORMATIONS

Par Arnaud NADINGA

Dans un communiqué daté du 16 février 2024, l'Autorité de Régulation des Télécommunications/TIC Côte d'Ivoire (ARTCI), Autorité de protection des données à caractère personnel de la République de Côte d'Ivoire, a tenu à rappeler aux responsables de traitement et aux correspondants à la protection des données (CPD), leurs obligations en matière de « communication de documents ». Le communiqué se rapporte précisément à la production et à la communication du Rapport annuel des activités de traitement du responsable du traitement.

En effet, l'article 42 de la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel impose à tout responsable du traitement, d'« d'établir un Rapport annuel pour le compte de l'Autorité de protection des données sur le respect des dispositions annoncées à l'article 41 » de la même loi. Ce rapport est plus qu'un simple document administratif. Il s'agit d'un outil de transparence et de conformité. D'une part, en tant qu'instrument de transparence, il offre, par son contenu, à l'Autorité de protection, une vue d'ensemble sur les traitements réalisés au cours de l'année par un responsable de traitement. Il doit notamment contenir, selon le modèle rendu public par l'ARTCI, une liste des traitements, une fiche détaillée de chaque traitement et un tableau des tâches (demandes d'accès, plaintes, demandes de modification, failles de sécurité...) sur les traitements. D'autre part, comme le souligne la disposition ci-dessus, il doit également permettre au responsable du traitement de faire état des mesures prises pour se conformer aux exigences issues de la loi sur la protection des données à caractère personnel. C'est ce qu'exprime le renvoi fait à l'article 41 de la loi. Le rapport doit contenir des informations sur le respect des exigences issues de cette disposition qui énumère en une dizaine de points un certain nombre d'obligations à la charge du responsable du traitement. Ces obligations expriment dans l'ensemble l'idée que le responsable du traitement est tenu de mettre en œuvre des mesures techniques et organisationnelles afin d'assurer la sécurité des installations servant aux traitements et des données personnelles traitées, mais aussi l'intégrité et la disponibilité desdites données.

Le modèle de rapport d'activité du CPD rendu public par l'Autorité de protection sur son site web précise, par un renvoi à l'article 13, alinéa 2 de l'arrêté n° 511/MPTIC/CAB du 11 novemb-



© iStock

re 2014 portant définition du profil et fixant les conditions d'emploi du correspondant à la protection des données à caractère personnel, que la production du rapport annuel est à la charge de ce dernier. Il est tenu, aux termes de cette dernière disposition, de produire en fin d'année, un rapport de ses activités qu'il présente au responsable du traitement et expédie copie à l'ARTCI pour information.

L'Autorité de protection souligne par ailleurs que la communication du rapport doit intervenir au plus tard le 31 mars de l'année suivant l'exercice écoulé. Le défaut de communication est considéré comme un refus de communication à l'Autorité de protection des documents utiles à sa mission. Pour rappel, aux termes de l'article 45 de la loi relative à la protection des données à caractère personnel, le refus de communiquer aux membres ou aux agents de l'autorité de protection, les renseignements et documents utiles à leur mission, la dissimulation desdits documents ou renseignements ou le fait de les faire disparaître est puni d'une peine d'emprisonnement d'un mois à deux ans et d'une amende de 1 000 000 à 10 000 000 de francs CFA.

A.N

© iStock

DE L'UTILISATION DES DISPOSITIFS MÉDICAUX EMBARQUANT DE L'IA EN AFRIQUE SUB-SAHARIENNE : AVERTISSEMENT SUR LA DOUBLE PÉNALITÉ POUR LES FEMMES NOIRES ET AFRO-DESCENDANTES

Par Prof. Benjamin C. GUINHOUYA

L'intelligence artificielle (IA) est très prometteuse pour transformer la médecine clinique, la santé publique, la recherche en santé et les services de soins en assurant des diagnostics, des stratégies préventives et des pronostics plus rapides, plus abordables et plus précis. Ces dernières années, des organismes de régulation tels que la Food and Drug Administration (FDA) des États-Unis et la Commission européenne ont approuvé plusieurs appareils d'IA à usage clinique. A titre d'illustration, au mois d'Octobre 2023, 700 dispositifs médicaux (DM) intégrant de l'IA ont reçu une autorisation de mise sur le marché par la FDA américaine. Ceci indique clairement une tendance croissante de l'intégration de l'IA dans les soins de santé.

