Africa Data Protection Report

Janvier 2024

AFRICA DATA PROTECTION

Africa Data Protection est une association à but non lucratif qui vise à contribuer activement à un avenir numérique sûr et éthique pour tous les citoyens africains

www.africadataprotection.org/don

SOUTENEZ-NOUS

AFRICA DATA PROTECTION (ADP).
Association déclarée, régie par la loi du 1er juillet 1901
Numéro RNA : W913014770

Sommaire

AVANT-PROPOS DU PRÉSIDENT

Jules Hervé YIMEUMI
Président de l'association
Africa Data Protection

2023 a été l'année comptant le plus gros nombre d'entrées en vigueur de législations africaines dédiées à la protection des données. En effet, on a noté l'entrée en vigueur des lois tanzanienne, nigériane, algérienne et de plusieurs articles de la loi ghanéenne.

Face à l'entrée en vigueur de ces textes, on note également le développement de l'intelligence artificielle sur le continent. En Afrique, l'essor de l'intelligence artificielle (IA) et la protection des données sont étroitement liés notamment aux aspects culturels, présentant des enjeux spécifiques. Les diversités linguistiques et culturelles posent le défi de développer des solutions d'IA inclusives qui respectent les particularités locales. Certaines autorités de protection des données commencent à s'approprier le sujet.

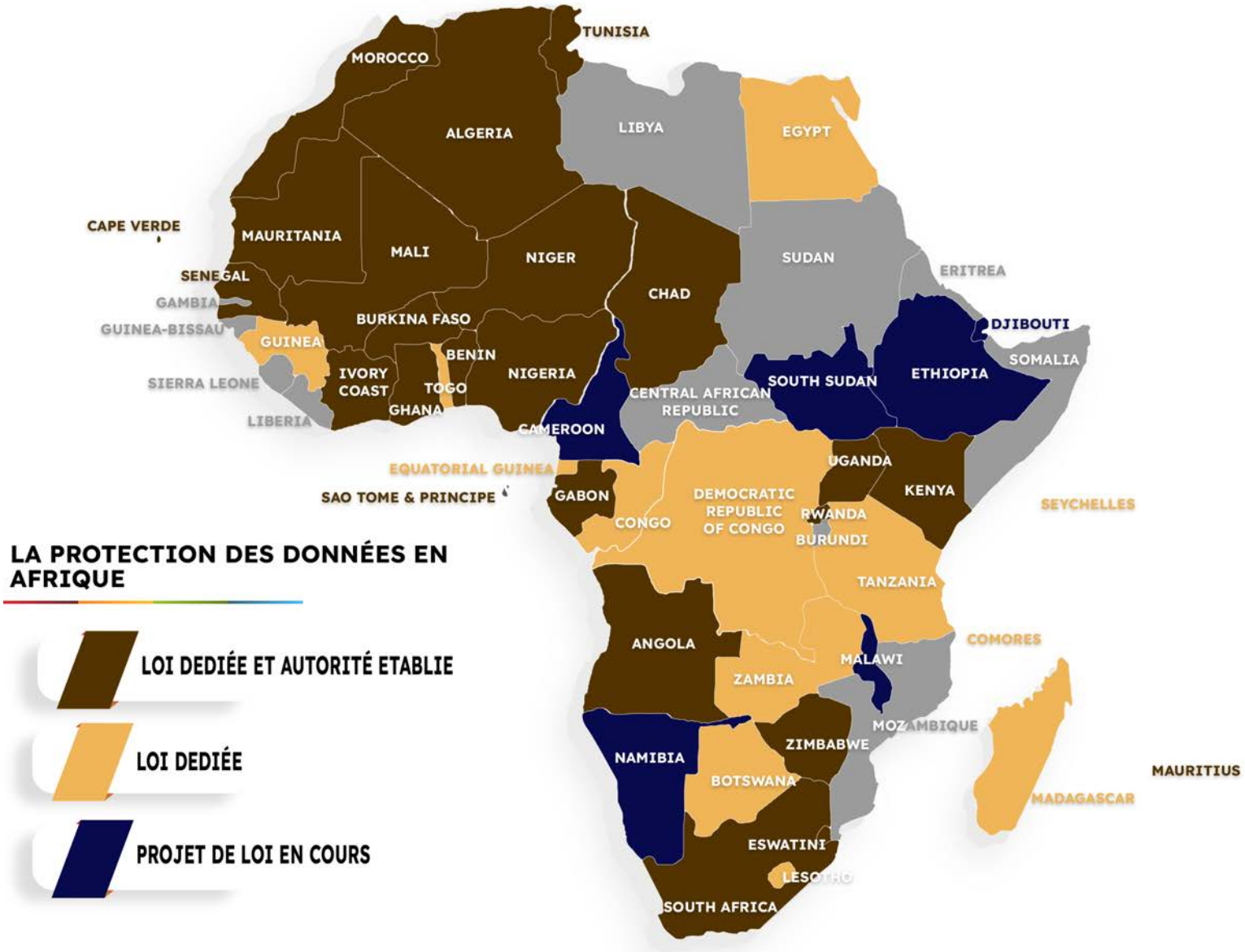
La technologie qui a attiré l'attention des autorités en 2023 est le cryptoactif Worldcoin au Kenya. Ce cryptoactif permet d'authentifier des individus en ligne à l'aide de données biométriques de scan de l'iris.

Pour faire la promotion de ce cryptoactif, World-Coin a proposé aux kényans de recevoir l'équivalent de 7.000 shillings (45 euros) en monnaie virtuelle en échange du scan de leurs iris.
C'est ainsi que plusieurs milliers de Kényans ont fait la queue dans des centres commerciaux et dans le principal centre de conférences pour se soumettre au scan.

En réaction, les autorités kényanes ont donc suspendu les activités de Worldcoin dans le pays.

Dans un communiqué commun du gouvernement et de l'autorité de protection des données (Office of the Data Protection Commissioner), daté du 2 aout 2023, il avait été expliqué que des enquêtes portant notamment sur « le manque de clarté concernant le stockage et la sécurité des données sensibles » et « l'absence d'encadrement approprié » de cette immense base de données, avaient été lancées.

La sensibilisation à la protection des données en Afrique est essentielle pour informer les citoyens sur l'importance de la vie privée. Les autorités intensifient leurs efforts pour éduquer le public et renforcer la compréhension des risques liés à la monétisation des données personnelles. À ce jour, il existe 24 autorités de protection des données en Afrique.



EDITO

Winnie Franck DONGBOU
Juriste en droit de la protection des données

Wissem SEMMAR-BELGHAZI
Responsable conformité

L'ENTRÉE EN VIGUEUR DE LA CONVENTION DE L'UNION AFRICAINE SUR LA CYBERSÉCURITÉ ET LA PROTECTION DES DONNÉES : QUELLE PERTINENCE NEUF ANS PLUS TARD ?

La Convention de Malabo sur la cybersécurité et la protection des données (ci-après « la convention ») est entrée en vigueur en juin 2023, soit neuf ans après son adoption par l'Union africaine en 2014. Bien que cet énorme retard dans l'entrée en vigueur de la convention mériterait une interrogation particulière, l'objet de notre propos se limite à la pertinence d'un tel instrument dans le paysage africain actuel de la protection des données personnelles.

Une simple déclaration de principes

L'article 8 de la convention, dédié à son objet, précise clairement qu'il s'agit d'un engagement pour les États ayant ratifié la convention (actuellement une quinzaine parmi cinquante-quatre) d'introduire un cadre légal national spécifique à la protection des données à caractère personnel, visant à protéger certains droits fondamentaux tels que la liberté d'expression et le droit à la vie privée. Cependant, la convention ne fournit pas de garanties tangibles contre la violation de ces droits, et laisse aux Etats membres le soin de mettre en place un cadre juridique et de confier son contrôle à une autorité nationale.

Ainsi, l'objectif de la convention n'est pas de conférer un droit direct aux citoyens de l'Union. Pour rappel, sauf mention contraire, le contenu des conventions et traités internationaux doit être incorporé dans la législation nationale des États membres, pour devenir directement applicable aux citoyens et ainsi leur permettre de s'en prévaloir auprès des juridictions ou autorités compétentes.

Un cadre général dépassé

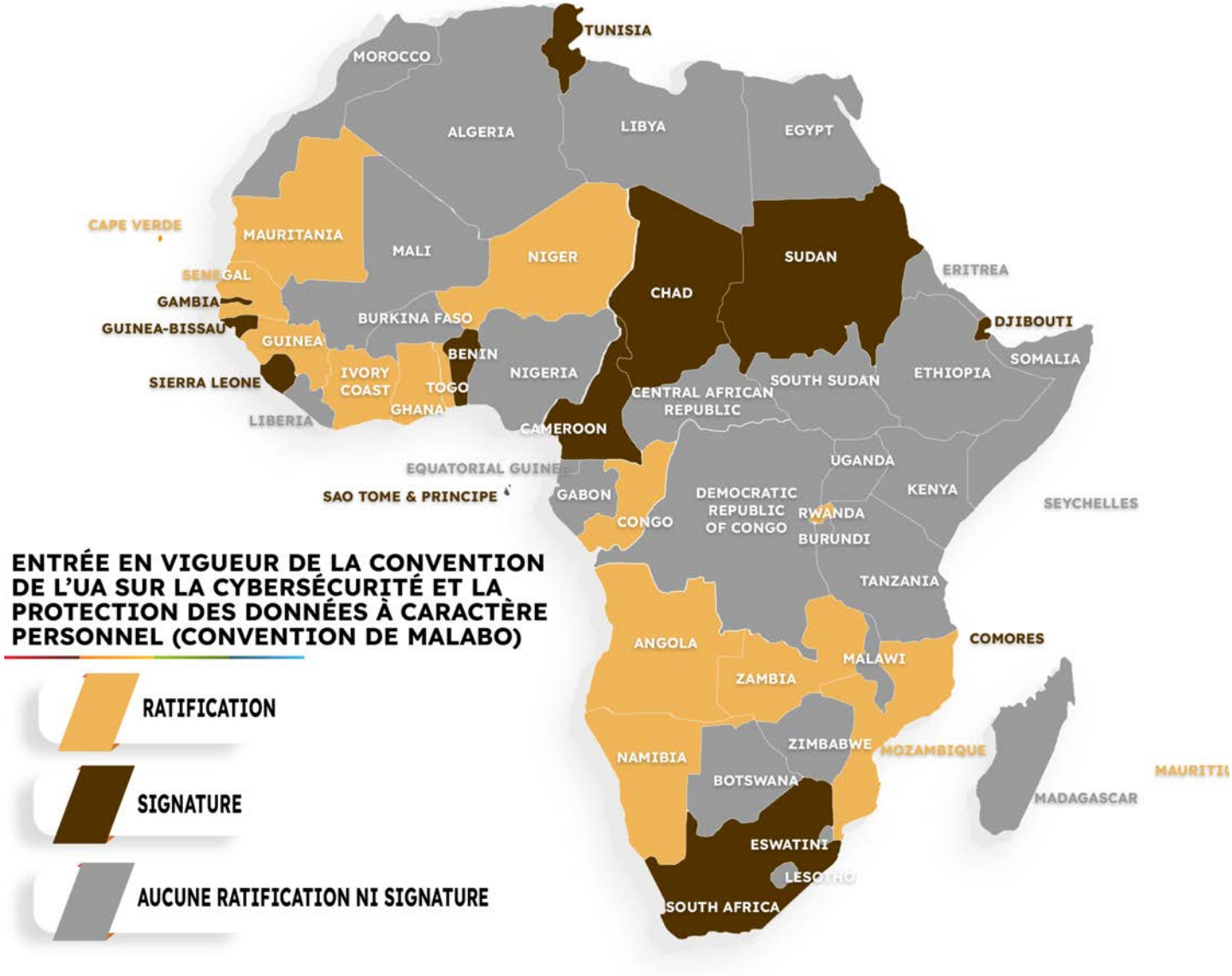
La convention regroupe la protection des données, la cybercriminalité, la cybersécurité et le commerce électronique sous un seul cadre juridique. En effet, seulement 12 pages sont dédiées à un sujet si important, omettant des définitions et des processus essentiels en la matière. Cette généralité s'explique sans doute par le fait que la convention constituait il y a neuf ans un appel urgent formulé aux États membres de se saisir de la question de la protection des données à caractère personnel. Aujourd'hui, les États africains doivent faire face à une évolution et à une démocratisation des technologies de l'information et de la communication qui n'avaient pas été prises en considération lors de de l'élaboration de la convention. Il s'agit, entre au-

tres, de l'intelligence artificielle, des objets connectés, et surtout de la disparition des frontières physiques, qui oblige à renforcer l'encadrement du transfert des données personnelles vers de puissantes entreprises établies à l'étranger.

La nécessité d'une mise à jour

L'accent doit être mis sur une actualisation de la convention de Malabo, la mise en place d'un « Malabo + » ou « Malabo 2.0 », à l'instar de la convention 108+ du Conseil de l'Europe, version modernisée de la convention 108, venue proclamer l'importance de droits humains face aux développements technologiques. Les efforts visant à récolter plus de ratifications d'un texte désuet devraient être dirigés vers un travail de fond qui viendrait rectifier les lacunes et les anachronismes de la convention. Un protocole spécifique à la protection des données personnelles, intégrant la question des flux transfrontaliers, de la protection des droits humains en matière d'intelligence artificielle et de surveillance, ou encore la mise en place d'une autorité centrale de contrôle, serait utile.

Pour y parvenir, le législateur africain aurait tout à gagner de mettre à profit l'expérience de certaines autorités nationales de protection des données. La dynamique positive de l'entrée en vigueur récente de la convention offre une opportunité immanquable de sensibilisation des Etats, organismes et citoyens africains à la protection des données personnelles, grâce à l'expertise de certaines associations à but non lucratif telles que Africa Data Protection.



CONTRIBUTEURS

MAHA **TAZI**

Consultante
en cybersécurité

ADILA **SAKHRAJI**

Compliance Officer
DPO

FRANCK **ADOPO**

Doctorant en droit du numérique et de la protection des données à caractère personnel

JUSTIN **KOUMAKO**

Doctorant
DPO

PROF. BENJAMIN **GUINHOUYA**

Epidémiologiste
Expert en éthique du numérique en santé

PATRICK **NGUETCHOUESSI**

Doctorant en droit de l'IA - DPO

MAHADI **MAIFADA MAGOUDANI**

Docteur en
droit du numérique

ARNAUD **NADINGA**

Doctorant en
droit du numérique

JEAN-MARC **DIGBLI**

Juriste IT

BROZECK **KANDOLO**

Doctorant en
droit privé

THOMAS **HONNET**

DPO
Enseignant

L'AUTORITÉ SUD-AFRICAINE DE PROTECTION DES DONNÉES INFLIGE UNE AMENDE D'ENVIRON 250 000 € AU MINISTÈRE DE LA JUSTICE POUR VIOLATION DES DONNÉES

Par Franck ADOPO

Le 3 juillet 2023, l'autorité de protection des données à caractère personnelles de l'Afrique du Sud, ci-après dénommée « régulateur », en charge de la protection des renseignements personnels, a émis à l'encontre du ministère de la Justice et du Développement constitutionnel une sanction pour manquement au respect de la loi sud-africaine sur la protection des renseignements personnels de 2013 (POPIA).

Cette sanction survient à la suite d'une mise en demeure émise par le régulateur à l'encontre du ministère, le 9 mai 2023, conséquemment à des faits suspectés d'atteinte à la sécurité informatique survenus en septembre 2021. En effet, après les investigations du régulateur, il s'est avéré que l'interruption des services dudit ministère au public en septembre 2021 et les difficultés d'accès des employés aux systèmes d'exploitation du ministère étaient effectivement dues à une compromission du système informatique par des logiciels malveillants, ayant engendré une fuite de plus de 1200 fichiers. Cette fuite de données était la conséquence du non-renouvellement du package de licences de trois antivirus expirés depuis plus d'un an.

Après la constatation de ces manquements graves à la loi nationale sur la protection des renseignements personnels, le régulateur a formulé une série de mesures à mettre en œuvre par le ministère. D'une part, le ministère devait renouveler ou fournir au régulateur la preuve du renouvellement des licences expirées dans un délai de 31 jours; d'autre part, il devait formuler des sanctions disciplinaires à l'encontre des fonctionnaires responsables du renouvellement de ces licences.

Or, il s'est avéré que le ministère n'avait mis en exécution aucune de ces mesures à l'expiration du délai imparti. Le régulateur a finalement prononcé à son encontre une sanction administrative de 5 millions de rands (soit plus de 250.000€ d'amende) le 3 juillet 2023. Cette sanction était assortie de la possibilité pour le ministère d'interjeter appel de la décision, ce qu'elle n'a pas fait, rendant ainsi la sanction définitive.

Les recommandations du régulateur étaient-elles fondées et réalisables ?

Pour rappel, dans sa mise en demeure, le régulateur demandait au ministère de rapporter la preuve de la mise à jour de son package d'antivirus, soit une preuve actuelle de la robustesse de son système de sécurité informatique, afin d'éviter qu'une violation similaire ne puisse se reproduire. De plus, des mesures disciplinaires devaient être prises à l'encontre des fonctionnaires responsables de la sécurité informatique, précisément ceux qui devaient veiller au renouvellement des licences des antivirus expirés, sans doute pour négligence.

Tout d'abord, pour la légalité et la faisabilité des mesures techniques de sécurité, il s'avère qu'il s'agit d'une obligation prévue par la POPIA. En effet, l'article 19 de ladite loi prévoit que le responsable de traitement a l'obligation de garantir la sécurité, l'intégrité et la confidentialité des données personnelles. Il doit à cet effet mettre tout en œuvre selon l'état de l'art pour se conformer à cette obligation. Or, il est clairement ressorti des investigations du régulateur que trois antivirus chargés de détecter, alerter, mettre à jour afin d'empêcher l'atteinte au système informatique étaient tous défaillants. Ils avaient expiré depuis plus d'un an. Par conséquent, les recommandations techniques étaient bel et bien fondées et réalisables. En conservant son système d'antivirus expirés malgré les recommandations du régulateur, le

© iStock

ministère a persisté dans le manquement à son obligation légale, entrainant ainsi une violation de l'article 103 (1) de la POPIA relatif au non-respect des avis d'exécution.

