AFRICA DATA PROTECTION

REPORT

NIGERIA FINES META A RECORD $220 MILLION: ANALYSIS OF A HISTORIC SANCTION!
PAGE 7

HEALTH DATA IN SUB-SAHARAN AFRICA: CHALLENGES, RISKS, AND OPPORTUNITIES
PAGE 10

DEC. 2024

EDITORIAL: HARMONIZATION OF PERSONAL DATA FRAMEWORKS IN AFRICA: FROM CONTINENTAL STRATEGY TO SUBREGIONAL INITIATIVES
PAGE 5

AFRICA DATA PROTECTION

Contents

FOREWORD

Jules Hervé YIMEUMI
President of Africa Data Protection association

These last few months, personal data protection in Africa has seen significant progress, reflecting the growing awareness among governments and local institutions of the importance of ensuring the security and privacy of citizens' data.

In Ethiopia, the entry into force of the new data protection law marks a significant turning point, positioning the country among the ones committed to defending individuals' rights in the face of information technology usage.

In Botswana, the publication of a bill aimed at replacing the existing data protection legislation reflects a desire to adapt to the rapid changes in the global digital environment.
In Cameroon, a bill on the protection of personal data has been presented to Parliament, reflecting a similar drive to regulate digital practices.

Furthermore, the recent fine imposed on Meta in Nigeria highlights an increasing vigilance from the African regulators toward tech giants and underscores the importance of ensuring responsible handling of personal data by multinational companies.
Lastly, in Benin, the Personal Data Protection Authority (APDP in French) has recently clarified the requirements for certifying the qualifications of Data Protection Officers (DPOs). This emphasises the need for specific skills and qualifications for professionals in this field.

These recent measures demonstrate the coordinated effort of many African countries to develop a robust and effective personal data protection framework, in line with growing concerns around digital rights and digital sovereignty on the continent.

AWARDS

CALL FOR PAPERS OPEN TO STUDENTS, RESEARCHERS, PROFESSIONALS, ACADEMICS, ENTREPRENEURS, ETC., DISTINGUISHED BY THEIR INNOVATIVE WORK ON THE ISSUES OF ARTIFICIAL INTELLIGENCE OR PERSONAL DATA IN AFRICA