Le recours de l'écrasante majorité des systèmes d'IA (SIA) actuels à des algorithmes basés sur des données présente quelques risques, en particulier lors de leur utilisation pour des populations différentes de celles dont les données ont été utilisées lors des phases d'entraînement et de validation des SIA. Par exemple, les algorithmes construits principalement sur les données obtenues de populations caucasiennes (à peau claire) peuvent avoir du mal à diagnostiquer avec précision les affections des personnes à la peau plus foncée (exemple : populations africaines), exacerbant ainsi les disparités diagnostiques existantes.

Un autre aspect qui devrait faire l'objet d'une attention constante concernant la santé des femmes. En effet, la santé des femmes est l'objet d'une dissymétrie par rapport à celle des hommes dans la recherche (bio) médicale ; les traitements, les essais cliniques et autres tests étant principalement développés à partir de modèles masculins. Cette lacune des connaissances médicales concernant la santé des femmes est de plus en plus admise et reconnue. Et c'est justement en raison de différences entre les sexes dans la manifestation de certaines maladies et la réponse à certains traitements, que les femmes font souvent face à une moindre efficacité des thérapeutiques qui leur sont prescrites, et qu'elles sont plus enclines à signaler davantage d'effets indésirables liés aux médicaments, y compris des effets indésirables graves. Une étude danoise récente a mis en évidence des retards de diagnostic importants chez les femmes pour plus de 700 maladies, dont le cancer et le diabète. C'est d'autant plus important que des études antérieures ont montré que les erreurs de diagnostic, à elles seules, peuvent représenter près de 60% de toutes les erreurs médicales, avec environ 40 000 à 80 000 décès chaque année.

Ces défis sont particulièrement prégnants pour les femmes africaines et afro-descendantes, qui peuvent être confrontées à la double discrimination raciale et sexiste. Par exemple, dans un travail publié en 2018, Buolamwini et Gebru ont montré sur le plan intersectionnel, lorsqu'on croise les discriminations raciales et sexistes, que les pires performances de trois systèmes de reconnaissance faciale étaient obtenues avec les femmes noires (avec des taux d'erreur allant jusque 35%) alors que les hommes blancs étaient les mieux classés (Taux d'erreur de 0.8%) suivis par les femmes blanches et les hommes noirs, avec respectivement des taux d'erreur de 7% et 12%.