En ce qui concerne les sanctions, il faut savoir que l'Afrique du Sud dispose d'un système qui se décline en deux modalités. En effet, la sanction peut consister en une peine d'emprisonnement et une peine administrative, ou l'une des deux peines seulement. La peine d'emprisonnement peut aller de 12 mois à 30 ans, en fonction de la gravité de l'infraction, et elle est prononcée à l'encontre d'une personne physique selon l'article 107 de la POPIA. Dans le cas de la présente décision, ces sanctions auraient pu être dirigées contre les fonctionnaires responsables du renouvellement des licences, mais le régulateur a jugé bon d'inviter le ministère à ne prononcer qu'une sanction disciplinaire. Encore faut-il pour qu'une sanction disciplinaire soit prononcée déterminer si ces fonctionnaires ont commis une faute ou si l'erreur vient de la hiérarchie, comme le prévoient les articles 14 du Public Administration Management Act et l'article 16B du Public Service Act pour les sanctions disciplinaires des fonctionnaires en Afrique du Sud.

La sanction administrative est, quant à elle, dirigée vers le responsable de traitement en tant qu'entité. La loi prévoit qu'elle ne peut excéder 10 millions de Rands selon l'article 109. Ce qui signifie que le régulateur sud-africain a infligé au ministère jusqu'à la moitié du montant maximal pour son manquement à la POPIA.

Il faut tout de même noter la particularité de la démarche du régulateur sud-africain. S'il est commun aux lois en Afrique de prévoir des sanctions pénales en cas de manquement aux dispositions de protection des données personnelles, la démarche de ce régulateur fait partie des premières en la matière sur le continent. En effet, il n'a pas hésité à prendre l'initiative de la proposition d'une sanction disciplinaire envers des fonctionnaires pour des fautes commises dans l'exercice de leurs fonctions, si ces fautes sont bel et bien établies. Il ouvre ainsi la voie à la prononciation d'une sanction individuelle en plus de la sanction principale prononcée contre l'entité responsable de traitement.

Cependant, dans ce cas de figure, il s'agit des employés d'une administration publique. Les recommandations du régulateur auraient-elles été les mêmes s'il s'agissait des employés d'une entité privée ? En tout état de cause, cette cyberattaque n'est pas isolée. En effet, elle s'inscrit dans un contexte marqué par une série de cyberattaques ayant touché plusieurs institutions étatiques et régionales en Afrique. Il n'est pas à exclure qu'une démarche et un raisonnement similaires puissent être adoptés par d'autres autorités de contrôle en cas de manquement aux lois sur la protection des données, surtout en cette période d'éveil des autorités de protection des données en Afrique.

F.A

© iStock

INTELLIGENCE ARTIFICIELLE ET COOPÉRATION INTERNATIONALE

Par Adila SAKHRAJI

"Si elle n'est pas contrôlée, l'intelligence artificielle (IA) générative et les autres technologies d'IA pourraient sérieusement porter atteinte à la confidentialité et aux autres droits fondamentaux" . A un jour d'intervalle de la clôture de la 45ème édition de la Global Privacy Assembly (GPA), l'OCDE publiait un article sur les défis posés par l'intelligence artificielle et la place grandissante qu'elle occupait dans le monde.

L'IA générative se démarque en utilisant des algorithmes capables de générer et créer du contenu aux formats divers (texte, image, vidéo etc.) en s'appuyant sur des volumes importants de données appelées "bibliothèque de savoir". Ces bibliothèques sont souvent alimentées par du data scraping (collecte de données publiques) ou par des databrokers monétisant des fichiers comportant des données personnelles.

Des exemples de coopération interétatique ont émergé pour répondre aux préoccupations communes sur la protection de la vie privée et des droits fondamentaux des individus.

Dans ce mouvement s'inscrit la résolution de la GPA du 20 octobre 2023 sur les systèmes d'IA générative, une rencontre co-sponsorisée par le Maroc, nommée en 2021 hôte de cette assemblée pour deux ans. Face au développement de l'IA générative, la GPA s'adresse aux acteurs de la mise en service de ces technologies et les responsabilise dans sa résolution construite autour de 9 axes de conformité.

1. Une base légale pour un traitement licite
Rappel de l'obligation d'identifier une base légale pour chaque étape du traitement des données (collecte, tests, apprentissage, interactions avec les utilisateurs, etc.).

2. Une finalité identifiée et un usage limité
Une finalité appropriée, raisonnable et légitime doit être identifiée en amont. Les moyens déployés par l'IA devront être proportionnés à la finalité.

3. Principe de minimisation des données
Les données traitées doivent répondre strictement aux nécessités de la finalité poursuivie afin de réduire les risques.

4. Fiabilité des données
L'Assemblée évoque les "hallucinations", situations où le contenu généré par l'IA est faux ou incomplet, et la nécessité de recours à des politiques de gouvernance de données pour en réduire l'occurrence et le risque.

© iStock

5. Transparence
Les développeurs, fournisseurs et utilisateurs de ces technologies génératives doivent s'inscrire dans une démarche transparente vis-à-vis des personnes. Cela signifie notamment pour les fournisseurs d'informer leurs clients par une documentation précise sur les risques que comportent ces solutions.

6. Sécurité
La confidentialité et la sécurité doivent être embarquées dès la phase de conception de la solution par la mise en place de mesure techniques, organisationnelles et logiques adéquates.

7. Privacy by design and default
La GPA recommande aux acteurs du secteur de conduire une analyse d'impact sur la protection des données (AIPD) tout au long de la durée de vie de la solution afin d'adapter les mesures de protection au regard de l'évolution du risque.

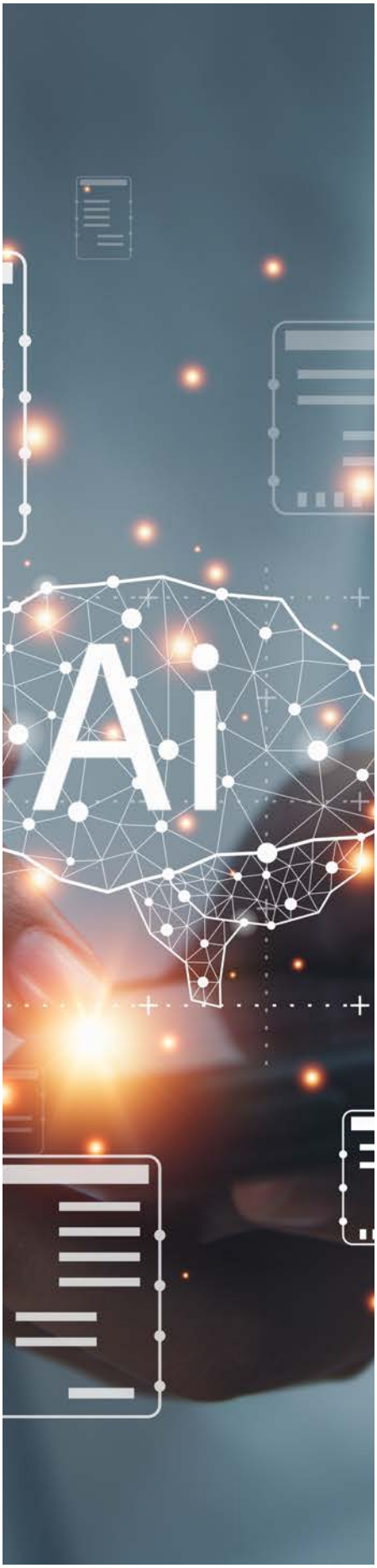
8. Droits des personnes
L'information des personnes concernées sur le traitement de leurs données personnelles est obligatoire. La possibilité d'exercice de leurs droits devra également être garantie.

9. Accountability - Reddition de compte
Les acteurs devront être en mesure de démontrer leur conformité aux règles nationales et supranationales en tenant à disposition des autorités de contrôle compétentes la documentation technique exhaustive nécessaire.

La Global Privacy Assembly appelle ses membres à reprendre la substance de cette résolution dans un cadre national contraignant. Si certains Etats se sont dotés de lois encadrant l'utilisation de l'IA, le législateur peine à suivre le rythme d'une technologie conquérante.

Dans un monde global et plus dynamique que jamais, il est déterminant pour les acteurs de coopérer ensemble pour l'adoption d'un premier cadre commun sur les nouvelles technologies. Celui-ci comporterait des principes et bonnes pratiques, sur le modèle des codes de conduite, qui pourront se traduire de manière plus détaillée au niveau national.

Enfin, notons que l'IA générative repose sur un système qui éduque l'outil pour assister l'utilisateur dans un domaine spécifique. L'apprentissage exploite des bibliothèques de savoir et d'événements gigantesques. C'est seulement une fois l'outil suffisamment expert du domaine de sa spécialité qu'il est mis en service. Il continuera d'apprendre et de produire, générer, en assistant l'utilisateur. L'outil exploite les données sur lesquelles l'humain a choisi et décidé de l'entraîner. Il est donc déterminant d'encadrer la décision prise par l'humain avant même de se pencher sur les aspects techniques de la solution. Une approche par les risques sera plus respectueuse des droits fondamentaux des individus.
A.S



© iStock

L'AUTORITÉ MAURICIENNE DE PROTECTION DES DONNÉES PUBLIE SON BILAN ANNUEL 2022

Par Justin Yao KOUMAKO

La Data Protection Office (DPO), l'autorité mauricienne de protection des données est l'une des premières sur le continent africain . Créée en 2009 et renforcée par la Data protection act de 2017, elle a plusieurs missions et l'obligation de présenter un rapport annuel au parlement . Riche de 44 pages, son dernier rapport, le 14ème depuis sa création en 2009, couvre l'ensemble de ses activités au cours de l'année écoulée, allant des aspects basiques relatifs au budget de l'autorité et à ses ressources humaines à l'instruction des plaintes et la coopération internationale, sans oublier ses activités prolifiques de sensibilisation.

Les points saillants des activités de la DPO en 2022

La mise en place d'une plateforme dématérialisée pour les responsables de traitement et le public : En 2022, la DPO a finalisé et mis à disposition des responsables de traitement et du public une plateforme baptisée e-DPO. Cet outil permet aux usagers de porter plainte en ligne, de notifier les violations de données, d'accéder au registre des responsables de traitement ou des sous-traitants, d'obtenir des certificats d'enregistrement etc. Il est opérationnel depuis le 7 décembre 2022.

Instruction des plaintes, avis consultatif et violation des données : La DPO a reçu 71 nouvelles plaintes en 2022. Ces plaintes portaient essentiellement sur des usages non-autorisés de la vidéosurveillance (66 cas au total, soit 93% des plaintes), des obstacles au droit d'accès et des traitements illégaux de données. Elle en a traité 36 dont 5 à l'amiable. Elle a également reçu 167 requêtes en interprétation de la loi sur la protection des données et 57 notifications de violations des données personnelles. Sur les violations de données, il est intéressant de noter que la plupart proviennent d'erreurs humaines (envoi de données par mail à un mauvais destinataire) et de divulgations illégales. Seules 6% des violations proviennent réellement de cyberattaques (rançongiciel et hameçonnage compris).

La sensibilisation : La DPO a fait une importante activité de sensibilisation en 2022. Celle-ci passe par des communiqués de presse, des campagnes de sensibilisation vidéo à l'attention des jeunes, la formation des officiers de police, la distribution de CD (en tout 3016 ont été remis à des responsables de traitements pour les aider dans leur mise en conformité), la participation à des activités liées aux données personnelles dans les entreprises, et enfin des interventions dans des universités. (The Centre for Human Rights, University of Pretoria).

© iStock

La coopération internationale : La DPO a été très active sur le plan international. Membre de plusieurs réseaux de protection des données personnelles ou de la vie privée plus généralement, elle a participé à des conférences et sommets organisés sur des thématiques l'intéressant. La participation à ces activités internationales a été une opportunité pour la DPO d'échanger avec ses pairs, de partager de bonnes pratiques et de contribuer à l'évolution du droit. Au niveau régional, elle a ainsi travaillé pour la révision de la loi type de la Communauté de développement de l'Afrique australe (SADC) sur la protection des données. Au niveau international, la DPO a contribué aux réponses de Maurice aux questions du rapporteur spécial des Nations-Unies sur le droit à la vie privée.

Il est important de préciser que le rôle du rapporteur spécial est de promouvoir et protéger la vie en examinant, entre autres moyens, les politiques et les lois nationales sur l'interception des communications numériques et la collecte des données personnelles. Dans le dernier rapport de la Rapporteuse spéciale Ana Brian Nougrères, Maurice est ainsi cité parmi les 18 Etats contributeurs . Les travaux entrepris avec la Commission européenne pour une décision d'adéquation de Maurice au RGPD restent cependant l'activité la plus intéressante à bien des égards.

Haro sur le processus de demande d'adéquation avec la Commission européenne

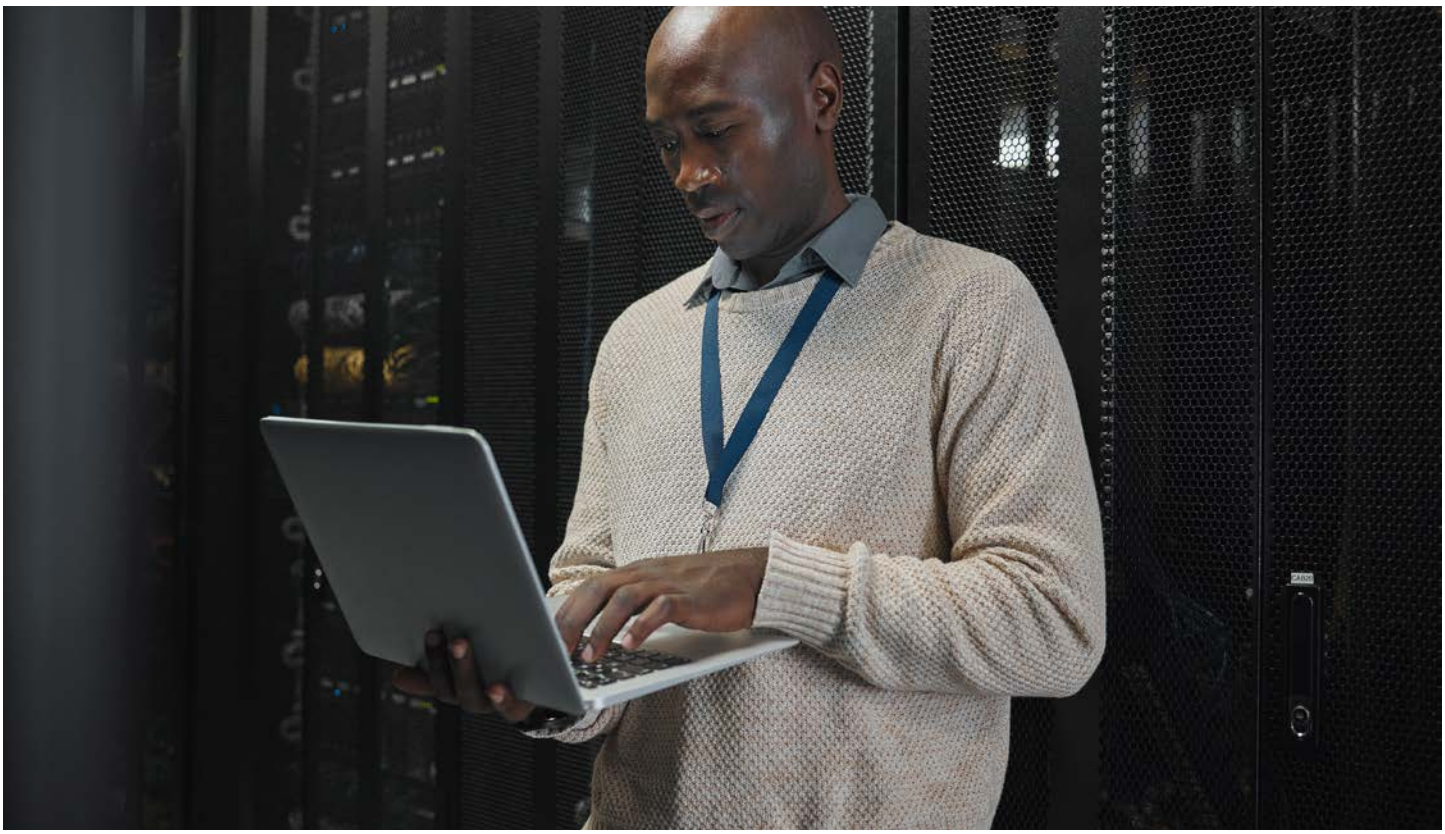
La DPO a établi un rapport pour faciliter l'évaluation de l'adéquation de Maurice au RGPD par la Commission européenne. L'objectif du rapport est de fournir une vue d'ensemble fidèle du système mauricien afin que la Commission européenne puisse procéder à une évaluation objective. L'adéquation est l'une des conditions pour le transfert des données personnelles de l'Union européenne vers un Etat tiers. Conformément au RGPD, les données ne peuvent être transférées hors UE qu'à trois conditions non cumulatives :
- soit le transfert intervient sur la base d'une décision d'adéquation accordée par l'UE (article 45 du RGPD) ;
- soit le transfert intervient sur la base de garanties appropriées telles que les clauses contractuelles (article 46 du RGPD) ou les règles d'entreprise contraignantes (article 47 du RGPD) etc;
- soit le transfert intervient à titre dérogatoire pour des situations particulières (article 49 du RGPD).

Le feuilleton des décisions d'adéquation pour les transferts vers les Etats-Unis met l'accent sur la complexité de ce régime juridique . Au moment où ces lignes sont écrites, seuls 15 Etats sont considérés par la Commission européenne comme adéquats. Si l'Île Maurice est admise comme Etat adéquat, elle serait le premier Etat africain à accéder à ce statut, et elle possède les arguments pour. Ce petit Etat de l'Afrique australe fait partie des rares Etats africains à avoir signé la convention de Budapest sur la cybercriminalité, actuel et unique instrument international contraignant sur les questions de cybercriminalité et de protection des données. Depuis plusieurs années, elle est classée comme le 1er Etat africain en matière de cybersécurité et occupe le 17ème rang mondial dans le dernier rapport Global Cybersecurity Index . Elle dispose d'une loi sur la protection des données personnelles, une autorité proactive sur la question et des voies de recours juridictionnels effectives.
En Afrique, l'Ile Maurice se positionne comme un modèle en matière de protection des données personnelles et son admission comme Etat adéquat serait une belle récompense pour les efforts déployés. Ce ne serait que justice !
J.Y.K


© iStock

L'ÉPINEUSE QUESTION DE LA « SOUVERAINETÉ NUMÉRIQUE » : LES COULISSES DU DATA CENTER IVOIRIEN

Par Mahadi MAIFADA MAGOUDANI



© iStock

Dans l'écosystème ouest-africain francophone en pleine mutation numérique, la Côte d'Ivoire se distingue par le lancement ambitieux de son Data Center national, destiné à héberger des données des entités administratives nationales. Cependant, au-delà des avantages apparents, des défis techniques et juridiques émergent, soulignant ainsi la complexité de la quête de souveraineté numérique dans un contexte où la protection des données personnelles occupe une place importante.