SUBMISSION DEADLINE: JANUARY 13, 2025

FURTHER INFORMATION: WWW.AFRICADATAPROTECTION.ORG

EDITO

HARMONIZATION OF PERSONAL DATA FRAMEWORKS IN AFRICA: FROM CONTINENTAL STRATEGY TO SUBREGIONAL INITIATIVES

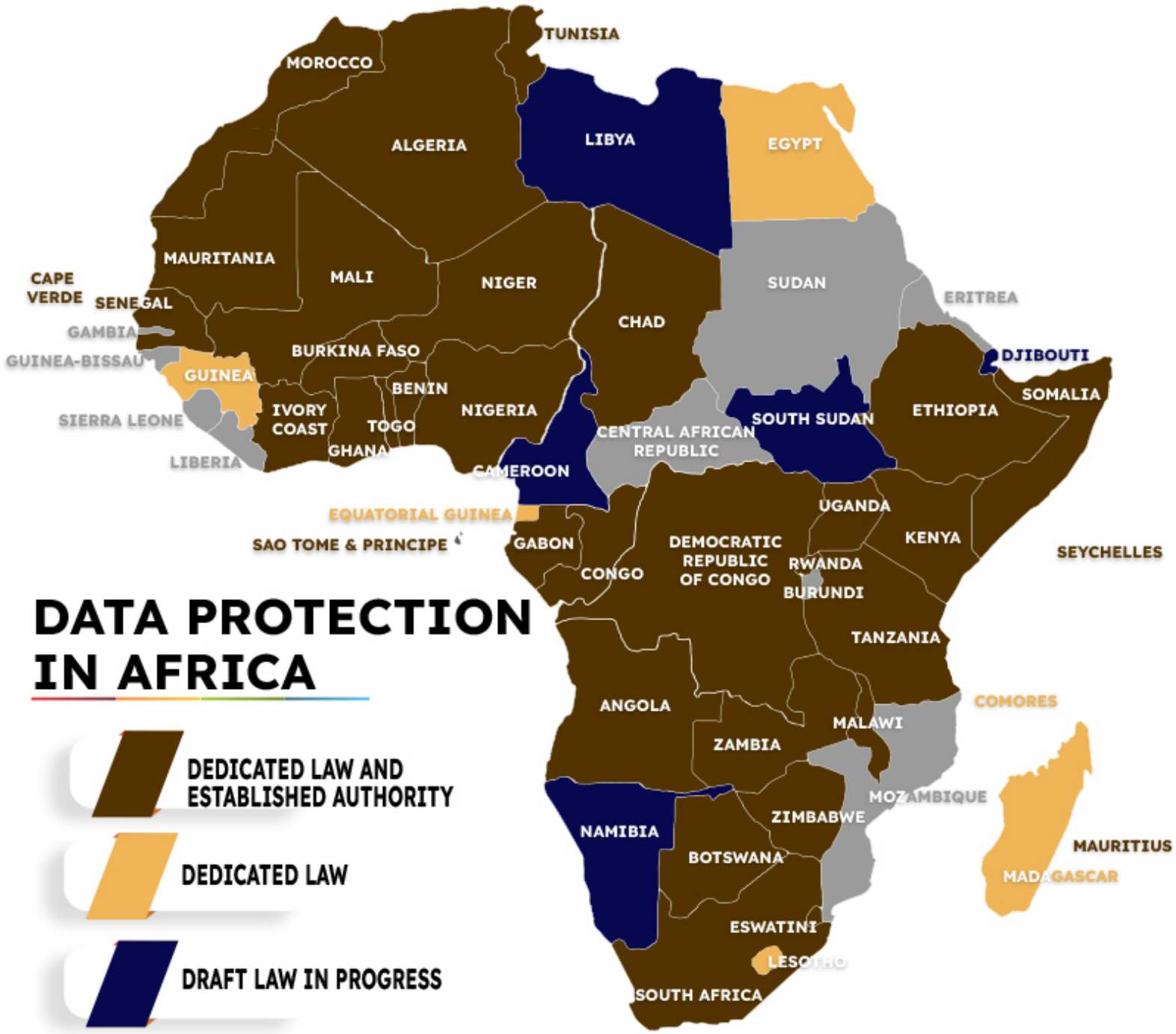
By Winnie Franck DONGBOU
Senior Data Protection Lawyer & PhD Candidate in Health Data Governance

On July 28, 2022, the African Union (AU) unveiled its data governance policy through a strategic guide aimed at African states. This document aims to harmonize data governance policies across the continent and facilitate the smooth flow of data exchanges in order to build trust in digital systems.

In order to achieve this, the AU makes several recommendations emphasizing the importance of protecting personal data and facilitating its transfer across the continent. For example, it recommends that member states « cooperate to allow data to flow across the continent while maintaining human rights, data protection, security, and the fair sharing of benefits. » Recognizing the need to involve regional economic communities (RECs), the AU also makes recommendations to encourage the creation of « a common framework for categorizing and sharing data that takes into account major types of data and associated levels of confidentiality and security. »
Therefore, it is rightly that the AU encourages collaboration of its member states with national data protection authorities, including the African Network of Data Protection Authorities.

These AU recommendations reflect the initiatives of the Economic Community of West African States (ECOWAS) and the East African Community (EAC). In fact, from October 16th to 18th, of 2024 , Rwanda hosted 70 delegates representing the 8 EAC member states to promote the harmonization of regional data governance frameworks and strengthen legal cooperation in data protection. On this occasion, Immaculate Kassait, the Kenyan Data Protection Commissioner, highlighted that harmonizing data protection laws across Africa will allow national authorities to adopt a coherent and coordinated approach to managing data protection disputes, particularly when they involve multinational companies.