Bien que ce type d'observation

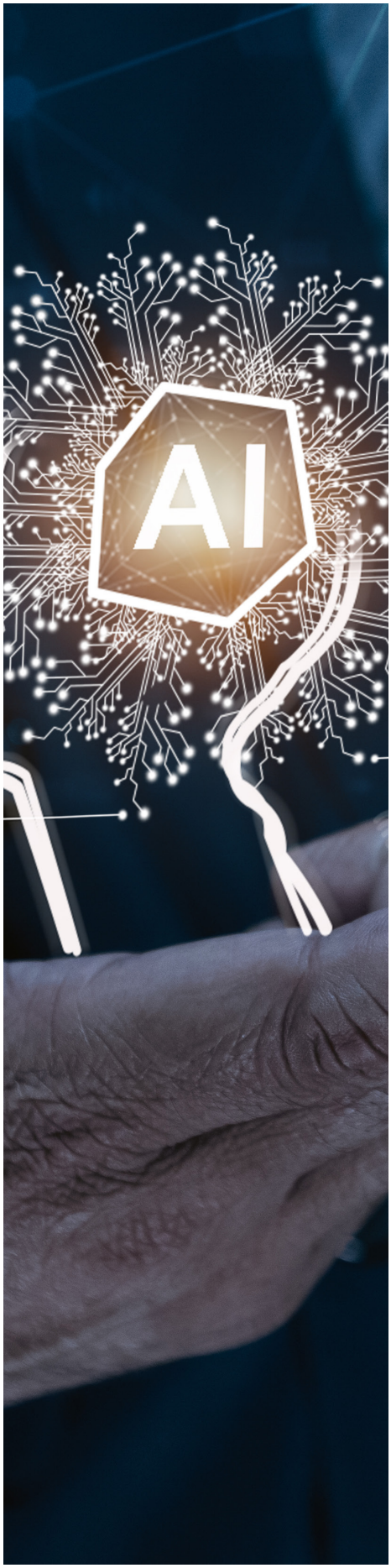
© iStock

ne soit pas encore très répandu dans la littérature (bio)médicale en raison de la récence de la pénétration des DM embarquant de l'IA sur le marché, on ne peut s'empêcher de craindre la matérialisation de ce risque de double pénalité pour la santé des femmes africaines et afro-descendantes. Par exemple, un article récent explorant l'utilisation de l'IA pour poser un diagnostic à partir d'images de radiographie de poitrine a révélé, bien que l'algorithme ait été entraîné à partir de milliers d'images, un sous-diagnostic de groupes ethniques/raciaux minoritaires. Ceci serait particulièrement manifeste chez les noirs et les hispaniques comparativement aux caucasiens. Il est également reconnu aux Etats-Unis que les personnes noires ou afro-descendantes ont moins de chance d'avoir un diagnostic précoce dans le cas d'un cancer du poumon, comparativement aux populations caucasiennes.

Il convient donc, lors de l'utilisation de dispositifs d'importation en Afrique sub-saharienne, d'anticiper ce type de risque d'autant que non seulement il y a une pénurie de données de santé numérisées ainsi que de connaissances médicales spécifiques de la santé des femmes en provenance de l'Afrique sub-saharienne, mais il est également à remarquer le peu voire l'absence de représentation africaine dans l'élaboration des SIA en développement, en particulier dans le domaine de la santé.

Malgré les efforts en cours pour construire des stratégies d'IA dans quelques pays sur le continent, il est clair au regard des résultats de l'indice global de l'IA, que l'Afrique en général, et l'Afrique sub-saharienne en particulier est loin d'être prête pour mettre au point ses propres solutions d'IA en santé, conçues suivant un cadre normatif pertinent. Dans les prochaines décennies, à la faveur d'une dynamique commerciale globale, associée à l'intention louable de ne pas manquer l'occasion de suivre le rythme des développements en cours dans d'autres régions du monde, que la tentation d'adoption/importation de solutions d'IA construites ailleurs soit grande. Il semble primordial dès à présent, tout au moins en ce qui concerne le domaine de la santé, que les documents stratégiques en cours d'élaboration tiennent compte de cette donne, en mettant l'emphase sur un cadre minimal d'évaluation et de domestication rigoureuse des DM embarquant de l'IA d'importation. Il convient également d'anticiper sur la sensibilisation et le remaniement du curriculum d'éducation des professionnels qui seront amenés à inclure ces solutions d'IA dans leurs pratiques. Lors de la prise en charge des femmes, ils devront veiller avec une grande acuité à ajuster leurs prises de décision clinique au potentiel d'erreurs de ces dispositifs. Enfin, les populations africaines doivent également disposer de toutes les informations/formations utiles pour pouvoir exprimer des choix de santé en conscience face à des DM potentiellement inadéquats aux caractéristiques locales, et qui auraient manqués d'intégrer les spécificités sanitaires des africaines et des afro-descendantes.