Premièrement, il est essentiel de passer en revue les Data Centers d'ores et déjà existants. Comme mentionné dans un rapport de l'ANSUT , l'administration ivoirienne comptait jusqu'alors 5 Data Centers répartis comme suit : Le Data Center de Grand Bassam à VILIB, celui de la Présidence, le Data Center de la Société Nationale de Développement Informatique (SNDI), ainsi que deux Data Centers du projet E-Education situés à Cocody et Yamoussoukro.

Ainsi, ce nouveau Data Center national constituera un atout majeur pour l'industrie technologique ivoirienne. Le développement de ces infrastructures peut s'expliquer par la situation géographique privilégiée de la Côte d'Ivoire, offrant des avantages distincts pour leur implantation, contrairement aux membres enclavés de l'UEMOA tels que le Burkina Faso ou le Niger. Cette initiative renforcera incontestablement le secteur en Côte d'Ivoire, voire dans l'espace UEMOA, marqué par des contraintes de stockage et une prédominance du marché du Cloud détenu en grande partie par des multinationales étrangères. Malgré les avantages évoqués, des défis liés à la

souveraineté numérique semblent persister.

En effet, historiquement, la question de la souveraineté numérique aurait dû être abordée à la suite des politiques publiques relatives aux télécommunications initiées dans les années 1990 lors de la libéralisation du marché des télécommunications. Cette ouverture a particulièrement encouragé la forte implication des multinationales étrangères, surtout dans le domaine de la téléphonie mobile , dans la construction des outils de traitement et de stockage des données. Cela a conduit à une prédominance des multinationales étrangères, souvent sous forme de consortium, et à une dépendance technologique de l'espace UEMOA.

Cette question refait surface avec le lancement des projets dits de « modernisation de l'administration publique » dans l'espace UEMOA. Dans ce cadre, l'annonce de la construction de ce Data Center national constitue une manifestation concrète du processus ivoirien démarré en 2016 . Il est à noter que ces projets bénéficient souvent du soutien de financements extérieurs, principalement européens, impliquant fréquemment la participation de sociétés ou multinationales étrangères pour le déploiement des outils de traitement des données.

Cependant, derrière la façade des solutions informatiques performantes offertes par ces acteurs internationaux notamment pour la dématérialisation des services publics, la question cruciale de la souveraineté émerge. En examinant de près le cas concret du projet ivoirien, il est évident qu'il résulte d'un partenariat entre la Côte d'Ivoire et les États-Unis, formalisé par deux accords . Selon les autorités ivoiriennes, ce partenariat vise, « dans le cadre de la souveraineté numérique (...), à rassembler toutes les structures de l'Etat qui interviennent dans le domaine de l'Economie numérique sur un seul site et à sécuriser les données de l'administration (...) » . Bien que les détails complets de ces accords soient difficilement accessibles, il est à noter que la mise en œuvre de ce projet est financée à hauteur de 60 millions de dollars US par Washington et supervisée par le consortium américain Cybastion Institute of Technology, un membre du Conseil d'Administration de la Chambre de Commerce des États-Unis d'Amérique . Dans un tel contexte plusieurs préoccupations émergent.

Tout d'abord, il se pose le constat paradoxal de la recherche de la « souveraineté numérique » dans un projet dépendant de financements extérieurs et impliquant significativement des entités étrangères dans sa mise en œuvre. Une préoccupation accentuée par le récent épisode au Mali, dans lequel les autorités ont dénoncé « la prise en otage » du fichier des données biométriques en vue des élections par une multinationale française . Cette situation semble résulter des tensions politiques entre la France et le Mali, mettant en évidence les risques liés à une dépendance vis-à-vis d'acteurs étrangers dans des projets sensibles. Un parallèle à considérer attentivement dans le contexte du Data Center ivoirien financé et conçu par les États-Unis. La question de la dépendance technologique des autorités ivoiriennes suscite également des interrogations, en particulier en ce qui concerne les impératifs de mise à jour pour garantir le bon fonctionnement de l'infrastructure. En outre, la préoccupation concernant l'accès aux données stockées peut se manifester de deux manières. D'un côté, la possibilité que les politiques de confidentialité et les lois régissant cet accès soient influencées par l'investisseur américain. De l'autre, l'implication d'experts étrangers augmente le risque d'accès à des données spécifiques, voire sensibles pour la sécurité nationale, générées dans le cadre des activités de l'administration publique, compte tenu de la centralisation facilitée par cette infrastructure. Par ailleurs, l'implication explicite de l'autorité de contrôle, l'ARTCI, dans ce partenariat n'a pas été clairement définie selon les différents communiqués. Cette remarque soulève des interrogations quant au rôle de cette autorité, d'autant plus qu'elle demeure l'instance garante du respect de la réglementation en matière de données personnelles pour l'ensemble des projets.

Pour conclure notre analyse, nous préconisons vivement aux décideurs ivoiriens, et plus largement à l'échelle UEMOA, de privilégier des financements autonomes, notamment dans le déploiement des infrastructures essentielles à l'administration publique. Dans le cas spécifique des infrastructures de stockage, cette approche permettrait d'assurer un contrôle local sur les données générées et traitées par l'administration, quitte à y allouer un budget national propre conséquent, tout en favorisant les compétences locales et en investissant dans l'industrie technologique et la formation d'experts locaux. **M.M.M**

PERSPECTIVES DE L'AUTORITÉ DE PROTECTION DES DONNÉES PERSONNELLES

Par Brozeck KANDOLO

© iStock

Depuis le 13 mars 2023, la République démocratique du Congo (ci-après RD-Congo) a mis en place une réglementation dans le domaine du numérique, à travers l'ordonnance-loi n°23/010, qui concerne le Code du numérique. Une partie importante de cette nouvelle législation aborde la question cruciale de la protection des données personnelles. Ces dispositions sont détaillées dans le titre III du Code du numérique.

La pertinence d'une législation sur la protection des données personnelles repose souvent sur l'autorité de contrôle qui lui est associée. Cette autorité de contrôle joue un rôle essentiel en veillant à ce que les règles établies dans ce domaine soient respectées, dans le but de protéger les personnes concernées. En d'autres termes, la force de cette législation se mesure à la puissance de son organe de surveillance, garantissant ainsi une protection efficace des données personnelles.

Afin de garantir le respect de cette réglementation, le législateur congolais prévoit la mise en place d'une autorité de contrôle en matière de protection des données personnelles appelée Autorité de Protection des Données ou « APD ». Il est important de noter qu'à la rédaction de cette note, cet organe de contrôle n'a pas encore été créé. Cependant, nous examinerons ici les compétences prévues, ainsi que les pouvoirs de sanctions qui lui sont reconnus.

Les compétences de l'autorité de protection des données en RD-Congo

Le fonctionnement de l'Autorité de Protection des Données

Congolaise (APD) s'inspire largement de ses homologues européens et africains. Sa mission principale est de contrôler le respect de la protection des données personnelles afin de sauvegarder la vie privée de ceux dont les données sont hébergées en RD-Congo. Cependant, sa particularité réside dans sa compétence, celle de contrôler également les traitements des données publiques.

Cette entité possèdera le statut d'une autorité administrative indépendante, avec une personnalité juridique, jouissant d'une autonomie administrative et financière. Parmi les compétences qui lui sont attribuées, les plus marquantes incluent la capacité de rendre des avis et de formuler des recommandations sur les traitements des données personnelles et publiques. Ceci vise à informer les personnes concernées ainsi que les responsables de traitement de leurs droits et obligations.

Une particularité distinctive de cette autorité est le système déclaratif des traitements des données personnelles. En d'autres termes, les responsables de traitement doivent soumettre des déclarations à cette autorité avant de traiter certaines données personnelles. Cela diffère du système d'accountability, qui permet la mise en place de traitements sans nécessiter une déclaration préalable à l'autorité de contrôle.

L'APD a également le pouvoir d'engager des actions devant les tribunaux et de mener des enquêtes en cas de constatation de violations des données personnelles et publiques. Cependant, toutes ces actions doivent avoir une finalité répressive ou corrective. En conséquence, l'APD est habilitée à prononcer des sanctions en cas de non-respect des règles relatives aux données personnelles et publiques.

Pouvoirs et sanctions de l'Autorité de Protection des Données

Un certain nombre de mesures administratives sont reconnues par cette autorité. Notamment, elle peut émettre des avertissements à l'encontre d'un responsable de traitement. De plus, elle a le pouvoir de mettre en demeure pour faire cesser le manquement, et le délai de mise à conformité ne peut excéder huit jours.

L'APD peut également imposer des sanctions pécuniaires à l'encontre d'un responsable de traitement ne respectant pas les dispositions du code du numérique en matière de protection des données. Ces sanctions peuvent inclure un paiement de huit millions à deux cents millions de francs congolais. En cas de violation ayant entraîné la mort ou une tentative de meurtre d'une ou plusieurs personnes, une amende équivalente à 5% de son chiffre d'affaires annuel peut être infligée. De plus, elle a le pouvoir de prononcer une injonction de cessation de traitement des données à caractère personnel si la violation a mis en danger la sécurité et la sûreté nationales et/ou conduit à un crime de masse ou à un génocide.

Bien que l'organe de contrôle en matière de protection des données ne soit pas encore opérationnel, son établissement représente un pas significatif vers l'instauration d'un cadre réglementaire solide. Cette initiative vise à trouver un équilibre entre l'innovation numérique et la protection des droits individuels, nécessitant un suivi attentif pour évaluer son impact sur le paysage numérique congolais.
B.K

© iStock

LA PROTECTION DES DONNÉES PERSONNELLES DANS LE SECTEUR FINANCIER, OBJET D'UN GUIDE PUBLIÉ PAR LA DATA PROTECTION OFFICE (DPO)

Par Justin Yao KOUMAKO

Le secteur financier traite massivement des données à caractère personnel, qui présentent une certaine sensibilité pour les personnes concernées. Le traitement de ces données représente par ailleurs des enjeux importants, dans la mesure où ces données sont convoitées par des personnes au profil varié, en particulier les cybercriminels. Cet état de fait n'a pas échappé au Bureau mauricien de protection des données personnelles (Data protection Office en anglais, ci-après « la DPO » ou « le Bureau »), qui s'est saisi du sujet et a publié, en novembre 2023, un guide sur le traitement des données personnelles dans le secteur financier. Une analyse de ce guide permet de constater que le Bureau a pris soin, dans un premier temps, de recenser les catégories de données personnelles concernées, avant de rappeler les obligations et principes à respecter par les responsables de traitement. Enfin il a bien pris en compte les particularités du secteur financier.

Tout d'abord, se voulant pédagogique, le guide procède à la définition d'une donnée personnelle, conformément à la loi mauricienne. Il dresse ensuite une liste non-exhaustive des données personnelles qui font souvent l'objet de traitement dans le secteur financier. Sans qu'il soit nécessaire de reprendre intégralement la liste établie par le Bureau, il est intéressant de relever qu'il s'agit d'un large spectre de données, allant de simples données nominatives, aux données financières (numéro de carte bancaire, historique de paiement, informations de revenus, de prêts, de KYC ...), en passant par les données d'identité. Un accent spécial est mis sur les données sensibles, au sens de l'article 9 du Règlement Général sur la Protection des Données (RGPD), et les données relatives aux infractions pénales, comme les catégories particulières de données personnelles traitées par les institutions financières. Les données de santé, la biométrie et le casier judiciaire sont cités en exemple.

Dans un second temps, une fois les catégories de données concernées rappelées, le Bureau revient sur le cadre juridique qui s'applique aux traitements des données personnelles à Maurice.

L'enregistrement. Au premier rang des obligations figure celle de l'enregistrement. Conformément au droit mauricien , nul ne peut agir comme responsable de traitement ou sous-traitant (autrement dit, procéder à un traitement de données personnelles) s'il n'est au préalable enregistré auprès de la DPO. Les institutions financières ont ainsi l'obligation basique de procéder à leur enregistrement auprès de la DPO. Cette obligation d'enregistrement est facilitée par la mise en place d'une plateforme numérique (e-DPO).

Principes clés. Une fois le formalisme d'enregistrement rempli, le responsable de traitement, ou le sous-traitant, doit respecter les principes clés suivants : transparence et licéité du traitement, limitation, minimisation des données, exactitude, limitation de la durée de conservation des données, respect des droits des personnes concernées. Le guide s'est attelé à une explication de chacun de ces principes.

© iStock

Sécurité des données et conformité juridique. En tant que responsables de traitement, les institutions financières doivent par ailleurs définir des politiques et prendre des mesures techniques et organisationnelles appropriées pour démontrer que les traitements auxquels elles procèdent sont conformes à la loi. Ces mesures sont d'abord relatives à la sécurité des données. Des standards tels que ISO 27001 et la National Institute of Standards and Technology Cybersecurity framework existent et sont préconisés par le guide. D'autres mesures, telles que l'établissement d'un registre, la rédaction d'une analyse d'impact (PIA ou AIPD), ou la désignation d'un délégué à la protection des données, sont aussi à la charge du responsable de traitement.

Cloud computing et prospection commerciale. En cas d'utilisation du cloud impliquant des transferts de données, les institutions financières doivent être en mesure de fournir la preuve de garanties appropriées pour la protection et la sécurité des données, ou en cas de doute, demander l'avis de la DPO. En cas de prospection commerciale, elles doivent obtenir un consentement valide et être en mesure de le démontrer.

Sanctions pécuniaires et pénales. Le guide permet également de voir le tableau des sanctions prévues par le droit mauricien en cas de manquements. La non-conformité ou les contraventions à la loi sont punies par exemple par une amende ne pouvant dépasser 200 000 roupies. Le refus de collaboration avec la DPO, le traitement illégal des données, les fausses déclarations sont également visés et sont punis par des amendes, voire même passibles de peines d'emprisonnement.

Autres concepts. Enfin, le guide souligne les conditions du consentement, rappelle les conditions de traitement des données sensibles, dont celles des enfants, insiste sur la nécessité et les conditions de notification d'une violation de données, et détaille les droits des personnes concernées, notamment le droit d'accès, le droit d'effacement et le droit à l'opposition.

Pour conclure, le guide relève les particularités du système financier: les traitements relatifs au blanchiment d'argent et le financement du terrorisme d'une part, et les technologies financières (fintechs) d'autre part.

Le blanchiment d'argent et le financement du terrorisme. Transparence financière, lutte contre le blanchiment d'argent et protection de la vie privée... Les enjeux liés à certains traitements de données dans le secteur financier sont importants. La DPO note que ce type de traitement doit avoir une base légale claire et détaillée sans manquer d'être nécessaire et proportionnel à la finalité poursuivie. Le consentement libre doit être considéré quand c'est possible. Dans le cas contraire, il est possible de fonder ce type de traitement sur la base de « mission d'intérêt public » pour les organismes publics ou d' « obligations légales » pour les organismes privés. Ces traitements permettent la lutte contre le blanchiment d'argent et le financement du terrorisme en garantissant l'existence d'informations adéquates, exactes, et actualisées sur les bénéficiaires effectifs et le contrôle des personnes morales. Ils doivent être accessibles aux autorités compétentes à travers, par exemple, la mise en place d'un registre des bénéficiaires effectifs.

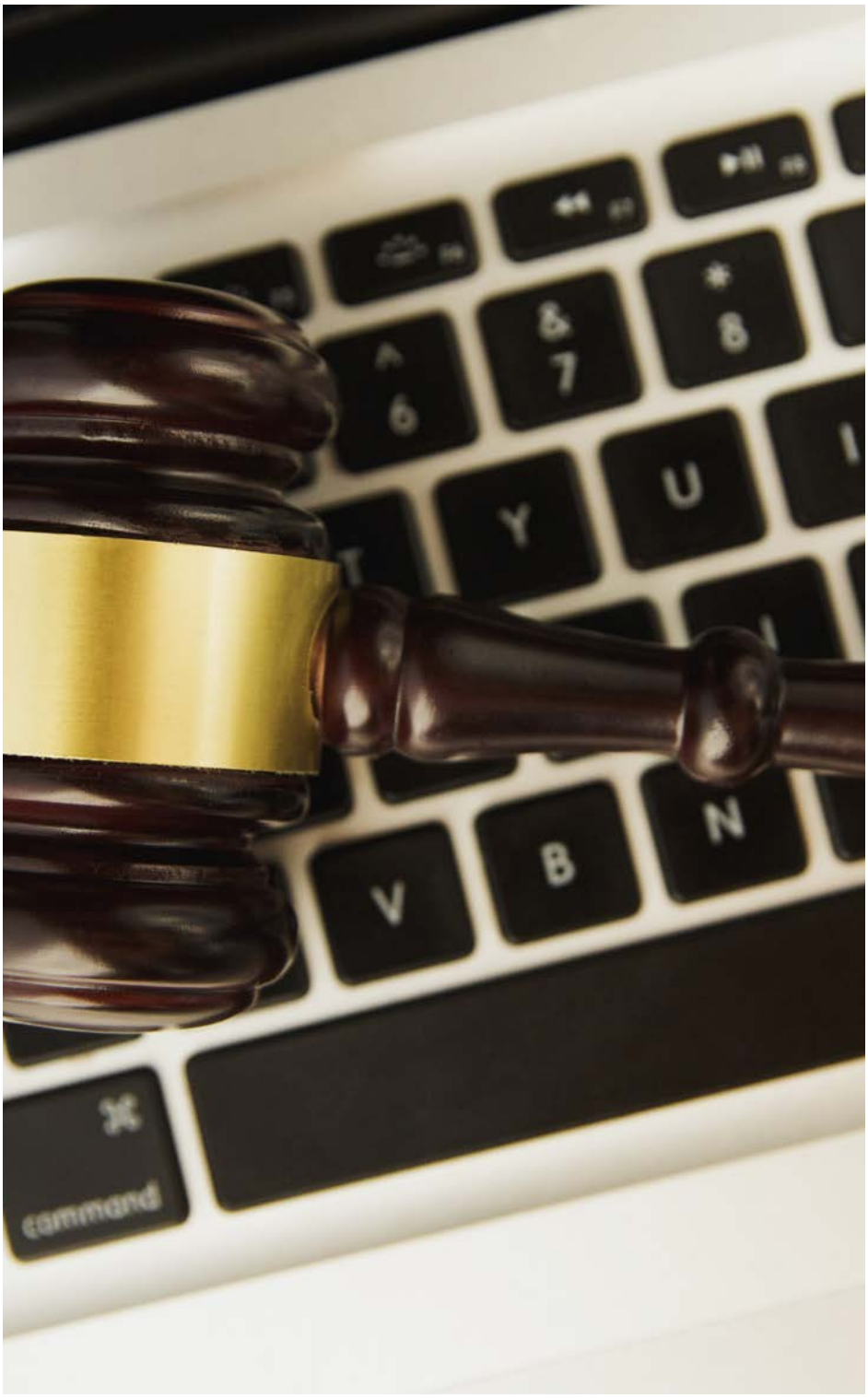
Les technologies financières (fintechs). Les fintechs sont des entreprises qui proposent des services financiers, à travers de nouvelles technologies, pour concurrencer les méthodes traditionnelles. Les technologies utilisées sont l'intelligence artificielle, la blockchain, le big data, ou encore le cloud computing. Le guide tient à rappeler qu'en plus des principes clés précités, les fintechs doivent adopter une approche basée sur le privacy by design, faire preuve de loyauté dans les traitements, et procéder à des audits de conformité réguliers.
La DPO œuvre pour l'acculturation à la protection des données personnelles en Ile Maurice. Les précisions sectorielles telles que celles-ci revêtent donc une importance particulière.
J.Y.K

© iStock

L'AUTORITÉ DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL INFLIGE UNE AMENDE TOTALE D'ENVIRON 55 000 € À TROIS ORGANISATIONS

Par Franck ADOPO

Le traitement de données à caractère personnel, quelle que soit leur nature, doit obligatoirement reposer sur une base légale. C'est ce que l'autorité de protection des données à caractère personnel du Kenya (ci-après « l'ODPC ») a reproché à trois établissements kenyans. Elle a infligé dans les décisions n°0778, n°0607 et n°0841 de septembre 2023, trois sanctions record d'un montant total de 9.375.000 Kenya Shillings (KES) soit environ 55.000 euros.