The ECOWAS Commission, for its part, organized a workshop in Nigeria focused on revising the Additional Act on Personal Data Protection and strengthening capacities for harmonizing protection frameworks and cross-border data flows. From a draft of approximately eighty pages, ECOWAS aims to eliminate barriers to the free transfer of data between its member states while setting common conditions for data transfers outside the region.
These regional initiatives undoubtedly represent part of the broader goal of continental harmonization, which will need to be coordinated and aligned. In the absence of full harmonization, the interoperability of regional legal frameworks will be the cornerstone of effective data governance in Africa. **W.F.D**



Source : blog.africadataprotection.org/en/legislation

NIGERIA FINES META (FORMERLY FACEBOOK) A RECORD $220 MILLION: ANALYSIS OF A HISTORIC SANCTION!

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

Both institutional and individual actions in favor of better privacy protection are multiplying across the continent. Africa, long considered a "regulatory desert" in this area, is now witnessing major steps forward. Nigeria did not wait for the entry into force of its latest data protection law in 2023 to begin scrutinizing Meta's (formerly Facebook) activities within its territory.

What's the issue?

On July 19th 2024, the Federal Competition and Consumer Protection Commission (FCCPC) imposed a record fine of $220 million on Meta. This is one of the heaviest penalties ever levied in Africa against a tech giant and marks the beginning of a showdown between Nigeria and Meta. One of the key aspects of this case is the strong collaboration between the FCCPC and the Nigerian Data Protection Commission (NDPC), a first in Africa. The FCCPC's stated goal was clear: to demonstrate how data protection issues can be leveraged to address consumer protection concerns and competition matters. To simplify the understanding of this case, both entities will be referred to as the "Commission."

The starting point of this case was the update to WhatsApp's privacy policy on May 15th, 2021. WhatsApp, a subsidiary of Meta, was the subject of the complaint. For clarity, no distinction will be made between WhatsApp and its parent company, Meta, as the sanction applies equally to both. The privacy policy is the legal document that explains to users what data is processed by a company, the forms of processing, and its impact on users. It specifies the security measures put in place to protect user privacy. However, the recent changes to WhatsApp's policy sparked a wave of reactions in Nigeria. According to the Commission, these policies were imposed on consumers and violated the fairness rules governing data process-

ing. This led to a preliminary investigation into Meta for potential violations of the Federal Competition and Consumer Protection Act (FCCPA) and Nigeria's Data Protection Regulation (NDPR), which has now been replaced by the Nigerian Data Protection Act (NDPA) of 2023.

The Process and Meta's Response

Following these events, a preliminary investigation was launched by the Commission to assess the voluntary nature of the users' acceptance of the updated privacy policies. On June 10, 2021, Meta was issued a justification order (OSC) in accordance with the FCCPC's mandate under Section 17 of the FCCPA, to present its defense. Meta's responses during interactions with the authorities in the 38 months of proceedings centered around the claim that "the Commission's regulatory intervention was unjustified and based on a misunderstanding of the objective and impact of its privacy policy," despite the detailed evidence provided by the Commission. This lengthy procedure highlights the complexity of the case, as the Nigerian authorities accused Meta of both competition-related violations and data protection breaches, including: disregarding the right to self-determination, unauthorized data transfer and sharing, discriminatory treatment of data, abuse of dominant position, and tied selling of products and services.

What Does Nigerian Regulation Say?

Under Section 1.2, the regulation applies to "individuals residing in Nigeria or outside Nigeria who are Nigerian citizens." In this case, WhatsApp, an instant messaging service, uses data from Nigerian users through their contacts to provide services. In addition to the information shared by users, WhatsApp collects data on user activity and habits. This activity is thus subject to the regulation, as it meets the criteria outlined in Section 1.2. However, the regulation's scope remains unclear, especially regarding territorial aspects. It does not specify whether the data controller or processor must be located in Nigeria, which could potentially lead to regulatory violations. However, the NDPA offers clearer protection and clarifies the framework. Its scope includes targeting criteria, emphasizing the offering of goods and services to individuals, regardless of the location of the data controller.