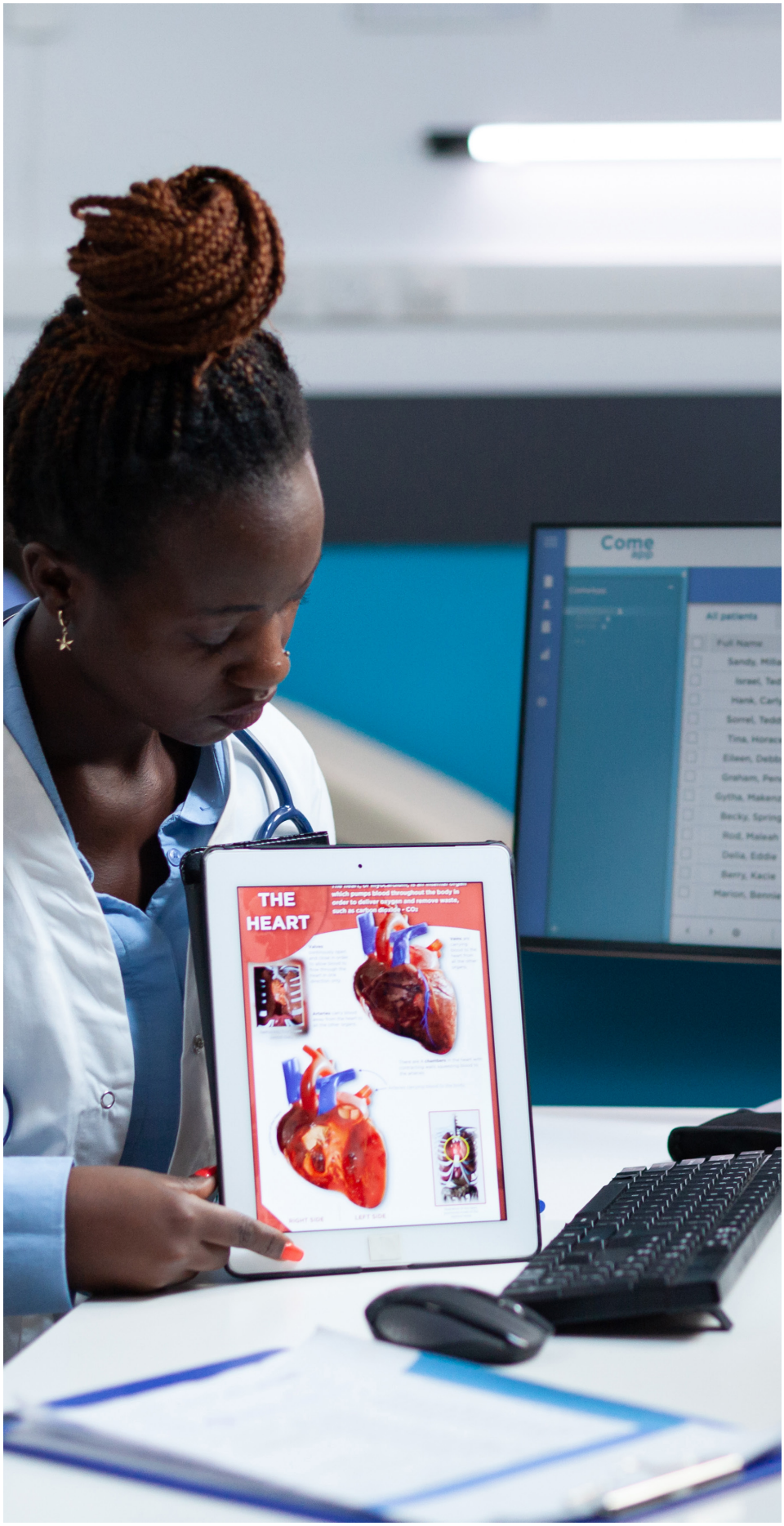
Il convient de pointer et d'insister encore une fois sur le fait que



© iStock

les données de santé, en particulier les données médicales utilisables pour le développement des DM embarquant de l'IA pouvant être utilisées en Afrique, sont non seulement des « données biaisées », mais surtout des données intrinsèquement informatives, et nécessitant des considérations autres que les tentatives techniques d'atténuation ou de correction d'un biais. En effet, ce qui est généralement considéré comme un « biais algorithmique » à l'origine d'une discrimination algorithmique fait souvent l'objet de réponses techniques à l'instar des techniques d'apprentissage fédéré (intégrant les données démographiques représentatives de plusieurs institutions), ou en procédant par imputation des données manquantes concernant certaines catégories démographiques. Ces efforts, bien intentionnés, peuvent sans doute contribuer à la modération desdits biais d'IA et de leur discrimination associée. Il est néanmoins important d'accepter le fait que les données « construites » à partir de ces procédés techniques ne peuvent qu'introduire de réels biais, liés cette fois aux choix et hypothèses faits sur les données, avec comme conséquence, la production d'un résultat biaisé reflétant davantage ces choix-là que le phénomène recherché.

Au lieu d'arguer un biais de l'IA, on peut raisonnablement concevoir les données médicales comme des « artéfacts » au sens archéologique ou historique. Les artéfacts sont des objets susceptibles de fournir des informations sur les sociétés, y compris sur les institutions, les pratiques et les valeurs. Les artéfacts sont essentiels parce