© iStock

La première sanction, d'un montant 2.975.000 KES a été infligée à un établissement de crédit en ligne. Cette sanction est survenue à la suite de deux différentes plaintes déposées les 11 et 30 mai 2023 auprès de l'ODCP. Les plaignants reprochaient à l'établissement de crédit de les avoir contactés à travers des messages et des appels téléphoniques sans leur consentement. Ces appels et messages étaient accompagnés de menaces pour l'un et d'injures pour l'autre. En réalité, ces personnes ont été contactées à plusieurs reprises par l'établissement de crédit en ligne à propos de dettes qu'elles n'avaient pas contractées personnellement. En effet, ces dettes avaient été souscrites par des personnes de leurs entourages respectifs. Selon le mode opératoire de l'éta-

© iStock

blissement de crédit, le souscripteur est amené à désigner une personne référente au moment de la souscription du prêt et à donner accès à son annuaire téléphonique à l'établissement de crédit via une application mobile. L'établissement de crédit se charge alors en cas d'insolvabilité de contacter la personne référente afin de mettre la pression sur le souscripteur. L'établissement de crédit a reconnu ces faits.

La deuxième sanction, qui s'élevait à un montant de 1.850.000 KES a été prononcée contre un restaurant-bar. Cette sanction fait suite à la publication d'images de leurs clients sur les réseaux sociaux, sans le consentement de ces derniers. Enfin, la troisième sanction est la plus sévère. Le montant de l'amende s'élève à 4.550.000 KES. Dans cette affaire, il s'agissait d'un établissement d'enseignement scolaire qui avait procédé à la publication de photos d'enfants mineurs à des fins de marketing sur ses réseaux sociaux, notamment Tik Tok, sans le consentement exprès des parents. L'ODPC a alors été saisie d'une plainte d'un parent d'élève à qui l'établissement d'enseignement a refusé de communiquer les bases légales du traitement. À l'issue de son enquête, il s'est avéré que les faits niés par l'établissement d'enseignement étaient fondés.

Il s'agit en réalité de sanctions inédites. Dans son communiqué de presse, l'ODPC a rappelé qu'à travers ces sanctions, elle souhaitait envoyer un message fort aux établissements de crédit en ligne, aux restaurants et bars et aux établissements d'enseignement qui traitent en majorité des données de mineurs. Par ailleurs, elle rappelle que c'est la première fois qu'un établissement d'enseignement est sanctionné aussi lourdement.

L'ODPC reproche à l'ensemble de ces établissements plusieurs manquements à la législation kenyane sur la protection des données. Le manquement commun à l'ensemble des décisions est le défaut de recueillement de consentement des personnes concernées avant le traitement de leurs données. Cette absence de consentement a été constatée tant dans la collecte directe des données que dans la collecte indirecte.

Ce défaut de consentement entraine ainsi l'absence de base légale au traitement. Or, l'absence de base légale est une cause de

non-respect des obligations du responsable de traitement prévues par la loi kenyane.
En somme, ce sont plusieurs articles de la loi qui ont été ignorés. La lumière doit être principalement mise sur la violation des articles 26, 30 ou encore 33, portant dans ce dernier cas sur le traitement des données des mineurs.

Il est important de rappeler que le point de convergence des décisions est bien le défaut de base légale au traitement des données, y compris pour le traitement de données de mineurs.
Il faut aussi rappeler que le Kenya, par le biais de l'ODPC, fait du respect de la loi sur la protection des données une priorité. Cette priorité se manifeste par la multiplication des contrôles, l'exécution des plaintes et les sanctions prononcées à toutes les entités assujetties à la loi de 2019.
Selon l'article 4 de la loi, toutes les entités établies sur le territoire kenyan et qui traitent les données sont soumises à tous les principes liés au traitement des données. En raison de la nature de leurs activités et de leur situation géographique, les trois établissements en l'espèce sont soumis à la législation kenyane. En effet, ils traitent respectivement les données comme les contacts téléphoniques, les noms, les images d'adultes et de mineurs, tout en étant établis sur le territoire kenyan.
Or, dans le cadre des mécanismes mis en place par la loi, aucun traitement de données ne peut se faire sans base légale. Il s'agit des exigences établies afin de garantir le respect des principes de licéité et de légitimité des traitements.
Par ailleurs, en vertu de ces principes, chaque traitement de données mis en place ne saurait se faire de manière illicite et doit répondre aux exigences prévues par la loi. À ce propos, la loi kenyane prévoit plusieurs bases légales sur lesquelles le responsable de traitement peut asseoir son traitement à l'instar de la plupart des lois nationales sur la protection des données.
Ces bases légales ne sont pas cumulatives. Et c'est à juste titre que certains auteurs parlent d'hypothèses (1). Tandis que d'autres font du consentement la base légale de principe et les autres bases légales des exceptions (2). En marge de cette divergence, certains auteurs ont choisi de s'aligner sur la position du G29 qui considère toutes les bases légales comme équivalentes (3). En ce qui concerne la loi du Kenya, elle semble donner une place de choix au consentement.
À cet effet, le consentement est défini par l'article 2 comme « toute manifestation de la volonté expresse, non équivoque, libre, spécifique et informée de la personne concernée, exprimée par une déclaration ou par une action affirmative claire, signifiant son accord pour le traitement des données à caractère personnel la concernant » (4). C'est le consentement tel que défini qui est à la base des trois récentes décisions de l'ODPC.
En l'espèce, les personnes concernées, dans la première affaire, n'ont reçu aucune information sur les pratiques de l'établissement de crédit. Or, ce dernier avait accès à leurs contacts par le biais de l'application mobile installée par les débiteurs. Dans son argumentaire, l'établissement de crédit alléguait qu'elle avait obtenu le consentement des débiteurs téléphoniques. Cependant, pourrait-on étendre aux personnes concernées le premier consentement obtenu auprès des débiteurs ? Ce premier consentement est-il valable pour le traitement postérieur effectué sur les données des personnes concernées ? La loi exige que le consentement soit personnel, spécifique et clair.
Par ailleurs, il est ressorti de l'argumentaire du responsable de traitement que des employés de l'établissement ont outrepassé leurs compétences. En effet, l'établissement de crédit a reconnu que certains de ses employés avaient eu recours à l'intimidation pour arriver à leurs fins. Face à cette situation, elle allègue avoir présenté ses excuses pour ces excès. Toutefois, le repenti et les excuses pourraient-ils écarter l'application de la loi dans toute sa rigueur ?

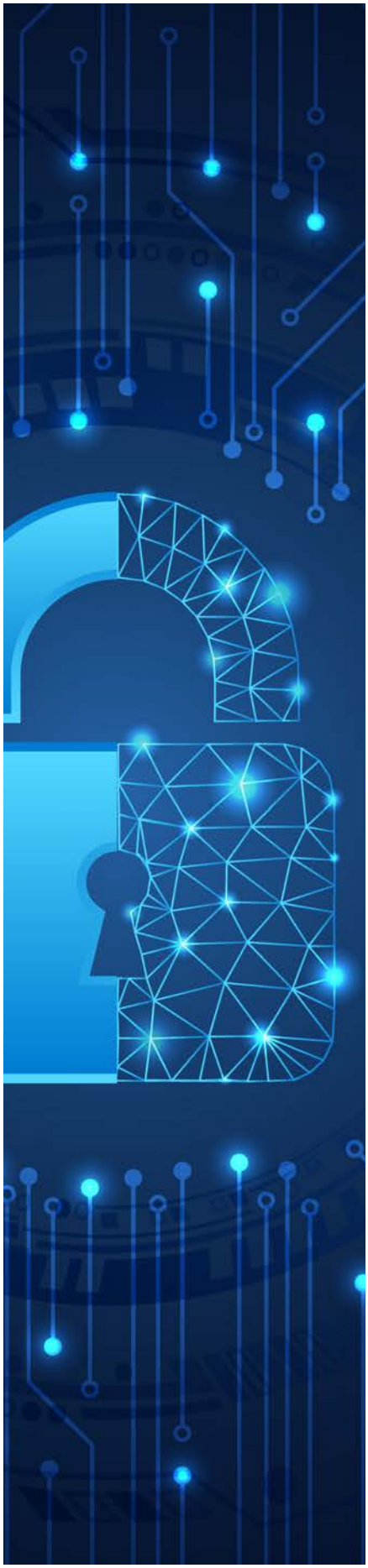
Dans le deuxième cas, les images des clients ont été collectées et diffusées après leur passage dans le restaurant-bar. Or, ces clients n'ont nullement donné leur consentement pour que leurs images soient collectées et encore moins diffusées sur les réseaux sociaux. En soi, la seule présence des clients dans le restaurant-bar pourrait-elle valoir un consentement pour l'utilisation de leurs images sur les réseaux sociaux ? La loi prévoit que le consentement ne peut être tacite. Il doit plutôt être clair et exprès.

Dans la troisième situation, le responsable de traitement a tout d'abord opposé une résistance. En effet, dans son argumentaire, il avait nié les faits qui lui étaient reprochés par le parent d'élève. Ce n'est qu'à l'issue des investi-

gations de l'ODPC qu'il a fini par reconnaître les faits. Cependant, il précise avoir informé les parents d'élèves via un message diffusé dans un groupe de discussion.
Alors, la simple mesure d'information constitue-t-elle une base légale de traitement ? D'autant plus que la forme de la mesure d'information est très contestable. En effet, la mesure d'information comme prévu par la loi doit obligatoirement contenir certaines mentions. Au titre de ces mentions figurent notamment la finalité du traitement, la base légale du traitement et les différents droits dont dispose la personne concernée vis-à-vis du traitement en question. Or, l'information collective fournie par le responsable de traitement dans le groupe de diffusion ne respectait pas les formes requises par la loi. Cependant, ce qui retient plutôt l'attention de l'ODPC, c'est l'absence de consentement des parents. L'autorité déplore le fait que les parents n'aient pas eu l'occasion de donner leur consentement pour le traitement des données de leurs enfants mineurs comme le prévoit l'article 33 de la loi. Ce fait constitue un manquement encore plus grave selon l'ODPC, car il retire à ce traitement sa base légale.
Dans l'ensemble des cas, l'ODPC a retenu des sanctions contre les différents responsables de traitement pour absence de base légale au traitement.

À travers ces sanctions, l'ODPC a tenu à envoyer un message fort aux établissements appelés à traiter des données soumis à la loi kenyane. L'objet de ce message était de rappeler à ces derniers que la protection des données n'était pas une tendance ou une option. Il s'agit plutôt d'une obligation pour tous.
F.A

(1) Jacquemin H, Degrave E, eds. Le Règlement Général Sur La Protection Des Données (R.G.P.D./G.D.P.R.): Premières Applications et Analyse Sectorielle. Anthemis; 2020, p.25.
(2) Lo M. La protection des données à caractère personnel en Afrique: réglementation et régulation. Baol éditions; 2017, p.103.
(3) Tambou O, López Aguilar JF. Manuel de droit européen de la protection des données à caractère personnel. Bruylant; 2020, p.130.
(4) The Data Protection Act, 2019, article 2 (traduit).



© iStock

CONTRÔLE OU SENSIBILISATION ? LES ENJEUX DE LA HAPDP

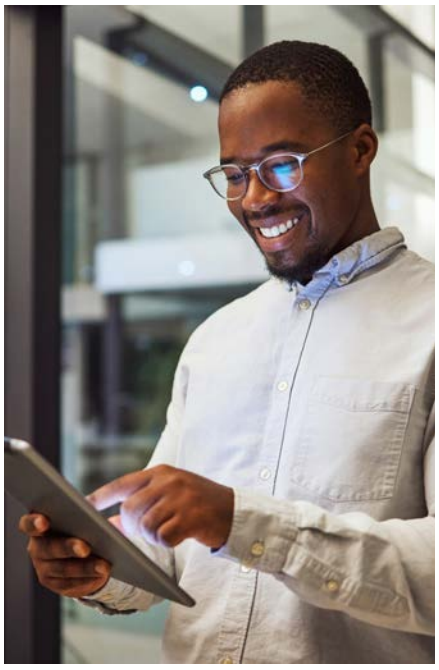
Par Mahadi MAIFADA MAGOUDANI

Dans un contexte de sensibilisation et de diffusion de la réglementation, cet article explore les débuts de la Haute Autorité de Protection des Données Personnelles (HAPDP), mettant en lumière les obstacles rencontrés, qui pourraient expliquer le délai observé pour le lancement de son premier programme de contrôle. Nous examinons ensuite ce programme pour évaluer s'il représente un véritable virage vers un contrôle effectif ou s'il prolonge la stratégie préventive initiale. Enfin, des suggestions seront formulées pour renforcer l'action de la HAPDP et favoriser la conformité aux normes de protection des données au Niger.

La HAPDP, créée en vertu de la Loi n° 2017-28 du 03 mai 2017 en tant que l'une des autorités de contrôle les plus récentes en Afrique de l'Ouest francophone, a débuté ses activités en 2020, faisant face à des défis majeurs liés à des ressources insuffisantes et à des ajustements constants de son statut. Comparée à ses homologues notamment burkinabè, ivoirienne et sénégalaise, elle demeure l'autorité ayant subi le plus de réformes.

Ces obstacles ont retardé la mise en œuvre de contrôles effectifs pendant plusieurs années et ont également influencé la compréhension de la réglementation par les acteurs contrôlés, appelés responsables de traitement. Dans sa première année d'activité, la HAPDP a adopté une approche stratégique peu engageante en mettant en place des formulaires de traitement de données sans consultation préalable des acteurs contrôlés. Cette démarche a engendré des difficultés, notamment des problèmes de compréhension des textes et des réticences de certains acteurs à payer les frais de délivrance des actes de conformité . À la suite de ces difficultés initiales, les conditions idéales pour des contrôles effectifs n'étaient manifestement pas réunies au cours de ces premières années, d'autant plus que seuls quatre récépissés ont été délivrés entre 2020 et 2021, selon les discours officiels de la HAPDP . Cette situation soulève des interrogations sur les critères employés par l'autorité pour déclarer conforme un responsable de traitement.

En effet, malgré ces chiffres limités, la HAPDP a publié à la fin de l'année 2021 sur son site la liste des responsables de traitement jugés conformes à la loi . Cette initiative soulève des questions sur la proactivité des acteurs contrôlés dans l'adaptation aux normes de protection des données. La publication de cette liste peut être interprétée comme une réaction à la nécessité de rendre compte de l'état de conformité dans le pays, mais elle souligne également la nécessité d'une réadaptation de la stratégie de l'autorité nigérienne. La stratégie, revue et adaptée en cours de 2021 avec le soutien d'organismes partenaires tels que l'Organisation internationale de la francophonie (OIF) , la Commission de l'informatique et des libertés (CNIL) et divers réseaux, a constitué une étape significative en consolidant le statut de l'autorité et renforçant la capacité du personnel . Cette démarche a donné naissance au « Plan stratégique 2021-2025 », dont découle directement le programme de contrôle au titre de l'année 2023 examiné en l'espèce.



© iStock

En analysant concrètement la déclaration de la HAPDP concernant les acteurs contrôlés dans le cadre de ce programme, on observe une sélection de secteurs clés qui traitent probablement des volumes significatifs de données personnelles. Les secteurs mentionnés, tels que les compagnies de transport, la santé, les banques, et les assurances, sont souvent des domaines où le traitement des données personnelles et sensibles est fréquent. En particulier, le secteur des compagnies de transport semble être celui où le transfert de données personnelles est le plus manifeste.

Malgré tout, il est surprenant que le secteur des télécommunications, mais aussi certaines structures et organismes publics, ne fassent pas partie des secteurs visés.

Pour le premier point, il importe de souligner que l'ensemble de l'industrie de production de données repose largement sur les télécommunications, gérées par les opérateurs du secteur. Plus spécifiquement, la téléphonie mobile se distingue dans l'espace ouest africain en tant que secteur clé dans la facilitation de la connectivité et de l'échange massif de données entre les différents acteurs. La HAPDP aurait dû accorder une attention particulière à la conformité de ces opérateurs.

S'agissant du deuxième point, avec l'émergence actuelle des projets dits de « modernisation de l'administration publique » et la multiplication des initiatives de traitement de données biométriques par les pouvoirs publics et partenaires, il aurait été judicieux pour la HAPDP de donner la priorité à ces activités lors de ses premières actions de contrôle.