The right to self-determination implies adherence to the general principles of data processing, namely legality, consent, transparency, and clarity in privacy policies. These principles are outlined in Sections 2.1, 2.2, 2.3, 2.5, and 3.1 of the regulation. According to these principles, all processing must be lawful and transparent, requiring the consent of the data subject. The regulation notably provides clear conditions regarding consent, making it a fundamental requirement in data processing activities. Consent must be free, informed, and unequivocal. According to the Commission's findings, WhatsApp's data processing lacked the necessary elements of free, informed, and unequivocal consent. The privacy policy updates were introduced in a manner that did not respect this principle. The policies were opaque and did not allow consumers to provide free and informed consent, constituting an abuse of process by WhatsApp.

In addition to recognizing the fundamental principles of data processing, the regulation organizes data transfers under the joint supervision of the Federal Attorney General (HAGF) and the National Information Technology Development Agency (NITDA) under Sections 2.11 and 2.12. Several conditions are specified, particularly for transfers to countries deemed adequate. In November 2020, NITDA published a "whitelist" of countries deemed adequate for safe data transfers, including EU countries, Singapore, and the USA. WhatsApp might have argued that its data transfers to these countries were legitimate based on this list. However, the key issue here is how the data was collected in the first place. The failure to obtain informed consent rendered these transfers illegal. No data transfer can occur without the individuals' knowledge and consent, which was not the case with WhatsApp's practices. The Commission ruled that the transfers were therefore illegal.

A unique argument in this case is the disparate treatment of Nigerian and European consumers' data, despite a similar regulatory framework. The Commission's report and evidence from WhatsApp showed that the company did not treat Nigerian users the same way as EU users. This "discrimination" was easily verifiable on WhatsApp's website. This disparity might be explained by local regulatory specifics and the strictness of the General Data Protection Regulation (GDPR) in Europe regarding data protection. While there are similarities in general principles and individual rights, it's important to note that

European and Nigerian laws are not identical. Several factors, as outlined in Article 45 of the GDPR, need to be considered, including the rule of law, human rights, relevant legislation, and the recourse available to data subjects. Additionally, Nigeria is not yet deemed an adequate country by the European Commission. Will Nigeria's new 2023 law allow it to qualify as a candidate for the EU's list of adequate countries? Given the recent regulatory and institutional developments, this is a real possibility.

Regarding violations related to competition law, they involve abuse of dominant position and tied sales. Based on Section 70 of the FCCPA, the Commission's investigation revealed that WhatsApp was in a dominant position and abused it. WhatsApp's market power in Nigeria is estimated at 93%. The abuse stems from the imbalance created for consumers, as WhatsApp did not respect their right to self-determination in data processing and denied their consent for data usage. WhatsApp argued that it had substantial competitors, but the Commission found that the evidence provided was insufficient to refute the allegations.

Section 72, 2, d, iii of the FCCPA prohibits practices akin to tied sales. In this case, WhatsApp shared data with Facebook or other partners for profiling and marketing purposes, without allowing consumers to opt out. During data collection, WhatsApp did not inform users about this sharing. The Commission concluded that this diversion from the original purpose, which did not benefit Nigerian users, constituted tied selling.

This analysis reveals that WhatsApp's practices harmed Nigerian consumers. According to the principle of self-determination in data processing, data controllers must ensure that processing does not harm the individuals concerned. The Commission justified its sanction by asserting that the imposition of privacy policies on users caused harm to them. The FCCPC's approach is similar to that of European regulators, seeking to force Meta to comply with the law through hefty financial penalties due to the lack of consent. While this is a historic first fine in Africa, Nigerian authorities have sent a strong message to tech giants: respect for the fundamental rights of Africans remains a priority. The long-sought digital sovereignty is not a utopia. However, the key question remains: can Nigeria alone achieve this goal? Could competition-based data protection offer a solid new approach to privacy protection in Africa? **F.A**

HEALTH DATA IN SUB-SAHARAN AFRICA: CHALLENGES, RISKS, AND OPPORTUNITIES

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

© iStock

Sub-Saharan Africa (SSA) bears a heavy health burden, accounting for 20% of global diseases, while having only 1% of the world's scientists and an alarming ratio of 20 doctors per 100,000 people. This critical shortage of human and material resources is magnified by the concentration of services in urban areas, leaving rural populations in precarious health conditions. SSA also faces a double epidemiological transition.