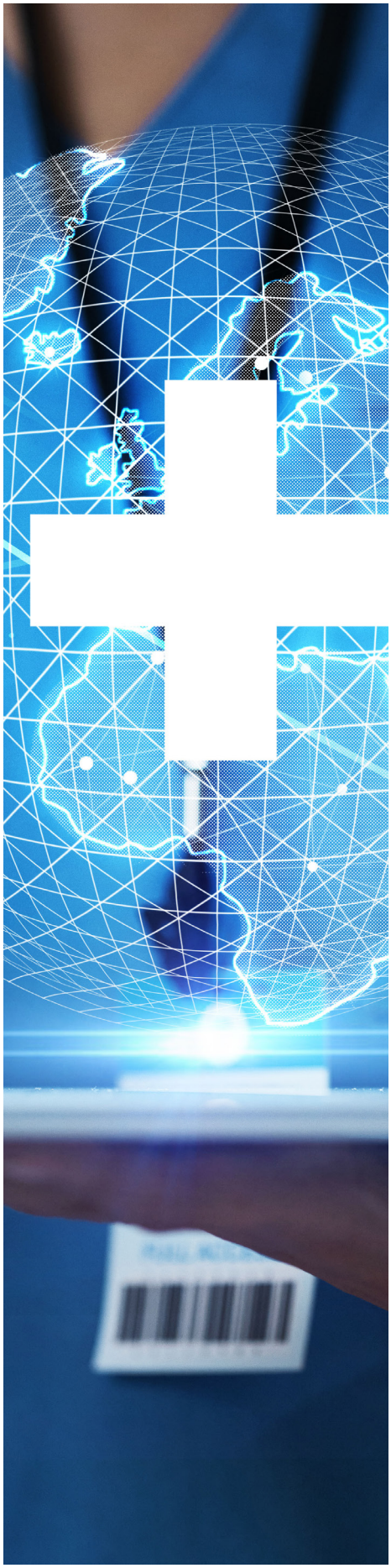


© iStock

qu'ils rendent compte des systèmes de croyance et des pratiques aussi inégalitaires soient-ils. Ainsi, les données médicales utilisables actuellement pour développer des DM embarquant de l'IA, en tant qu'artéfacts, nous mettent face à des réalités inconfortables. Si elles sont effectivement conçues comme des artéfacts informationnels, éclairant sur les valeurs sociales, les représentations sociétales et les pratiques de soin, on pourrait alors en tirer de la connaissance. On peut par exemple utiliser la puissance des algorithmes de reconnaissance de patterns pour nous aider à mieux appréhender les contextes historiques et les structures contemporaines. En outre, la considération et l'examen des données médicales comme artéfacts, pourraient conduire à imaginer et construire des alternatives techniques et/ou politiques aux approches actuelles mobilisées lors de la conception et le développement des solutions numériques en santé, y compris les DM embarquant de l'IA. Enfin, une telle reconnaissance devrait amener les cliniciens à modérer/ajuster leur attitude et/ou prise de décision face à certaines populations, surtout lorsque la décision doit être aidée par l'IA. Cette prise en compte pourrait même, à terme, avoir la vertu d'induire des changements de pratiques pour aller vers des pratiques médicales un peu plus équitables.

Pour déployer des SIA adaptés particulièrement à la santé des femmes africaines, une étape cruciale consisterait à penser à organiser les processus de numérisation des données médicales prenant en compte les disparités en matière de santé entre les femmes et les hommes. Il s'agit en l'occurrence de remédier à la fois au manque de connaissances médicales et au manque de données collectées sur la santé des femmes. Ensuite, il est essentiel d'examiner en profondeur les connaissances endogènes ancrées dans les pratiques médicales traditionnelles africaines afin d'identifier si possible, et de combler les éventuelles inégalités entre les sexes. Les data scientists/ingénieurs en apprentissage automatique, les concepteurs d'appareils, les cliniciens et autres acteurs de soins doivent désormais intégrer les inégalités liées au sexe, inhérentes aux pratiques médicales actuelles, reposant majoritairement sur le modèle masculin. Lors de la mise en œuvre de solutions d'IA auprès des femmes africaines, les praticiens doivent donner la priorité à la transparence. Ils ont le devoir et la responsabilité d'engager des conversations avec les femmes, en leur fournissant des informations complètes sur les dispositifs d'IA soutenant leur prise de décision clinique.