Pour conclure, le contrôle réalisé par les équipes de la HAPDP semble davantage exprimer un exercice pédagogique et de sensibilisation des responsables de traitement qu'un véritable processus de contrôle à finalité répressive. Toutefois, en comparaison, la CDP du Sénégal a mis en place aux premières années de son démarrage deux mécanismes intéressants. Le premier, nommé l'appel à déclaration, enjoint les responsables de traitement à se conformer à la législation. Le second, appelé demande d'explication, aboutissant le plus souvent à des mises en conformité, est consécutif à une plainte. Ces approches ont l'avantage de préparer le terrain avant d'éventuels contrôles, tout en intégrant une dimension pédagogique. Cette expérience pourrait inspirer l'autorité nigérienne à réajuster sa stratégie et à intégrer des méthodes similaires afin de renforcer son influence dans un écosystème qui semble relativement moins réceptif à la question de la protection des données personnelles.

M.M.M

© iStock

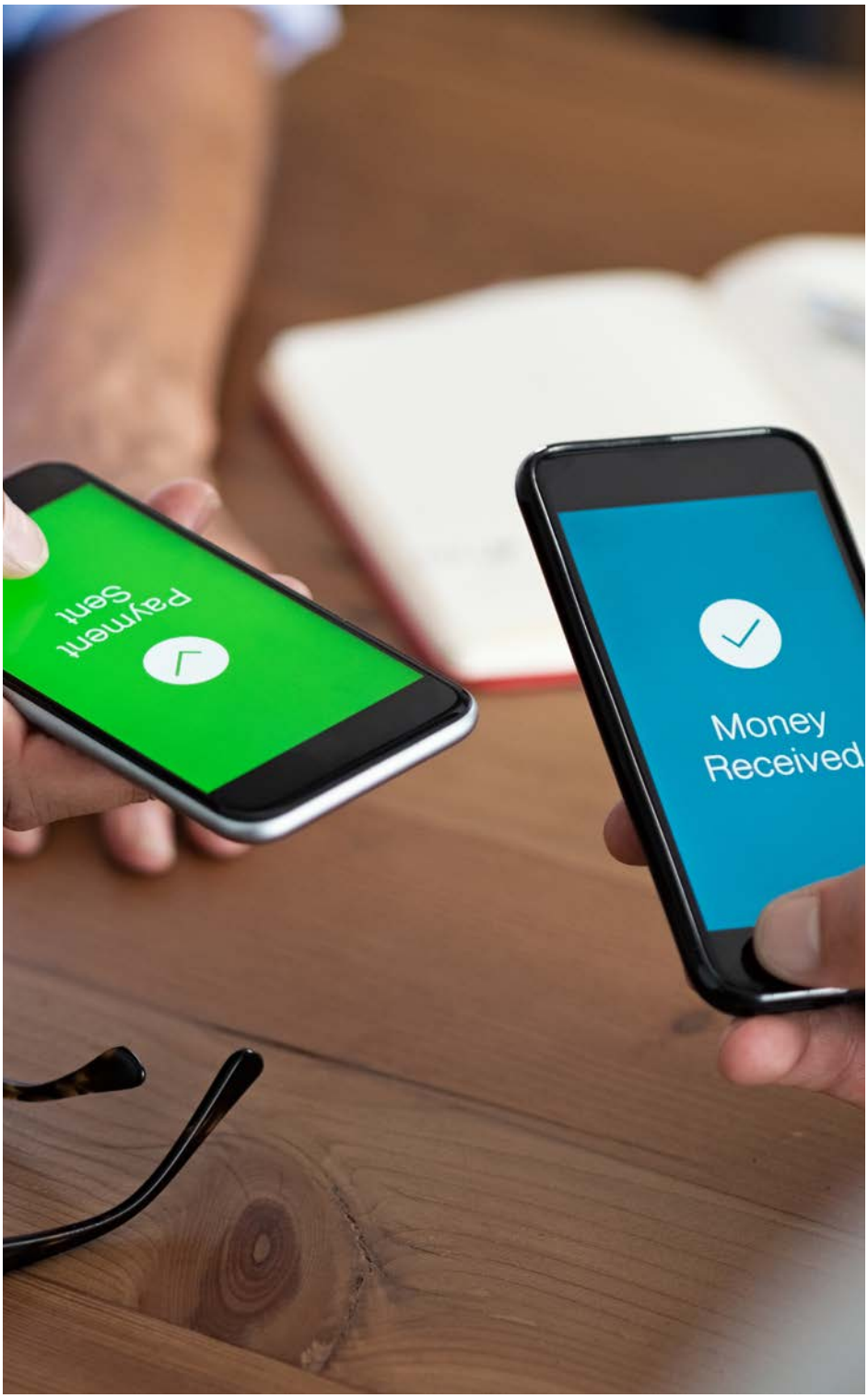
MISES EN DEMEURE DE L'ARTCI À L'ENCONTRE D'APPLICATIONS DE PRÊT EN LIGNE

Par Jean Marc DIGBLI

La Côte d'Ivoire, de même que de nombreux pays en Afrique, fait face à une rapide évolution technologique ainsi qu'à la montée en puissance de l'utilisation des applications mobiles pour les services financiers. Ces applications mobiles jouent un rôle important dans l'inclusion financière en Côte d'Ivoire. Des services tels que le paiement mobile, les transferts d'argent et la banque mobile sont de plus en plus populaires, ce qui permet aux populations non bancarisées d'accéder aux services financiers.

Toutefois, cette évolution n'est pas exempte de risques liés à la protection des données personnelles des citoyens ivoiriens. Les entreprises opérant donc dans le secteur financier, en raison de la nature hautement confidentielle des informations qu'elles manipulent, notamment les données financières, devraient être conscientes de ces risques. Malheureusement, en pratique, ce n'est pas toujours le cas.

A titre d'illustration concrète, nous évoquerons dans cet article les mises en demeure émises le 8 août 2023 par l'autorité de protection des données à caractère personnel de la Côte d'Ivoire (ARTCI) à l'encontre de certaines de ces applications mobiles, précisément de prêt en



© iStock

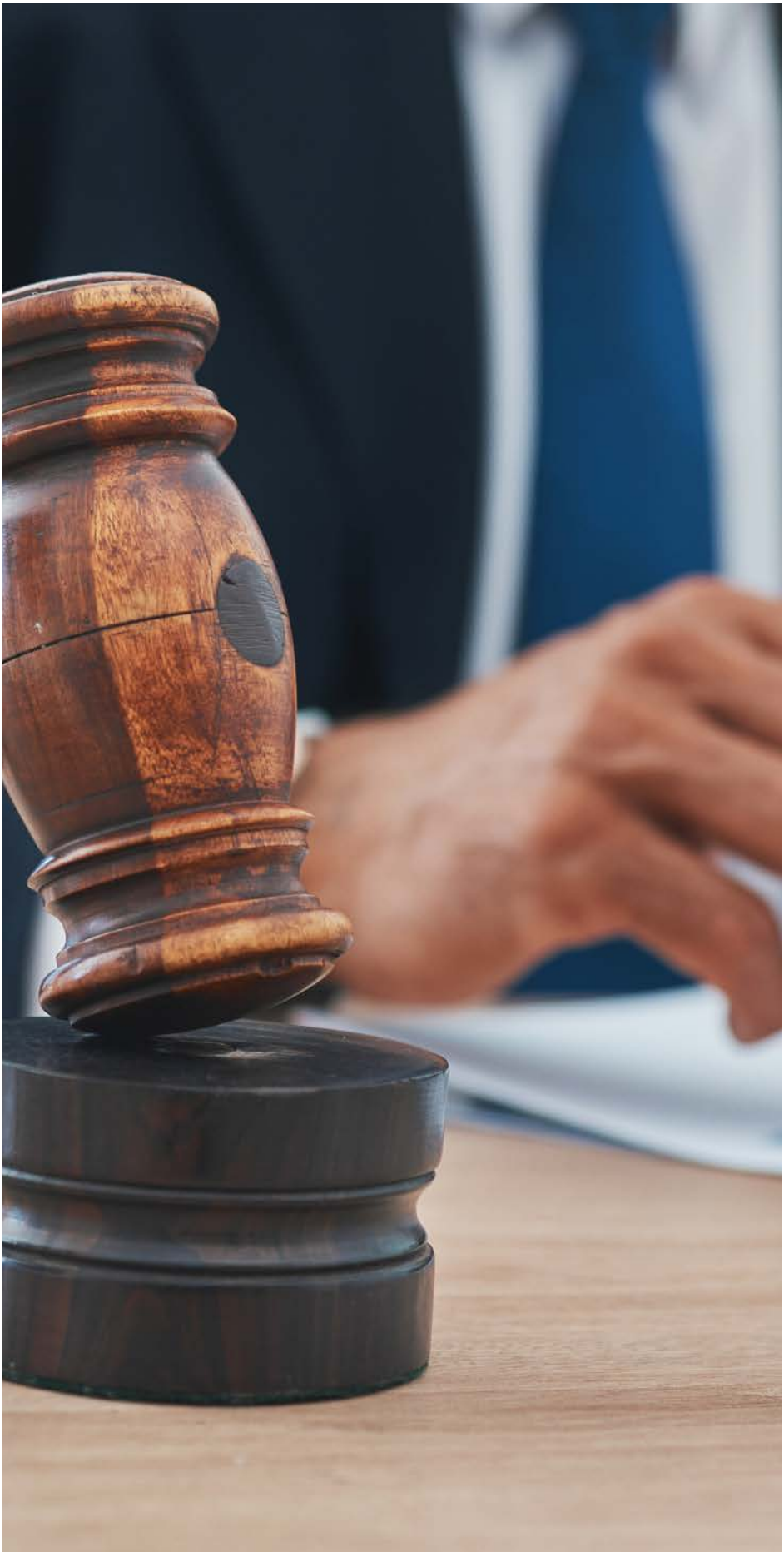
ligne. Les applications ciblées sont les suivantes : le prêt-prêt d'Argent Mobile, Prêtfacile, Easy, Cash-prêt en ligne, PrêtRapid, le djai225-prêt en ligne, MiniPrêt, Joliprêt-application de prêt, Juju argent-prêt en ligne, Hiprêt et CI money.

Au-delà d'un simple appel à la conformité, ces mises en demeure ont également eu pour but d'alerter la population et de l'inciter à faire preuve d'une extrême vigilance à l'égard de ces applications.

Les principaux manquements constatés par l'ARTCI

Il est reproché aux applications en cause de traiter des données personnelles sans avoir effectué auprès de l'ARTCI les formalités nécessaires pour être conformes à la loi n°2013-450 du 19 juin 2013, relative à la protection des données à caractère personnel en Côte d'Ivoire. Cette loi est considérée comme la principale législation en la matière en Côte d'Ivoire. Elle vise, entre autres, à garantir la sécurité et la confidentialité des données personnelles collectées par toute personne physique ou morale. En vertu de ses articles 5 à 7, toute personne physique ou morale qui procède à la collecte de données personnelles, selon sa situation, a l'obligation de les déclarer ou d'obtenir au préalable une autorisation formelle pour le traitement de ces données auprès de l'ARTCI.

L'ARTCI a par ailleurs relevé que ces applications se servent des informations qu'elles recueillent à des fins illégales, notamment pour exercer du chantage, harceler ou extorquer de l'argent. Ces activités criminelles



© iStock

peuvent causer des dommages substantiels à la dignité et à la vie des personnes concernées, ce qui a engendré de nombreuses plaintes.

L'appel à la conformité des entreprises

Dans un premier temps, l'autorité de régulation a invité les entreprises impliquées dans le développement, ou la promotion de ces applications de prêt en ligne à se rapprocher des services compétents afin de se soumettre aux exigences de la loi dans un délai de 10 jours à compter du mardi 8 août 2023. Cette démarche est conforme au mandat conféré à l'ARTCI en tant qu'autorité de protection des données à caractère personnel, en accord avec la loi en vigueur en Côte d'Ivoire. En effet, conformément aux dispositions légales en vigueur, l'autorité de contrôle veille à ce que l'usage des technologies de l'information et de la communication ne porte pas atteinte aux libertés et à la vie privée des utilisateurs situés sur le territoire national.

En dépit de l'appel lancé par l'ARTCI, aucun des responsables de ces plateformes de prêt en ligne n'a répondu à cette demande de mise en conformité.

Recommandations de L'ARTCI

En attendant la mise en place de dispositifs réglementaires pour le blocage des sites internet donnant accès à ces applications, l'ARTCI a formulé, face à ces préoccupations, des recommandations importantes pour la population. Les utilisateurs sont encouragés à :

© iStock

- Passer en revue les autorisations accordées aux applications déjà installées sur leurs appareils mobiles et à supprimer celles qui posent des problèmes;

- Effacer toutes les données en cache de ces applications à partir des réglages des appareils mobiles.

- Ou encore procéder à la désinstallation complète de ces applications de tous les appareils mobiles.

Ces mesures simples peuvent aider les utilisateurs à réduire les risques pour leurs données personnelles et leur vie privée en éliminant l'accès de ces applications non conformes à leurs informations personnelles.

Ces recommandations sont-elles suffisantes ?

L'absence de coopération des entreprises visées par ces mises en demeure est révélatrice des défis auxquels est confrontée l'autorité ivoirienne lorsqu'elle s'efforce de faire respecter la législation sur la protection des données. Il faut donc se demander si, 10 ans après l'adoption de cette loi, le moment n'est pas venu pour l'ARTCI de prendre des sanctions plus sévères à l'encontre des entreprises non conformes à la loi.

Une action plus ferme de l'ARTCI serait non seulement justifiée, mais également nécessaire pour renforcer la protection des données personnelles et de la vie privée des citoyens ivoiriens. Cette approche renforcée pourrait consister à infliger des sanctions pécuniaires aux entreprises qui ne se conforment pas à leurs obligations en matière de protection des données. L'imposition de sanctions dissuasives aurait pour effet d'inciter les entreprises à se conformer à la réglementation, créant ainsi un environnement où les données personnelles seraient mieux protégées.

Il faut tout de même reconnaître les progrès réalisés par l'ARTCI grâce à ces mises en demeure, dont l'un des objectifs était de sensibiliser la population aux risques associés aux applications de prêt en ligne en encourageant par la même occasion la vigilance des utilisateurs.

Cela met en évidence la nécessité de continuer à sensibiliser le public aux enjeux de la protection des données personnelles et à la régulation de leur utilisation dans le contexte numérique actuel en Afrique. Une compréhension accrue de ces questions est essentielle pour que les citoyens puissent protéger leurs droits à la vie privée et pour que les entreprises se conforment aux réglementations en vigueur.
J.M.D


© iStock

VERS UNE SANTÉ NUMÉRIQUE RÉGULÉE, ÉTHIQUE ET SOUTENABLE POUR L'AFRIQUE : LEÇONS DE LA LOI « DIGITAL HEALTH BILL 2023 »

Par Prof. Benjamin GUINHOUYA

© iStock

Une loi sur la santé numérique, « The Digital Health Act » a été votée par le parlement du Kenya le 08 Septembre 2023, après une présentation initiale en date du 20 juillet 2023. Cette loi représente une initiative majeure visant à réglementer l'utilisation des technologies numériques dans le secteur de la santé. Il s'agit sans aucun doute du premier cadre réglementaire complet pour optimiser l'intégration des technologies de l'information et de la communication (TIC) au domaine de la santé. L'objectif du présent travail est de prendre appui sur ce texte en vue de stimuler des discussions et des actions collaboratives pour exploiter pleinement le potentiel de la santé numérique en Afrique, en impulsant ainsi une transformation positive du secteur de la santé sur le continent. Toutefois, avant de présenter les aspects saillants de cette loi kényane et ses leçons en termes d'opportunités et de défis pour le continent africain, il semble nécessaire de tenter une clarification des termes autour du concept de « santé numérique ».

Bref aperçu du concept de « santé numérique »

Au fil des décennies, les termes comme informatique médicale, e-santé et m-santé ont émergé pour décrire l'utilisation des technologies de l'information et de la communication (TIC) dans le domaine de la santé.

La santé numérique, introduite par Seth Frank au début des années 2000 (Frank, 2000), s'est imposée actuellement en englobant ses concurrents. Corrélativement, elle s'est élargie pour inclure divers domaines tels que

les omiques (e.g. génomique, métabolomique), l'Intelligence Artificielle (IA), la science des données, les dispositifs embarqués, les applications mobiles ou encore la télémédecine. Cette expansion qualifie la santé numérique au-delà de la simple utilisation des technologies numériques dans le domaine de la santé, la positionnant pour l'Organisation Mondiale de la Santé (OMS), comme « le domaine de connaissances et de pratiques associé à tout aspect de l'adoption des technologies numériques pour améliorer la santé, de leur conception à leur implémentation ». Cette définition est alignée avec la résolution WHO EB142/20 de 2017 et montre bien que la santé numérique englobe la e-santé, dont l'usage la confond encore avec la santé numérique (Safon, 2021).

La transition de la e-santé à la santé numérique met l'accent sur l'importance des consommateurs numériques, avec l'utilisation accrue d'appareils intelligents, d'équipements connectés, et d'autres concepts émergents tels que l'Internet des objets (ou Internet of Things en anglais :"IoT"), l'IA, le big data et la science des données. Cette perspective connecte la santé numérique aux applications pratiques et aux résultats mesurables, soulignant que les technologies numériques sont des moyens pour atteindre un objectif, à savoir l'amélioration de la santé. Dans notre analyse, nous adoptons la définition de Kairo et al. (2022) pour dissiper toute ambiguïté. Selon ses auteurs, la santé numérique englobe la gestion de la santé et la prévention des maladies, la promotion de la santé, la prédiction des risques, et le développement d'outils pour les professionels de santé. Cela va au-delà des soins médicaux spécifiques, qui relèvent de la médecine numérique, une modalité particulière de la santé numérique.