While communicable diseases like HIV/AIDS, malaria, and tuberculosis continue to devastate the region, there is also a rapid rise in non-communicable diseases, such as diabetes and cardiovascular diseases. This dual challenge requires a reassessment of public health priorities and a more strategic allocation of resources. In this context, health data is essential for targeted planning and effective interventions, helping to overcome some of these inequalities.

Health data comes from multiple sources, ranging from healthcare professionals' notes to complex genetic databases, from simple medical records (more or less structured) to medico-administrative data.

According to the definition in the European General Data Protection Regulation (GDPR), health data includes any information related to the physical or mental health of an individual, whether collected directly (via medical records) or indirectly (via connected devices).

In Kenya's Digital Health Bill, health data refers to information about the physical or mental state of the individual, including past, present, or future health records, data collected during health service provision, or data linking the individual to specific health services. Unfortunately, there remains persistent inefficiency in data management. Many health systems still rely on paper documents, slowing diagnostic processes and hindering rapid decision-making, especially during crises.

With the rise of digital tools and artificial intelligence (AI), health data has become a key driver in improving epidemiological surveillance, personalizing healthcare, and optimizing the allocation and use of limited resources. Some innovative programs are already operational, especially in English-speaking SSA countries such as Tanzania, Kenya, and Nigeria.
However, these innovations, while promising, also come with major challenges, particularly in terms of personal data protection and equitable access to technology. Furthermore, substantial progress is still needed in French-speaking SSA countries in terms of processing and leveraging health data.

Opportunities Offered by Digitalization: Functional Examples in English-speaking Sub-Saharan Africa

The digital transformation of health systems in SSA offers a promising solution to the region's structural and epidemiological challenges. Digital health data has become a strategic resource for improving system efficiency while enhancing access to and quality of care. These digital tools have already started to transform key areas.

In Tanzania, for instance, the "Wazazi Nipendeni" initiative demonstrates how simple technologies like SMS can have a significant impact. This program uses personalized messages to provide essential information about prenatal care, nutrition, and vaccinations to mothers and families. As a result, there has been a significant increase in prenatal consultations and vaccination rates, contributing to better maternal and child health.

In Kenya, hospitals such as the Kenyatta National Hospital have adopted electronic medical records (EMR), simplifying patient information management. These systems improve communication among healthcare professionals, reduce medical errors, and ensure better continuity of care. At the same time, more sophisticated tools, such as AI-assisted analysis, are being used to identify complex conditions. For example, blood smear images analyzed by algorithms allow for more accurate detection of malaria, speeding up diagnoses in areas where specialists are scarce.

In Nigeria, the SORMAS system illustrates how digital data can enhance responses to health crises. Initially designed for tracking infectious

© iStock

diseases, the system was rapidly adapted to manage responses to COVID-19, expanding its coverage to all 36 states in record time. This flexibility highlights the potential of digital solutions to respond quickly to ever-changing public health needs.

These examples show that digitalization can make health systems not only more efficient but also more resilient in the face of crises, by reducing reaction times and improving coordination among actors. However, to fully realize these opportunities, efforts must be made to ensure wide-scale adoption and the development of appropriate infrastructure.

Risks and Challenges Associated with Health Data

Despite their immense potential, digital health data presents significant risks that must be anticipated and managed. One of the main challenges is the vulnerability of this data to cyberattacks and security breaches. Without robust safeguards, health systems can become targets for malicious actors, exposing sensitive information and undermining public trust.

Another major concern is the risk of re-identification. Even when data is anonymized, advances in AI can sometimes enable the cross-referencing of data and the identification of individuals. This raises concerns not only about patient confidentiality but also about the social or economic consequences that could result from the disclosure of this information.