B.C.G



© iStock

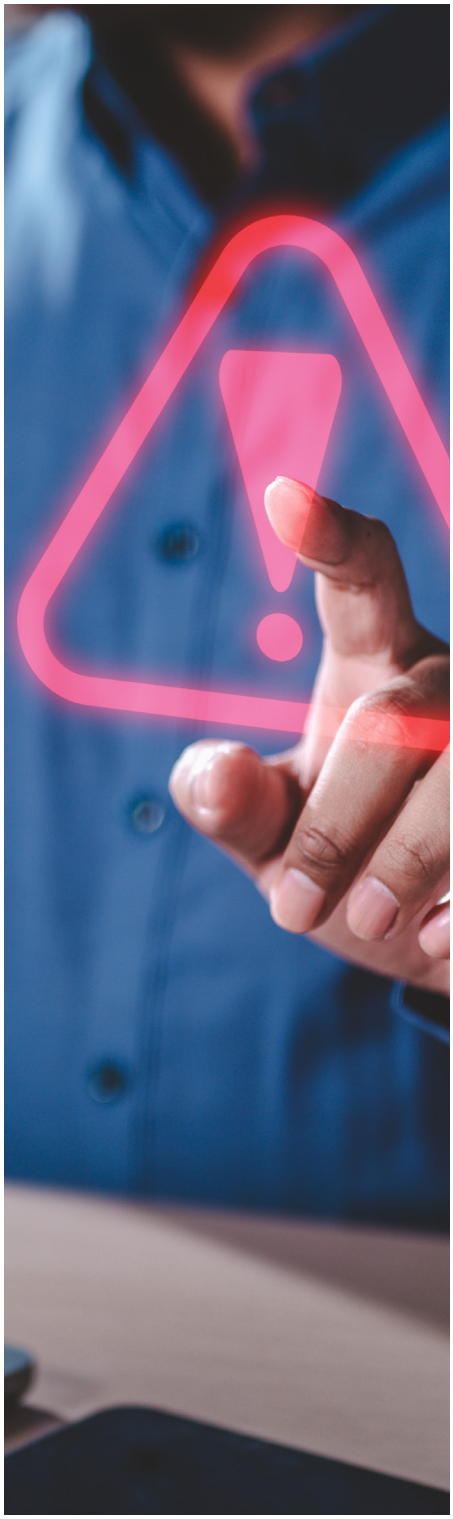
LE BUREAU DU COMMISSAIRE À LA PROTECTION DES DONNÉES PUBLIE DES LIGNES DIRECTRICES SUR L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

Par Arnaud NADINGA

Le 28 novembre 2023, le Bureau du Commissaire à la protection des données du Kenya a publié, en application de l'article 31 (6) de la loi sur la protection des données, ses lignes directrices sur l'analyse d'impact relative à la protection des données à caractère personnel (AIPD). L'objectif est notamment d'aider les responsables de traitement et les sous-traitants à comprendre leurs obligations issues de la loi. Elles devraient également les aider à saisir les risques que toute activité de traitement pourrait engendrer pour les personnes concernées et à savoir quand il est nécessaire de procéder à une AIPD. On rappelle que l'AIPD est consacrée à l'article 31 de la loi entrée en vigueur en novembre 2019. Aux termes de cette disposition, elle est nécessaire lorsqu'en raison de sa nature, de son contexte, de sa portée ou de sa finalité, une opération de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques, y compris les droits au respect de la vie privée et à la protection des données, mais aussi les droits fondamentaux énumérés au chapitre 4 de la Constitution du Kenya de 2010. Après l'avoir défini et souligné sa nature en tant que processus permettant d'identifier par avance les risques du traitement envisagé et leur gravité et de définir les mesures qui permettent de les limiter, les lignes directrices, du reste très proches de celles datées du 14 octobre 2017 du G29 européen, fournissent un certain nombre d'orientations quant aux traitements nécessitant une AIPD (I) et aux conditions qui entourent sa réalisation (II).

I. Les traitements soumis à une AIPD

La nécessité d'une AIPD dépend de la probabilité et de la gravité des risques que le traitement fait peser sur les droits et libertés des personnes physiques. Tel que cela ressort de l'article 31 (1) de la loi kenyane, une AIPD est nécessaire lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Une liste de critères alternatifs à prendre en compte dans l'appréciation de la gravité du risque et de la nécessité de l'AIPD est fournie et comprend : l'existence d'une prise de décision automatisée produisant des effets juridiques à l'égard de la personne concernée ou l'affectant de manière significative de façon similaire, y compris le profilage ou la prédiction fondés sur des aspects personnels comme la performance au travail, la situation économique, l'état de santé, les préférences, la fiabilité, le comportement, la localisation ou les déplacements