« Digital Health Act, 2023 » du Kenya

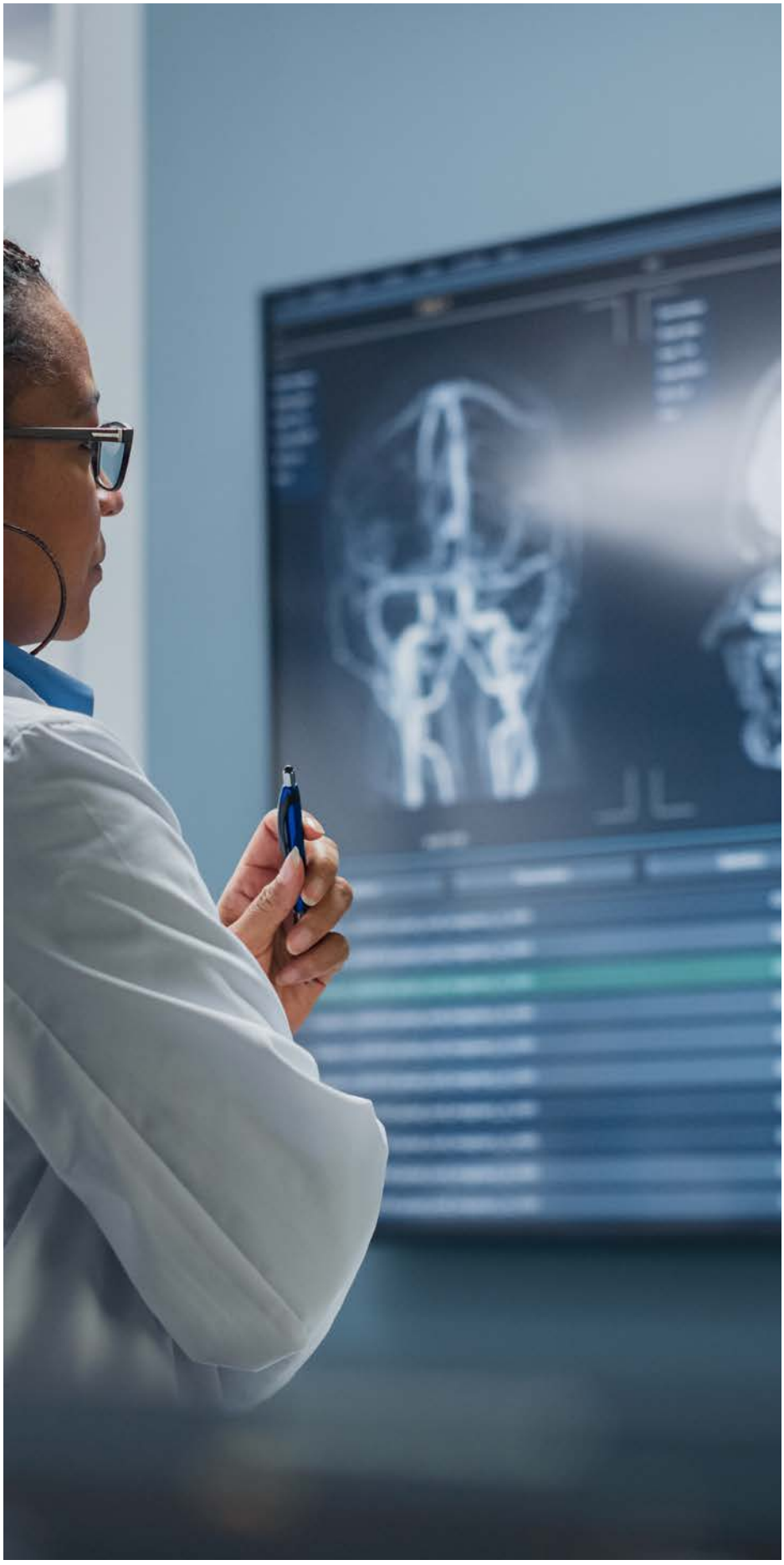
La loi kényane a proposé des définitions claires et différenciées de la santé numérique et de la e-santé. Dans ce texte, la santé numérique est conçue comme « le domaine de connaissance et les pratiques associés au développement et à l'utilisation des technologies numériques en vue d'améliorer la santé » alors que la e-santé signifierait « l'usage combiné de la communication électronique et des technologies de l'information dans le secteur de la santé, incluant la télémédecine». Au-delà des clarifications conceptuelles, le « Digital Health Bill 2023 » permet d'instituer l'Agence de la Santé numérique, chargée d'opérationnaliser les directives et dispositions de la loi, y compris dans la fourniture d'un cadre pour la prestation de services de santé numérique ; l'établissement d'un système d'information intégré et la protection des données de santé personnelles. La loi met également l'accent sur l'autonomisation des patients, l'innovation, l'interopérabilité et la confidentialité, et elle est conçue pour soutenir l'objectif du Kenya d'atteindre une couverture sanitaire universelle d'ici 2030 grâce à l'utilisation de la technologie numérique dans le domaine de la santé . En couvrant des domaines aussi larges et variés, cette loi établit un cadre réglementaire exhaustif pour le pays.

La « Digital Healt Act » présente de nombreux avantages pour le secteur de la santé au Kenya, avec un impact potentiel au-delà des frontières nationales. Ces avantages comprennent en particulier les possibilités liées à: i) l'amélioration de l'accès aux soins de santé : La mise en œuvre des technologies numériques offre des possibilités d'améliorer l'accessibilité des soins de santé par la réduction des coûts, l'augmentation de la disponibilité des services, et la diminution des distances géographiques entre les patients et les prestataires. À titre d'exemple, le programme de télémédecine « e-Kamoyo » au Kenya a considérablement amélioré l'accessibilité des soins de santé pour les résidents des régions rurales ; ii) l'augmentation de la qualité des soins : Les technologies numériques ont le potentiel d'améliorer la qualité des soins de multiples manières, notamment en facilitant la communication entre les professionnels de santé, en renforçant la prise de décision clinique, et en optimisant la surveillance des patients. Le programme de suivi des patients « mTrac » au Kenya illustre la manière dont ces avancées contribuent à une meilleure qualité de soins, en particulier pour les personnes atteintes de maladies chroniques ; et iii) l'accroissement de l'efficacité du système de santé: Les avantages de la santé numérique s'étendent également à l'efficacité du système de santé, avec des applications telles que l'automatisation des tâches administratives, la collecte et l'analyse de données de santé, et l'amélioration de la coordination des soins. Le programme « eHealth Kenya »

est un exemple concret de la manière dont ces technologies peuvent améliorer la coordination des soins en permettant le partage efficace des dossiers médicaux entre les prestataires de soins.

Défis potentiels de la santé numérique au Kenya et en Afrique subsaharienne

L'implémentation de la santé numérique soulève des préoccupations cruciales liées à la confidentialité des données. La collecte et l'utilisation de données de santé via les technologies de l'information nécessitent des mesures de protection adéquates. La loi propose des dispositions pour y remédier, telles que la création d'un registre d'organismes autorisés, l'obligation de mettre en place des mesures de sécurité, et la conformité aux lois sur la protection des données. Le Kenya, comme un nombre croissant de pays africains, dispose depuis 2019 d'une législation, la « Data Protection Act » visant la protection des données personnelles. La « Digital Health Act » doit pouvoir prendre appui également sur la précédente législation. A la limite, ces problématiques d'ordre technico-matériel et d'équité dans la distribution des services de santé numérique ne sont ni spécifiques au Kenya, ni spécifiques à l'Afrique. Au contraire, les pays africains peuvent faire de la quasi-inexistence de systèmes d'information pour la santé une opportunité unique pour anticiper les questions de standardisation, d'interopérabilité ou de mise à l'échelle de systèmes d'information résilients et efficaces, en tirant les meilleures leçons des initiatives déjà opérationnelles au niveau



© iStock

international.

En revanche, la « Digital Health Act » manque clairement, dans ses dispositions, de faire à la santé publique la place qu'elle mériterait ; l'emphase ayant encore une fois été mise sur les services de soins de santé (notés « services de santé ») dans un mode devenu classique et déséquilibré. Quand on prend conscience de l'importance des maladies chroniques non-transmissibles (impliquées dans plus de 2/3 des décès mondiaux) et du double fardeau de santé publique dont souffrent les pays africains, y compris le Kenya, il est urgent d'avoir une vision de santé publique et de l'inclure systématiquement au sein des développements technologiques contemporains. Il serait mal approprié aux pays africains d'avoir à limiter les efforts à la médecine numérique, qui devrait être incluse dans une stratégie de santé numérique, ne pouvant se résumer à sa seule dimension médicale.

Plus importantes encore sont les questions d'ordre non normatif que soulèverait l'implémentation des solutions de santé numérique au Kenya en particulier, et en Afrique subsaharienne en général. A l'heure où le panafricanisme se réactive, y compris dans l'espace africain d'expression française, pour proposer une vision tirée de l'expérience, autre que celle que l'Afrique a dû adopter jusqu'à présent, il est fort à parier que les infrastructures technologiques et/ou technico-matérielles ne sauront plus suffisantes pour satisfaire les exigences de développement endogène. Celles-ci sont en effet nourries par une jeunesse africaine de plus en plus éduquée.

En substance, dans cette volonté de reconquête et de réappropriation des savoirs et pratiques ancestraux, y compris par le biais d'une reconnaissance progressive des médecines traditionnelles africaines et la prise en compte des pharmacopées locales, il est urgent que les développements technologiques au titre de la santé numérique puissent aussi s'appuyer non seulement sur les compétences et acteurs locaux, mais également sur les principes et une certaine métaphysique authentiquement africaine.

Dans le cas des solutions de santé numérique, il apparaît que le développement et l'implémentation de telles solutions soient instruites d'une éthique ancrée dans les représentations africaines. Concrètement, l'éthique occidentale, qu'elle soit d'inspiration kantienne ou utilitariste, fait primer l'individu sur la nature et la collectivité. Même si les métaphysiques à l'œuvre dans l'action en Afrique subsaharienne ne sont pas consignées dans des textes, la morale et les principes éthiques s'expriment et se racontent, dans une tradition orale, à travers contes ou proverbes : classiquement, la mutualité y prime sur l'individualité.
Toutefois, en raison de la pénétration historique des cultures et valeurs européennes et orientales en Afrique, il devient fondamental de considérer la complexité de la cohabitation ainsi que l'expression différente de valeurs morales et principes éthiques que chacun a pris pour habitude de considérer comme « universels ». Ainsi, en Afrique subsaharienne, le « Cogito ergo sum » (« je pense donc je suis ») cohabite avec, et fait même

© iStock

parfois place au « Sumus ergo sum » (Cullivan, 1997), qui s'apparente au principe sud-africain du « Ubuntu » (i.e. « je suis parce que nous sommes »). Par ailleurs, non seulement, le « Sumus ergo sum » ne procède pas d'une modalité unique d'expression à travers toute l'Afrique subsaharienne mais encore plus, la composition ou le fonctionnement du couple {« Cogito ergo sum » ; « Sumus ergo sum »} procède d'un dosage bien différent d'une personne à l'autre, y compris au sein d'une même famille nucléaire.

C'est en cela que l'Afrique subsaharienne est plus plurielle, plus complexe et plus riche de sa diversité qu'on ne l'a pensée ou décrite jusqu'à date. L'accueil des principes et valeurs d'importation constitue rarement un rejet de soi et un effacement des valeurs ancestrales africaines. Sans la compréhension de ces subtilités et leur prise en compte, ce serait une nouvelle occasion manquée que de tenter de faire se rencontrer deux mutations fortes et profondes : l'une sociale et sociétale d'une Afrique qui veut se redéfinir ; l'autre technologique, au bénéfice de la santé des populations africaines et du développement du continent. Les répercussions d'une éthique de la mutualité à l'instar de l'Ubuntu, dans laquelle les bénéfices de la communauté prévalent sur ceux de l'individu, sont très concrètes en matière de santé numérique: Comme le soulignait le Dr. Corrigan : « Si une communauté peut utiliser une application de santé en vue d'un bénéfice collectif, alors l'individu devrait consentir à l'utilisation de ses données. » (Manhart, 2023). Il ne s'agit guère d'un appel à des abus divers et variés vis-à-vis

© iStock

d'un individu particulier, dont la protection devrait de fait être assurée par l'ensemble du corps social.
En conséquence, il est important que les décideurs de politique de santé vers l'Afrique, pour l'Afrique et en Afrique incluent ce corpus éthique à leur réflexion et stratégie d'autant qu'ils ont été construits et fonctionnent encore beaucoup sur la base d'organisations politico-administratives, pour le moins calquées sur le modèle occidental, sinon héritées de la période coloniale. S'ils l'ignorent, cette éthique devrait désormais figurer
dans les chapitres majeurs de leurs programmes de formation et/ou de préparation à l'exercice des fonctions de décideurs de politique de santé. Un tel niveau de responsabilité implique une pleine conscience de la nécessité de consultations préalables et sincères des communautés, y compris au niveau granulaire le plus faible.

Enfin, compte tenu des problèmes que soulèvent le changement climatique et le coût énergétique associé aux infrastructures telles que les « Data centers » ou celui lié à l'exploitation des données massives de santé pour les développements algorithmiques, les solutions de santé numérique pour l'Afrique devront prendre en compte ces enjeux planétaires, sur la base d'une analyse prospective et de l'évaluation du rapport entre les bénéfices de solutions alternatives. Pour que cela puisse se faire, l'engagement des acteurs locaux est primordial ; les solutions clé en main devront subir les tests les plus rigoureux en vue de leur adoption et mises en œuvre sur le continent.

Recommandations pour l'Afrique

1. Renforcement de la protection des données
o Instituer des évaluations régulières pour garantir la robustesse des mesures de protection des données et une efficacité constante.
o Encourager la collaboration entre nations africaines pour développer des normes communes et un cadre de réflexion éthique sur la protection des données en santé.

2. Promotion de l'inclusion et de l'équité
o Développer des programmes de télémédecine adaptés aux besoins spécifiques des régions rurales et des communautés à faible revenu.
o Mettre en œuvre des initiatives ciblées pour garantir que les avantages de la santé numérique touchent toutes les populations, en particulier celles des régions rurales et à faible revenu.

3. Assurance d'une mise en œuvre efficace
o Faciliter le partage des meilleures pratiques entre les pays africains.
o Instaurer des mécanismes de suivi et d'évaluation pour ajuster les stratégies en fonction des réalités locales.

4. Renforcement des capacités
o Investir dans la formation des professionnels de la santé pour maximiser les avantages des technologies numériques.
o Investir dans la culture de la littératie numérique au profit de la population, y compris en l'incluant dans les programmes scolaires et autres formations populaires.
o Favoriser la recherche sur l'efficacité et l'impact des solutions numériques dans des contextes divers.

En définitive, la Loi kényane sur la santé numérique de 2023, bien qu'ambitieuse, nécessite une mise en œuvre et une supervision attentive pour maximiser ses avantages tout en atténuant les inconvénients potentiels. Les leçons tirées de cette initiative peuvent servir de guide pour d'autres nations africaines, ouvrant ainsi la voie à une ère de santé publique, soins de santé numériques accessibles, de qualité, et efficaces sur le continent, notamment en Afrique subsaharienne. Au-delà des enjeux technologiques, les aspects relatifs à la soutenabilité et à l'éthique revêtent une importance capitale, possiblement bien plus qu'en Europe ou aux Etats-Unis. Une analyse séparée serait à faire au sujet de l'Afrique septentrionale.
B.G

RETOUR SUR LES LIGNES DIRECTRICES SUR LE CONSENTEMENT DE L'ODPC

Par Thomas HONNET

Le Bureau du Commissaire à la protection des données (ODPC) a adopté fin 2023 ses lignes directrices sur le consentement comme base légale d'un traitement de données à caractère personnel.

Avec le consentement, huit autres bases légales

Les lignes directrices de l'ODPC rappellent le cadre posé par le Data Protection Act (DPA), texte national sur la protection des données à caractère personnel adopté par le Kenya le 11 novembre 2019. On y retrouve huit grands principes qui recouvrent ceux qui sont reconnus par une majorité d'instances internationales comme étant des principes essentiels de la protection des données : droit à la vie privée, principes de légalité, d'équité et de transparence du traitement, de limitation des finalités, de minimisation et d'exactitude des données, de limitation de conservation, d'intégrité et de confidentialité, et d'accountability.
Une des spécificités kényanes réside dans le nombre des bases légales mobilisables par les responsables de traitement - neuf. La rédaction du texte est d'ailleurs intéressante : la Section 30 dispose qu'un « responsable de traitement ne doit pas traiter de données à caractère personnel, sauf si la personne concernée donne son contentement [...] ou si le traitement est nécessaire [aux autres bases légales] ». Le consentement a donc une place particulière ici, en étant distingué clairement des autres bases légales.

Là encore, malgré un nombre important, nous retrouvons dans l'esprit les bases légales partagées par une grande partie des règlementations considérées comme les plus protectrices, notamment le Règlement Général sur la Protection des Données (RGPD européen) : l'exécution d'un contrat ; le respect d'une obligation légale ; la protection d'intérêts vitaux ; la réalisation d'une mission d'intérêt public, ou par une autorité publique ou pour l'exercice, par toute personne dans l'intérêt public de toute autre fonction de nature publique ; un intérêt légitime du responsable de traitement (à mettre en balance avec les droits, libertés et intérêts légitimes de la personne concernée) ou encore la réalisation de recherches historiques, statistiques, journalistiques, littéraires, artistiques ou scientifiques.

Des lignes directrices très classiques, dans l'esprit de celles de l'EDPB européen

L'ODPC, dans ses lignes directrices, finalement assez courtes, rappelle que le consentement ne peut être une base légale appropriée que si la personne concernée a réellement le choix d'accepter ou de refuser le traitement de données, et que ce choix ne doit pas entraîner de conséquences négatives pour elle. Ce point est d'ailleurs une condition du caractère libre du consentement.

Le consentement doit également être donné de manière éclairée, notamment en bénéficiant de certaines informations listées par l'ODPC : l'identité du responsable de traitement et des sous-traitants, les finalités du traitement, le traitement réalisé, et le droit de retirer son consentement.

Sur l'obligation de prouver la collecte du consentement par le responsable du traitement, le DPA ne précise par les différents moyens d'y parvenir. L'ODPC préconise par exemple de tenir un registre de déclaration de consentement, qui contiendrait la date d'obtention de ceux-ci et la liste des informations qui ont été transmises à la personne

© iStock

concernée à ce moment-là.

Aussi, l'obtention du consentement par le responsable de traitement ne soustrait en rien ce dernier de ses autres obligations, issues du DPA. Enfin, il doit également redemander un consentement distinct en cas de changement de finalités (l'ODPC précise qu'il n'y a pas de consentement « évolutif », même en cas de « finalités compatibles »).

Le consentement est le parent pauvre des bases légales… Et c'est tant mieux !

On pense souvent que le consentement est l'alpha et l'oméga d'un traitement de données à caractère personnel, en atteste la rédaction de la Section 30 du DPA kényan évoqué ci-avant. Or, en réalité, le consentement est peu utilisé, au profit d'autres bases légales plus opportunes. En effet, avec les missions d'intérêt public, le respect des obligations légales et l'exécution d'un contrat, nous couvrons déjà un large spectre des traitements de données personnelles. Aussi, le consentement comme base légale porte en lui de nombreuses contraintes, rappelées par les lignes directrices de l'ODPC et par la Section 32 du DPA : il faut en conserver la preuve, il faut pouvoir gérer son retrait, et il faut s'assurer qu'il soit donné de manière libre, éclairée, et spécifique. D'autres bases légales nous semblent donc plus simples à mobiliser. Enfin, l'ODPC inscrit ses lignes directrices dans un cadre relativement classique et protecteur, et participe ainsi au concert des nations protectrices des données personnelles de leurs citoyens.