Furthermore, the ethical issue of informed consent remains critical. Many digital health platforms collect and use data without users being fully aware of its purpose. To address this challenge, some projects are adopting dynamic consent models, allowing individuals to adjust their consent at any time. This approach promotes greater transparency and strengthens public trust.

Lastly, unequal access to digital tools presents another obstacle. In rural areas or among marginalized populations, lack of connectivity or digital literacy prevents equitable adoption of these technologies. It is essential that health systems work to include these populations to avoid exacerbating existing inequalities.

To harness the full potential of health data, it is essential to establish ethical and secure governance frameworks that protect individuals while allowing for the effective use of data for the common good.

Recommendations to Maximize the Benefits of Health Data Digitalization

For SSA to fully benefit from health data while minimizing risks, coordinated actions are required. Harmonizing national and regional policies is a key first step. For example, adopting frameworks like the model law on health data governance can provide a common basis to ensure that data collection, storage, and use adhere to ethical principles and security standards. These policies should integrate mechanisms for transparency, consent, and oversight that inspire trust among populations.

The second pillar is the development of local skills. Training experts in health data management and analysis, coupled with investments in robust infrastructures, is essential in order to ensure the autonomy and sovereignty of African health systems. Without this, reliance on imported solutions could stifle local innovation and increase long-term costs.

Finally, it is crucial to focus on solutions tailored to the needs and contexts of populations. Digital tools should be designed with a user-centered approach, integrating feedback from both patients and healthcare professionals. Additionally, partnerships between governments, private companies, and international organizations can help mobilize the resources necessary to accelerate the adoption of digital technologies.

In the long run, these efforts should aim to establish equity in access to healthcare, strengthen the resilience of health systems, and turn structural challenges into sustainable opportunities. Health data is not just a technical tool; it is at the heart of transforming health systems for a more just and inclusive future.

In conclusion, to maximize the benefits of health data while minimizing risks, it is essential to implement harmonized policies and suitable infrastructures. Priority actions should include:

1. **Regional Harmonization**: Adopting common

frameworks like the model law on health data governance to ensure ethical and secure data management.

2. **Development of Local Skills**: Training health data experts and promoting local innovation to avoid dependency on foreign solutions.

3. **Investment in Infrastructure**: Modernizing health systems with robust, interoperable tools tailored to local contexts.

4. **User-Centered Approaches**: Designing solutions that meet the needs of populations and ensuring their active involvement in decisions related to their data. **B.C.G**

© iStock

NIGER DATA PROTECTION AUTHORITY PUBLISHES ITS 2023 ANNUAL REPORT: KEY TAKEAWAYS

By Mahadi MAIFADA MAGOUDANI, PhD in digital law

Since July 2023, Niger has undergone significant political changes that have influenced the priorities of national institutions, including the High Authority for the Protection of Personal Data (HAPDP). In this context, the Authority has demonstrated its ability to adapt its activities to meet current needs while maintaining a regulatory approach aligned with international standards.

Law No. 2022-59, regarded as one of the most comprehensive legal frameworks in Francophone West Africa, has strengthened the tools and missions of the HAPDP. This activity report provides an opportunity to assess the initial steps of its implementation and outline the path toward a more robust regulatory framework in the future.

Regulatory Actions of the HAPDP

The 2023 report introduces an innovative section dedicated to "audit missions," symbolizing the HAPDP's commitment to ensuring compliance with legal requirements. Two types of audits are highlighted:

- **Audit by Hearing**, focused on reviewing files in sectors such as telecommunications, banking, and NGOs. These audits provide an opportunity to ensure administrative compliance while assisting data controllers in regularizing their practices.

- **On-Site Audits,** which concentrated on various sectors (health, insurance, transport, telecommunications, NGOs). This type of audit has led to useful recommendations, emphasizing the HAPDP's constructive approach to raising awareness and continuously improving the practices of the relevant stakeholders.

Recommendations and Formal Notices

With 30 formal notices issued in 2023, the HAPDP

© iStock

demonstrates its commitment to promoting adherence to the current legislation. While the report does not provide detailed results of these actions, this reflects the evolving nature of the institution, which continues to refine its tools for greater transparency in the future.