© iStock

(art. 35 de la loi) ; la surveillance ou le suivi systématique des personnes concernées (dans l'objectif de les observer, les surveiller et les contrôler), y compris la collecte de données via les réseaux sociaux ou l'usage d'équipements de surveillance publique ; ceci parce que les personnes concernées peuvent se trouver dans l'impossibilité de s'y soustraire ou voir leur droit à l'information limité ; le traitement porte sur des données sensibles ou des données portant sur des aspects privés de la vie d'une personne concernée ; le traitement à grande échelle de données personnelles (en fonction du nombre de personnes concernées, du volume ou de l'éventail des données, de la durée ou de la permanence du traitement et de l'étendue géographique qu'il couvre) ; le croisement ou la combinaison d'ensembles de données provenant de traitements poursuivant des finalités différentes ou mis en œuvre par différents responsables de traitement (un tel rapprochement déjouerait les attentes raisonnables des personnes concernées) ; le traitement porte sur des données se rapportant à des personnes vulnérables (cela comprend, entre autres, les données des enfants, des employés, des personnes handicapées, des minorités [raciales ou ethniques], des demandeurs d'asile, des réfugiés, des personnes âgées et des patients. Le risque tient ici au déséquilibre de la relation entre les parties qui réduit les pouvoirs pour les personnes concernées d'exprimer librement leur consentement, d'exercer librement leur droit d'opposition et les autres droits qui leur sont accordés) ; l'utilisation de nouvelles technologies à l'image

© iStock

de l'internet des objets ou de la reconnaissance faciale (les conséquences de l'emploi de ces technologies peuvent être inconnues et une AIPD pourrait permettre de les mettre à nu) ; les traitements qui empêchent les personnes concernées d'exercer leurs droits, de bénéficier d'un service ou d'un contrat. L'appréciation de la nécessité de l'AIPD se fait au cas par cas. Les lignes directrices ne disent pas à partir de combien de critères elle est obligatoire. Néanmoins, la présence d'au moins deux de ces critères devrait suffire. En cas de doute, il est recommandé de réaliser l'AIPD conformément au principe de responsabilité. Si le responsable du traitement estime que le traitement n'est pas susceptible d'entrainer un risque élevé, il doit obtenir l'accord de l'autorité de protection, justifier et documenter les raisons pour lesquelles il estime que l'AIPD n'est pas nécessaire.

L'AIPD doit, conformément à l'article 31 (5) de la loi, être soumise soixante (60) jours avant le début du traitement. Néanmoins, il est recommandé aux responsables qui réalisent déjà des traitements susceptibles d'entrainer un risque élevé d'en soumettre une parce que cela sera pris en compte en cas de violation de données ou de toute circonstance pouvant entrainer une sanction. En revanche, l'AIPD n'est pas nécessaire si le traitement n'est pas susceptible d'entrainer des risques élevés pour les droits et libertés. C'est également le cas lorsque la nature, la portée, le contexte, la finalité et le risque du traitement sont très similaires aux traitements pour lesquels une AIPD a déjà été réalisée. Dans de telles situations, les résultats de la DPIA pour un traitement similaire peuvent être utilisés. Il en est de même lorsque le traitement relève des exceptions prévues à l'article 51, paragraphe 2 de la loi : traitement réalisé dans le cadre d'une activité purement personnelle ou domestique, traitement nécessaire à des fins de sécurité nationale ou d'intérêt public, la divulgation des données est requise par ou en vertu d'une loi ou par ordonnance d'un tribunal.

II. Les modalités de réalisation et de soumission d'une AIPD

En application de l'exigence de protection des données par défaut et dès la conception (art. 41 et 42 de la loi), il est précisé, conformément à l'article 31 (3) de la loi, que l'AIPD devrait être réalisée avant la mise en œuvre du traitement et dès sa conception. En sus, en tant que processus continu, elle doit être mise à jour régulièrement durant la vie du traitement. Cela permet d'assurer la conformité du traitement face aux éventuels changements. Les lignes directrices précisent qu'une seule AIPD peut être réalisée pour un ensemble de traitements à la condition qu'ils soient similaires et qu'ils comportent des risques élevés similaires. Cela permet notamment de limiter les coûts pour le responsable du traitement. La similarité des traitements peut tenir à leur nature, leur portée, leur contexte, leur finalité ou le fait que les risques qu'ils impliquent sont identiques à ceux d'un traitement antérieur pour lequel une AIPD a déjà été réalisée. Dans le cas où le traitement implique des responsables conjoints ou des sous-traitants, l'AIPD doit définir avec précision leurs obligations respectives. Une nouvelle AIPD est nécessaire en cas de changement de circonstances : changement des conditions du traitement (portée, finalité, nature des données…) depuis l'autorisation du traitement ou modification des risques (utilisation de nouvelles technologies, changement de finalités…). Cette révision de l'AIPD permet de veiller à la licéité du traitement de façon continue et de maintenir le niveau de protection dans un environnement en perpétuelle évolution. Une AIPD peut également devenir nécessaire parce que le contexte organisationnel ou sociétal du traitement a changé, par exemple parce que les effets de certaines décisions automatisées sont devenus plus importants ou que de nouvelles catégories de personnes concernées deviennent vulnérables.