T.H

© iStock

ALERTE DE CONFORMITÉ SUR LE TRAITEMENT DES DONNÉES PERSONNELLES

Par Patrick NGUETCHOUESSI

© NDPC

Le Nigeria, comme beaucoup de pays africains, s'est saisi des enjeux importants liés à la gouvernance de la donnée. Dans la mise en œuvre de sa stratégie visant à sécuriser son espace numérique et asseoir sa souveraineté digitale sur les 213,4 millions de nigérians, la Loi nigériane sur la protection des données de 2023 (Nigeria Data Protection Act, 2023) est entrée en vigueur le 12 juin 2023. Le texte garantit un cadre juridique formel pour la protection des données et informations personnelles des citoyens, et la pratique de la protection des données dans le pays.

La nouvelle loi établit la Commission nigériane de protection des données (NDPC) qui vient remplacer le Bureau nigérian de protection des données (NDPB). Cette nouvelle entité a pour mission, entre autres, de réglementer et promouvoir le déploiement de mesures technologiques et organisationnelles pour améliorer la protection des données personnelles ; imposer des sanctions pour toute violation des dispositions de la loi ou de la législation subsidiaire qui en découlent ; accréditer, agréer et enregistrer des personnes aptes à fournir des services de conformité en matière de protection des données.

Dans le cadre des directives d'application de cette loi, la commission a émis une notice d'information à destination des responsables de traitement et des sous-traitants pour leur rappeler l'échéance imminente de certaines obligations de conformité.

L'obligation de mettre en place un rapport annuel de conformité

Conformément au Nigeria Data Protection Act (NDP Act) et son texte d'application (General Application and Implementation Directive (GAID)), les responsables de traitement ainsi que les sous-traitants sont soumis à l'obligation de remplir et déposer auprès de l'autorité un rapport annuel d'audit de conformité en matière de protection des données (data protection compliance audit returns (CAR)). Ce rapport est la matérialisation du principe d'accountability, principe fondamental de la loi garantissant une démarche de conformité effective de la part des organismes concernés dans le secteur public comme privé.

Lorsqu'un responsable de traitement atteint le seuil légal de traitement de données de mille (1 000) personnes concernées dans un délai de six (6) mois et deux mille (2 000) personnes concernées dans un délai de douze (12) mois, il est tenu de déposer son rapport d'audit auprès de la commission, conformément à l'article 4.1, paragraphes 6 et 7 de la loi Nigériane. Le délai de dépôt dudit rapport est fixé au 15 Mars 2024 . Le processus de dépôt est facilité par des organismes agréés de conformité à la protection des données (DPCO). Ces organismes sont enregistrés sur une liste tenue par la commission et œuvrent pour leurs clients afin de les accompagner dans leur processus de mise en conformité.

Autres points de vigilance

Formation initiale des délégués à la protection des données (DPO)

Tous les délégués à la protection des données désignés doivent participer à une formation d'initiation qui sera organisée par la Commission en janvier 2024. Cette formation abordera spécifiquement les droits des personnes concernées, ainsi que les diverses obligations de conformité pertinentes pour les responsables de traitement et les sous-traitants, en vertu de la loi et de son décret d'application.

La formation prévue est gratuite et concerne spécifiquement les DPO désignés. Le format n'étant pas précisé, la commission se garde le droit de préciser ces modalités ultérieurement.

La liste blanche de la commission

La commission tient une liste blanche sur laquelle les responsables de traitement et les sous-traitants ayant démontré leur conformité seront inscrits, après réception des audits annuels de conformité.

La liste blanche est un outil de responsabilisation, car elle contient des informations fonctionnelles des responsables du traitement et des sous-traitants. C'est une présomption réfutable qu'un responsable du traitement, ou un sous-traitant figurant sur la liste, s'engage à prendre des mesures techniques et organisationnelles adéquates pour sauvegarder les droits des personnes concernées.

La présence d'un organisme sur cette liste n'emporte donc aucun engagement, certification ou labélisation quelconque de la part de la commission. C'est à l'organisme inscrit que revient l'obligation de mettre en œuvre des mesures de sécurité adéquate, les maintenir et en assurer l'amélioration continue.

Les sanctions de non-conformité

La notice de la commission prévoit également un ensemble de sanctions spécifiques en cas de non-respect des obligations mentionnées, notamment le dépôt du CAR, sur le fondement de la loi nationale de protection des données NDP Act. Les sanctions prévues sont de deux catégories : financières et procédurales ou réputationnelles. Le responsable de traitement ou le sous-traitant devra ainsi :

• Remédier à la violation ;
• Verser une indemnisation à la personne concernée qui a subi une perte ou un préjudice à la suite d'une violation ;
• Rendre compte des bénéfices réalisés grâce à la violation ;
• Payer une pénalité ou des frais de réparation.

P.N

JOURNALISME ET PROTECTION DES DONNÉES PERSONNELLES

Par Arnaud NADINGA

L'examen de la loi du 30 mars 2021, portant sur la protection des personnes à l'égard du traitement des données à caractère personnel, révèle une disposition intéressante.

Il s'agit de l'article 4, qui énumère les traitements qui ne sont pas soumis au régime institué par la loi. Au dernier point de cette disposition, on peut lire : « La présente loi ne s'applique pas aux [...] traitements de données à caractère personnel effectués aux seules fins littéraires et artistiques ou de journalisme, quel que soit le média utilisé, dans le respect des règles déontologiques et éthiques de ces professions, des mesures de sécurité assurant le secret des sources journalistiques, ainsi que des règles de modération applicables aux forums de discussion mis en œuvre par des éditeurs d'informations journalistiques ».

C'est le point concernant le journalisme qui interroge particulièrement, étant donné la quantité d'informations que les journalistes traitent et diffusent. Le texte précise que l'exception concerne tous les médias, y compris les publications sur les réseaux sociaux.

En clair, la disposition écarte tout le régime des traitements de données à caractère personnel issu de la loi du 30 mars 2021 pour le cas des traitements aux fins artistiques ou de journalisme.

Cela est une nouveauté, puisque cette exclusion ne figurait pas dans l'ancienne loi du 20 avril 2004. Chez les voisins, on ne la retrouve pas non plus, que ce soit à l'article 382 du Code béninois du numérique, ou à l'article 3 de la loi sénégalaise portant sur la protection des données à caractère personnel, pour ne citer que ces exemples.

On s'interroge donc sur sa conformité à l'Acte additionnel relatif à la protection des données à caractère personnel de la CEDEAO. Pour rappel, les articles 32 et 33 de cet Acte additionnel autorisent les traitements de données personnelles aux fins de journalisme ou d'expression artistique sous réserve que soient respectées les règles déontologiques de la profession de journaliste professionnel. Le dernier de ces articles est plus précis : « Les dispositions du présent Acte additionnel ne font pas obstacle à l'application des dispositions des lois relatives à la presse écrite ou au secteur de l'audiovisuel et du Code pénal qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes physiques ».

On en déduit que le texte communautaire acte pour une application cumulative de la législation sur les données personnelles et de celle sur la presse écrite, pour préserver les droits des personnes physiques dans le cadre des traitements de données mis en œuvre par des journalistes professionnels. Cela signifie également — et conformément à la recherche d'équilibre entre intérêts divergents qui est de l'essence même de ce droit — que d'une part, le droit des données personnelles ne doit pas empêcher les journalistes d'effectuer leur travail et d'exercer leur liberté d'expression et, d'autre part, que si dans le cadre de cet exercice, ils sont amenés à traiter des données personnelles, ils doivent respecter les règles déontologiques de leur profession et les garanties issues du droit des données personnelles pour les personnes physiques concernées. Ainsi,

pour permettre aux journalistes d'effectuer leur travail, il ne semble pas que l'on ait besoin d'écarter toute la législation sur la protection des données personnelles. Certaines garanties issues de cette législation devraient demeurer applicables. On pense aux principes de licéité (avec l'exigence de base légale qui peut être ici l'information du public), de finalité et de minimisation des données personnelles ou à l'exigence de mesures de sécurité, comme l'anonymisation et la pseudonymisation des données entre autres. En revanche, la particularité de leur mission, qui est l'information du public, pourrait justifier l'exclusion de certaines exigences qui auraient pour effet de limiter ou d'empêcher l'exercice de la liberté d'expression. On pense aux formalités préalables et à certaines obligations d'information ou au régime des flux transfrontaliers de données personnelles.

À titre d'exemple dans ce sens, l'article 3 (2) de la loi nigériane dédiée (Data protection Act, 2023) dispose que les traitements aux fins de journalisme ne sont pas soumis aux obligations figurant dans la partie V du texte (si elles sont incompatibles à ces fins), à l'exception de celles des articles 24 (principes directeurs), 25 (bases légales), 32 (désignation d'un délégué à la protection des données) et 40 (notification des violations de données). Il précise par ailleurs que ces traitements doivent s'effectuer dans le respect des droits et libertés consacrés par la constitution.

Contrairement à cette solution que l'on rencontre un peu partout, l'article 4 de la loi du 30 mars 2021 écarte l'application de celle-ci au profit « des règles déontologiques et éthiques [...], des mesures de sécurité assurant le secret des sources journalistiques, ainsi que des règles de modération applicables aux forums de discussion mis en œuvre par des éditeurs d'informations journalistiques ». Au sujet de ces dernières, on peut relever que la loi n° 057-2015/CNT, portant régime juridique de la presse écrite au Burkina Faso, ne comporte qu'une seule référence sur les données à caractère personnel. Il s'agit de l'article 69, qui ne concerne d'ailleurs que les circonstances dans lesquelles l'accès aux sources d'information peut être refusé au journaliste professionnel : « L'accès aux sources d'information peut être refusé dans le cas où il est de nature à porter atteinte [...] à la vie privée et à la protection des données à caractère personnel ».

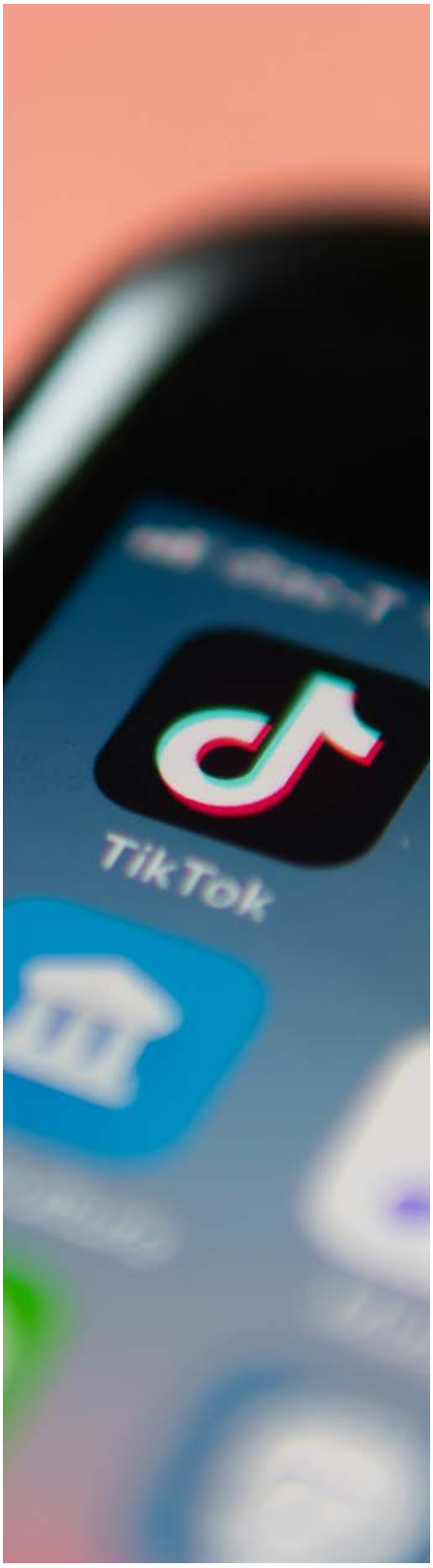
Les autres dispositions ne reprennent que les droits au respect de la vie privée et de l'image. C'est l'exemple de l'article 26 aux termes duquel : « Aucune publication d'information générale, d'opinion ou spécialisée ne peut comporter ni illustration, ni récit, ni information, ni insertion qui porte atteinte au droit à l'image et au droit à la vie privée ». De même, l'article 12 de la Charte du journaliste burkinabè (Observatoire burkinabè des médias, Bobo, 1990) n'évoque expressément que la vie privée : « Le respect du droit des personnes à la vie privée et à la dignité humaine en conformité avec les dispositions nationales et internationales en matière de droit concernant la protection des individus et interdisant la diffamation, la calomnie, l'injure, l'insinuation malveillante fait partie intégrante des normes professionnelles du journaliste burkinabè ».

De ce qui précède, on fait le constat qu'au-delà des formulations trop générales que ces normes comportent, il n'y est point fait référence aux dispositions et garanties relatives à la protection des données personnelles. Or, il est aujourd'hui clair que les traitements de données personnelles ne menacent pas que le droit au respect de la vie privée (traçage, profilage, constitution de casiers judiciaires et discriminations sont également à craindre). La solution n'est donc pas dans l'exclusion des traitements aux fins de journalisme du champ d'application de la loi sur les données personnelles.

A.N

RENCONTRE ENTRE LA CDP ET TIKTOK

Par Yao Justin KOUMAKO



© iStock

Le 6 octobre 2023, l'autorité sénégalaise de protection des données personnelles (Commission des données personnelles, ci-après la « Commission » ou la « CDP ») a organisé une rencontre d'échanges et de discussions avec le staff de la plateforme TikTok. Cette rencontre intervient après une séance de discussion avec le ministère de l'économie numérique et s'inscrit dans le contexte d'interdiction de TikTok dans le pays depuis le 2 août 2023, le gouvernement reprochant à la plateforme le manque de mesures préventives pour protéger la vie privée et les mineurs, ainsi qu'un manque de filtres pour garantir « la sécurité publique et les bonnes mœurs».

Les échanges ont porté sur les dispositions à prendre pour accélérer le traitement des plaintes et signalements relatifs aux contenus de la plateforme. Ils ont amené la Commission et la plateforme à convenir de la mise à en place d'un canal de communication, en l'occurrence via un email (nommé TSET) destiné exclusivement aux demandes urgentes de la Commission. Enfin, un délai de 24 heures a été fixé pour les traitements des demandes adressées à la plateforme par la Commission.

Une rencontre à l'allure d'une exception ?

Pour une autorité de protection des données, dont le rôle est de veiller à ce que les responsables de traitement respectent le cadre légal et de sanctionner en cas de manquements, une rencontre avec TikTok sur fond d'interdiction politique peut paraitre étrange. En général, les rencontres avec les plateformes relèvent de la sphère d'organismes ou de dirigeants politiques. Ainsi, si l'autorité française de protection des données personnelles (la CNIL) dispose d'un service chargé des relations avec le public et répond généralement présente lors de rencontres telles que le Forum International de la Cybersécurité (désormais Forum InCyber) pour discuter avec les acteurs, elle est plus connue pour les sanctions infligées aux plateformes qui manquent à leurs obligations que pour des rencontres d'échanges avec elles.

La question qu'on peut se poser est alors celle-ci : pourquoi une rencontre d'échanges avec TikTok au lieu d'une procédure de sanctions, alors même que la CDP admet faire face à une recrudescence des plaintes liées à la plateforme ?

Une rencontre de pédagogie et d'information

Pour comprendre la rencontre entre TikTok et la Commission, il faut s'intéresser au statut et aux missions de la Commission. Une lecture rapide du décret portant application de la loi sur la protection des données à caractère personnel , qui comporte pourtant un chapitre entier sur la Commission et une section détaillée sur ses attributions ne permet pas d'avancer sur le sujet. La loi sur la protection des données person-

nelles dispose, elle, en son article 5 que la Commission « informe les personnes concernées et les responsables de traitement de leurs droits et obligations et s'assure que les TIC ne comportent pas de menace au regard des libertés publiques et de la vie privée». L'article 16 §2 de la même loi reprend les mêmes dispositions mais ne mentionne pas de telles rencontres dans les alinéas qui détaillent les actions liées à la mission d'information qui incombe à la Commission. Au demeurant, cette rencontre pourrait s'inscrire dans cette mission d'information prévue à l'article 5 précité. Ainsi, on peut considérer que la Commission exerce sa mission d'information envers la plateforme afin de la situer sur ses obligations légales. Une telle rencontre permet également d'établir le cadre de collaboration nécessaire et préalable à toutes formes de procédures de sanctions.

L'information est au cœur de la protection des données, qu'elle soit destinée aux personnes concernées (droit à l'information) ou aux responsables de traitement et aux professionnels. L'obligation de clarté et d'accessibilité de l'information, prévue en général par les lois sur la protection des données personnelles, ne peut se faire sans pédagogie et sans cadre de discussions. L'action de la CDP fait écho à cette nécessité.

J.Y.K

© CDP

© CDP

LA CNDP ET 11 AUTORITÉS DANS LE MONDE INTERPELLENT LES GÉANTS DU WEB SUR LE DATA SCRAPING

Par Maha TAZI

© iStock

Avec près des deux tiers (64 %) de la population mondiale désormais connectée à Internet, nous nous retrouvons inévitablemment à partager des informations de nature de plus en plus personnelle sur diverses plateformes telles que les réseaux sociaux, les blogs, les sites de vente, et même en répondant à des offres d'emploi.
Cette digitalisation aiguë apporte indubitablement des avantages que nous connaissons bien, mais elle suscite également diverses inquiétudes. En diffusant nos empreintes digitales sur plusieurs plateformes au sein d'un réseau souvent décrit comme incontrôlable, nous exposons nos données, devenues la monnaie courante de notre époque, à des acteurs extérieurs aux motivations variées. Ces parties tierces peuvent avoir des intérêts commerciaux légitimes, le pouvoir et le choix de prise de décision ou, de manière plus inquiétante, des desseins malhonnêtes tels que la vente sur le dark web ou l'utilisation à des fins de personnification dans des attaques de social engineering.

Cet état de vulnérabilité est exacerbé par le data scraping, une pratique d'extraction massive de données en ligne, qui mine progressivement cette protection jadis préservée.

Le Data Scraping Décrypté

Qu'est-ce que le Data Scraping ?