The operations register introduction through Law No. 2022-59 is a significant advancement that sets Niger's legislation apart in the region. As a key compliance tool, this register could become a cornerstone for future inspections and audits. In a spirit of support, the HAPDP could strengthen its role by providing standardized templates and offering tailored training to facilitate the adoption of this tool by data controllers.
Although its implementation is still ongoing, this step underscores the modernity and ambition of Niger's legal framework, offering promising long-term prospects.

Perspectives and Recommendations

In the current security and political context, the HAPDP plays a strategic role in Niger's digital sovereignty. For example, its involvement in managing sensitive data, such as information related to individuals and entities associated with terrorism, could strengthen its position as a key player in personal data protection.
The following recommendations could help enhance its effectiveness:
- **Increased Transparency**: Providing more detailed information on the actions undertaken in future reports.
- **Support for Stakeholders**: Strengthening practical and educational tools, particularly for the operations register.
- **Capacity Building**: Ongoing training for teams to address technological and security challenges.

The HAPDP's report highlights the solid foundation laid to strengthen personal data regulation in Niger. In an evolving context, the Authority has demonstrated its adaptability and commitment to data protection. With an innovative legal framework and a progressive approach to compliance, the HAPDP is well-positioned to become a key player in national digital sovereignty, while gaining the trust of citizens and economic partners. This positive momentum will help establish Niger as a model for data protection in West Africa. **M.M.M**

© iStock

ARPTIC/ARPTC ASSUMES MISSIONS OF THE DATA PROTECTION AUTHORITY IN THE DRC

By Brozeck KANDOLO, PhD Candidate in digital law

© iStock

The year 2023 marks a significant milestone for the legal framework of digital technologies in the Democratic Republic of the Congo (DRC) with the enactment of Ordinance-Law No. 23/010 of March 13, 2023, which introduces the Digital Code. This ambitious legislation reflects a desire to modernize and enhance the regulation of digital technologies and their usage in the DRC. It provides for the creation of several administrative authorities tasked with overseeing various segments of the digital sector, as outlined in Articles 7 to 12, 275 to 280, and 41. Among these authorities is the Data Protection Authority (DPA), whose creation is provided for in Articles 262 to 270 (for more information on the functioning of the DPA, see Brozeck Kandolo, "DRC: Perspectives of the Data Protection Authority," Africa Data Protection Report – January 2024, p. 18). This independent authority is intended to regulate personal data processing, addressing the growing challenges of an increasingly digitalized world.

However, despite these promising developments, an unexpected regulatory change occurred on August 17, 2024, with Ministerial Decree No. cab/min/pt&n/akim/kl/kbs/051/2024. Contrary to the provisions of the Digital Code regarding DPA creation, this decree temporarily transferred the DPA's powers to the Regulatory Authority for Posts, Telecommunications, and Information and Communication Technologies (ARPTIC).

This decision raises significant legal and strategic questions. Legally, there are concerns about the compatibility of the ministerial decree with the stipulations of the Digital Code. Furthermore, could the temporary transfer of the DPA's responsibilities to ARPTIC be seen as a pragmatic measure to address financial, administrative, or political constraints hindering the effective establishment of the DPA?

I. Legality of the Decree Assigning DPA's Missions to ARPTIC

ARPTIC is legally grounded in the 2020 Telecommunications and ICT law. However, it was only in 2023, following a decree by the Prime Minister, that it was officially established. It is important to note that ARPTIC succeeded the former Regulatory Authority for Posts and Telecommunications of Congo (ARPTC), which was replaced by this new entity.

DPA's missions' assignment to ARPTIC raises significant legal concerns. On one hand, it calls into question the compliance of this expansion of ARPTIC's powers with fundamental legal principles, particularly the principles of legality and speciality (A). On the other hand, it highlights issues related to the transfer of powers between entities and the respect for the principle of separation of powers (B).