Les lignes directrices énumèrent un nombre minimal d'éléments que l'AIPD doit contenir. Elle doit comprendre une description des traitements (quantité de données collectées, étendue du traitement, durée et méthode de conservation des données et leur accessibilité, état de la technologie disponible, risques particuliers qui existent dans le traitement des données, une description systématique des opérations envisagées et de leurs finalités, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ou le sous-traitant). Doit également y figurer, une évaluation de la nécessité et de la proportionnalité des traitements par rapport aux finalités. Par ailleurs, l'AIPD doit inclure une évaluation des risques pour

les droits et libertés des personnes concernées et les mesures envisagées pour y faire face ainsi que les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données et à démontrer le respect de la loi. Ces mesures et garanties doivent tenir compte des droits et des intérêts légitimes des personnes concernées et de toute autre personne.

En définitive, il faut rappeler que l'AIPD est un outil interne de conformité. Elle participe à la mise en œuvre proactive des principes de traitement des données, notamment les principes de responsabilité, de sécurité et de la protection des données dès la conception et par défaut. Elle permet d'identifier et d'atténuer en interne les risques que pourraient induire les traitements. Ce faisant, elle peut contribuer, en tant que mécanisme de précaution, à éloigner le spectre de la mauvaise presse que pourraient occasionner les plaintes et les contrôles externes. L'AIPD a connu une application rétroactive par les juridictions kenyanes sur le fondement de l'article 31 de la Constitution de 2010 qui consacre le droit à la vie privée. Les faits remontent aux années 2018-2019 et concernent le projet de pièce d'identité numérique. Dans cette affaire, à la date du 14 octobre 2021, la Haute Cour du Kenya a annulé la décision du gouvernement de déployer la carte d'identité numérique nationale « huduma cards », pour violation de l'article 31 (1) de la loi (HIGH COURT OF KENYA, 14 October 2021, Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & another – Exparte – ; Immaculate Kassait, Data Commissioner – Interested Party – , JR.NO. E1138 of 2020). La Cour a relevé que le gouvernement n'avait pas procédé à une AIPD avant la décision de déployer la carte d'identité. En conséquence, elle lui a ordonné, compte tenu des risques que ce traitement comportait pour les citoyens (atteinte à la vie privée, risque de discrimination, collecte de données sensibles à l'image de l'ADN et des coordonnées GPS) de réaliser cette AIPD conformément à l'article 31 de la loi avant le traitement des données et le déploiement des cartes. Le projet qui a succédé les Huduma cards, en l'occurrence celui des Maisha Numbers avait également connu le même sort le 5 décembre 2023 avant la levée de la suspension le 23 février dernier (Nixon Kanali « Kenya's High Court lifts injunction on new digital IDs issuance », itweb.africa, 26 février 2024). C'est la preuve de son importance en tant que garantie protectrice. Au niveau africain, l'AIPD est absente de nombre de législations (Burkina Faso, Mali…), de la Convention de Malabo et de l'Acte additionnel de la CEDEAO relatif à la protection des données. Elle se rencontre néanmoins dans bon nombre de pays, à l'image du Bénin (art. 428, Code du numérique), du Nigéria (art. 28, Nigeria data protection Act 2023) ou encore du Cap-Vert (art. 29 de la loi modifiée en 2021). Espérons qu'à l'avenir, d'autres suivront ces exemples. En attendant, même dans les États où ce mécanisme n'est pas encore légalement consacré, les entités publiques et privées traitant des données personnelles gagneraient à s'y conformer spontanément. **A.N**

© iStock

WWW.AFRICADATAPROTECTION.ORG
INFO@AFRICADATAPROTECTION.ORG