Le data scraping est une technique ingénieuse visant à extraire de vastes quantités d'informations disponibles en ligne. Cette pratique repose sur l'utilisation de programmes automatisés, appelés "bots" ou "spiders", qui naviguent à travers divers sites web pour collecter

des données spécifiques. II faut les imaginer comme des explorateurs numériques, scrutant les pages web à la recherche d'informations précieuses.
Le processus commence généralement par l'identification des sources de données ciblées. Les bots parcourent ensuite ces sources en utilisant des algorithmes pour extraire des données, structurées ou non structurées, selon les besoins. Cette méthode est utilisée pour récupérer des informations telles que les prix des produits, les évaluations des utilisateurs, les coordonnées, ou tout autre contenu disponible en ligne.

Pourquoi le Data Scraping nous concerne tous?

Cette technique, apparemment inoffensive d'exploration des données en ligne, cache en réalité une myriade de risques qui touchent chacun d'entre nous au cœur de notre expérience numérique.

Il faut imaginer ceci : en parcourant des sites web à la recherche de nouvelles chaussures, soudainement, sans même nous en rendre compte, notre comportement de navigation est capturé et analysé à des fins de profilage. C'est là que réside le premier risque majeur du data scraping : le profilage abusif.

En effet, cette pratique peut être utilisée pour créer des portraits détaillés de chaque utilisateur, révélant leurs préférences, habitudes de consommation, et même leurs opinions politiques. Il est surprenant de constater à quel point ces données, a priori anodines, peuvent être exploitées, par exemple, pour cibler des publicités spécifiques

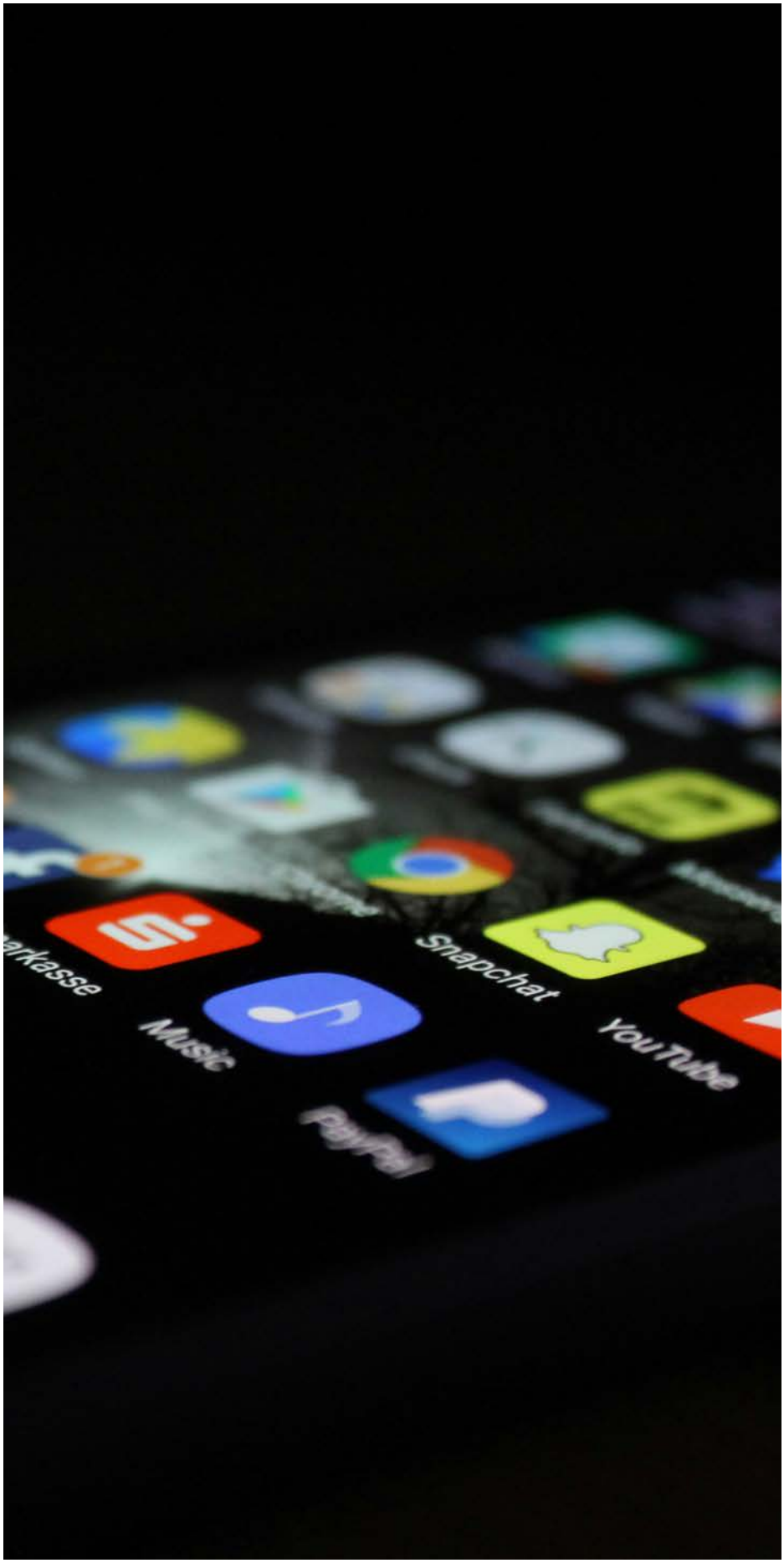
© Unsplash

ou influencer nos choix. Pire encore, le data scraping peut ouvrir la porte à l'usurpation d'identité. En collectant des informations telles que le nom, l'adresse, et l'historique d'achat, les malfaiteurs peuvent créer un portrait virtuel de chacun de nous, avec des conséquences désastreuses. Quelqu'un pourrait utiliser une identité usurpée pour effectuer des achats frauduleux ou même commettre des actes illégaux de manière dissimulée. C'est un scénario qui pourrait sembler être tiré d'un film, mais malheureusement, c'est une réalité qui peut découler du data scraping non réglementé.

En somme, le data scraping n'est pas simplement une question technique réservée aux experts en informatique. C'est une réalité quotidienne qui peut impacter chacun d'entre nous de manière directe. Il est temps de prendre conscience de ces risques, de défendre notre droit à la vie privée, et de demander des mesures réglementaires solides pour encadrer cette pratique omniprésente qui façonne notre expérience en ligne.

Au Maroc, une Commission Nationale pour défendre les données personnelles

Au Maroc, la Commission Nationale de Contrôle de la Protection des Données Personnelles (CNDP) incarne un rempart déterminé pour préserver les droits fondamentaux et les libertés des individus face aux traitements de données à caractère personnel. La loi marocaine 09-08 du 18 février 2009 lui confère une mission cruciale.



© Unsplash

La CNDP, une tête de pont dans la défense collective de la vie privée dans l'ère numérique

Dans la continuité de ses initiatives locales, en collaboration avec onze autorités de protection des données à travers le monde, la CNDP prend la tête d'une initiative majeure. Dans une lettre conjointe publiée le 24 août 2023, intitulée "Data scraping et la protection de la vie privée", la CNDP et ses homologues internationaux émettent un appel unanime aux GAMMAs, les géants du web, pour atténuer les risques associés au data scraping.

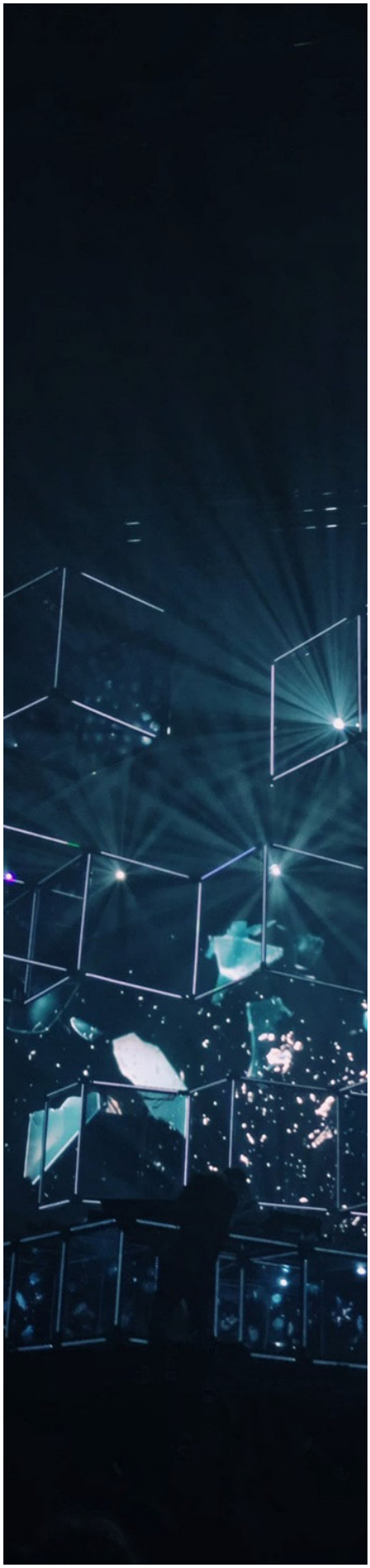
Cette correspondance n'est pas simplement une missive formelle, mais un cri d'alerte concerté. Elle souligne trois objectifs essentiels : premièrement, alerter sur les risques majeurs en matière de protection de la vie privée liés au data scraping; deuxièmement, inciter les médias sociaux et les autres sites web à renforcer leurs défenses pour se conformer aux réglementations en vigueur ; enfin, appeler ces organisations à prendre des mesures concrètes pour réduire les risques d'atteinte à la vie privée liés à cette pratique.

Cette lettre s'adresse directement à des acteurs clés tels qu'Alphabet Inc. (YouTube), ByteDance Ltd (TikTok), Meta, Inc. (Instagram, Facebook et Threads), Microsoft Corporation (LinkedIn), Sina Corp (Weibo), et X Corp. (Twitter). Elle vise également les individus utilisant ces plateformes pour partager leurs données personnelles.

L'initiative conjointe s'étend au-delà des frontières nationales, reflétant la collaboration de la CNDP avec les autorités de protection des données de l'Australie, du Canada, du Royaume-Uni, de Hong Kong, de la Suisse, de la Norvège, de la Nouvelle-Zélande, de la Colombie, de Jersey, de l'Argentine et du Mexique.
En unissant leurs forces, ces autorités tracent la voie vers une protection mondiale des données, marquant un appel international à l'action. La lettre conjointe représente ainsi une étape cruciale vers la défense collective de la vie privée dans l'ère numérique en constante évolution.

Nous sommes tous responsables : protéger notre vie privée dans le monde numérique

À l'ère numérique, la préservation de notre vie privée devient essentielle. Notre exploration du data scraping met en lumière les risques qui accompagnent notre présence en ligne. La CNDP se positionne comme une force protectrice au Maroc, mais la responsabilité de la vie privée ne repose pas uniquement sur les épaules des organismes de régulation. Chacun de nous doit être conscient de ce qu'il partage en ligne, comprendre les implications de ses actions numériques et exiger des pratiques responsables des plateformes.
M.T



© Unsplash

CYBERATTAQUE SUR LA CHAINE DE SUPERMARCHÉS NAIVAS

Par Patrick NGUETCHOUESSI

La sécurité informatique repose sur la garantie de l'intégrité, de la disponibilité et de la confidentialité de l'infrastructure concernée. Le but ultime est de protéger toutes les données en transit ou au repos sur le système. L'universalité reconnue à l'exigence de sécurité justifie son intégration au cœur du corpus réglementaire relatif à la protection des données à caractère personnel. Au Kenya, cette obligation de sécurité, bien qu'étant renforcée sous les auspices du Data Protection Act, reste d'actualité pour les organismes du secteur privé. Ce constat est au cœur de l'affaire Naivas Supermarket, entreprise Kenyane victime d'une violation de données.

Focus sur la cible de la violation de données

"Naivas Supermarket" souvent appelée « Naivas », est la plus grande chaîne de supermarchés au Kenya, avec 84 points de vente en juin 2022, devant Quick Mart Limited avec 51 points de vente . Le siège social, ainsi que les entrepôts de l'entreprise, sont situés dans le parc d'affaires Sameer, dans la zone industrielle de Nairobi, la capitale du pays. Naivas Limited a été enregistrée le 24 juillet 1990 , elle opérait auparavant sous le nom de Rongai Self Service Stores Limited.

L'attaque par ransomware

La chaîne de supermarchés Naivas a annoncé avoir été ciblée par une cyberattaque de type ransomware le dimanche 23 avril 2023. Son directeur commercial, Willy Kimani, a confirmé l'attaque et a déclaré que les données des systèmes de Naivas ne contenaient pas les détails bancaires des utilisateurs/clients. Le supermarché a alors pris des mesures immédiates pour empêcher l'accès externe et a engagé des experts en cybersécurité de chez CrowdStrike pour assurer l'intégrité de son système.

"À l'heure actuelle, nous ne sommes pas conscients de l'utilisation malveillante des données volées. Cependant, il est recommandé [aux clients] , face à ce type de situation, de prêter une attention particulière à toute tentative de phishing (par téléphone, SMS ou e-mail) ainsi qu'à la sécurité suffisante des mots de passe", a noté Kimani. Il assure par ailleurs que les informations de paiement sont traitées de manière sécurisée et protégées par chiffrement SSL. Cela fait suite aux rapports d'attaques de Ransomware Medusa sur KAA et Jubilee Insurance.

Non-respect du délai légal de signalement

L'article 43.1 du Data Protection Act, relatif à la notification des violations de données, précise: "Lorsque des données personnelles ont été consultées ou acquises par une personne non autorisée et qu'il existe un risque réel de préjudice pour la personne concernée dont les

© Unsplash

données personnelles ont été soumises à un accès non autorisé, un responsable du traitement doit :

(a) informer le commissaire aux données sans délai, qui doit dans les soixante-douze heures prendre connaissance d'une telle violation ; et

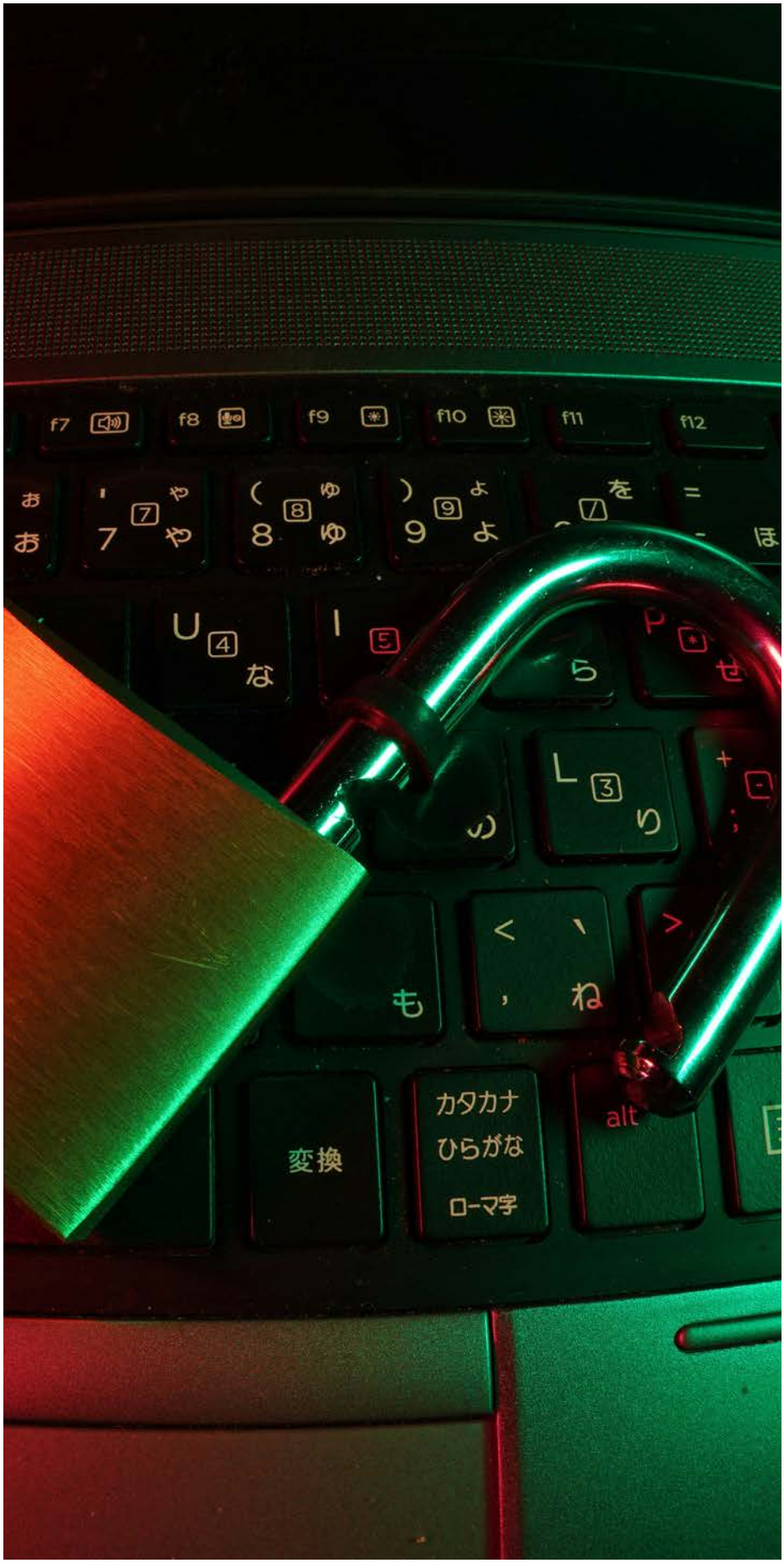
(b) sous réserve du paragraphe (3), communiquer par écrit à la personne concernée dans un délai raisonnablement pratique, à moins que l'identité du sujet des données ne puisse être établie. "

La déclaration effectuée par Naivas étant intervenue au-delà du délai de 72 heures mentionné au point (a), la commission sénatoriale des TIC du Kenya a donc ouvert une enquête sur la chaîne pour avoir omis de signaler la violation de données.

Le Bureau du commissaire à la protection des données (ODPC) a également lancé un audit et une inspection pour vérifier la responsabilité de Naivas et l'impact de la violation des données sur les droits et libertés des personnes concernées. Les conclusions sont très attendues, tout comme les résultats de l'audit de 40 autres entreprises par l'ODPC.

Le législateur a également demandé au comité d'établir le degré de culpabilité de Naivas dans la violation de données et de décrire les mesures spécifiques prises par le Bureau du commissaire à la protection des données (ODPC) pour demander des comptes à la chaîne de supermarchés.

P.N



© Unsplash

WWW.AFRICADATAPROTECTION.ORG
INFO@AFRICADATAPROTECTION.ORG