A. Extension of ARPTIC's Powers: A Violation of the Principles of Legality and Specialization?

DPA's missions' assignment to ARPTIC raises a crucial legal question: can a decree legitimately extend the powers of an administrative authority beyond the limits set by the law that created it? This question directly challenges the compliance with the principles of legality and specialization, which are fundamental in administrative law.
The principle of norms hierarchy, according to Hans Kelsen's theory, dictates that legal norms are organized in an order of priority, where each norm must adhere to those superior to it. Under this principle, any subordinate norm, such as a decree or regulation, must comply with the law that forms its basis. Therefore, regulatory power, exercised through decree, cannot either extend or restrict the powers of an authority created by law, unless the original law explicitly provides for such an extension. In the present case, the decree in question, which aims to expand ARPTIC's powers, grants it responsibilities that are not foreseen by the law creating this authority. In fact, only a law can modify or supplement the powers of an administrative authority, in accordance with the principle of the hierarchy of norms.
Furthermore, the principle of specialization restricts the powers of public legal entities to the tasks explicitly defined upon their creation. This principle mandates that any action undertaken by a public authority must remain within the boundaries of the powers assigned to it by law. For ARPTIC, this means that, although the authority has seen its responsibilities expanded to include data protection, these new powers must be accompanied by a prior modification of the original legal framework.

In the case of the August 17, 2024 decree, ARPTIC is assigned missions that were not included in the 2020 Telecommunications and ICT law. Consequently, this expansion of powers exceeds the prerogatives established by the 2020 law and could be legally challenged for non-compliance with the principle of legality.
Thus, the legality of this reform in relation to the principles of legality and specialization remains uncertain, and its adherence must be thoroughly examined to ensure that ARPTIC's missions, particularly in the area of personal data protection, are situated within a valid legal framework that respects the rule of law.

B. Transfer of Powers and the Separation of Powers

According to the Digital Code, the establishment of the DPA should be done through a decree issued by the Prime Minister. Unexpectedly, however, it was through a ministerial decree that the powers of the DPA were transferred to ARPTIC.
From a legal perspective, it is legitimate to question whether an entity, which should be created by a decree from the Prime Minister, can have its powers transferred by a decree from the Minister of Posts, Telecommunications, and Digital Technologies (PTN). This situation raises concerns about the respect for the competencies and autonomy of public institutions.

Under the principle of power separation, enshrined in the Congolese Constitution (Article 68 of the Constitution of the DRC), each entity must operate within the scope of its defined powers. Therefore, the transfer of powers from an entity whose creation is conditioned by an act of the Prime Minister, if carried out by another authority without a clear legal basis, could constitute a violation of the principle of separation of powers.

II. The Challenges Posed by the Expansion of ARPTIC's Powers

The temporary assignment of the DPA's missions to ARPTIC can be seen as a positive move, reflecting the Congolese government's intention to regulate digital issues while limiting the significant costs associated with creating a new authority. This choice seems particularly relevant in a context where Congo already has several institutions, such as the Digital Regulatory Authority and the National Electronic Certification Authority, some of whose powers have also been transferred to ARPTIC.

However, the issue of personal data protection is of particular significance. Since it involves fundamental rights, it requires heightened vigilance. Thus, assigning the DPA's missions to ARPTIC raises several questions: does ARPTIC possess the necessary independence to carry out these new tasks impartially (A)? And what is the relevance of combining ARPTIC's economic objectives with such a sensitive mission as personal data protection (B)?

A. ARPTIC Independence

ARPTIC operates under the oversight of the Minister of Posts, Telecommunications, and New Technologies (PTN), which raises concerns about its ability to function fully autonomously. The hierarchical dependency of ARPTIC on the ministry could undermine its impartiality and lead to conflicts of interest, especially in politically sensitive matters. This administrative subordination may affect the autonomy of its decisions, compromising the transparency and impartiality necessary to ensure effective protection of personal data.

Another major issue lies in the appointment of ARPTIC's leaders, particularly those on the board of directors and the executive management. According to Articles 15 and 21 of Decree No. 23/13 of March 3, 2023, these individuals are appointed, removed from their positions, and dismissed by presidential order. Furthermore, Article 24 of the same decree states that auditors are appointed by a decree from the Prime Minister. This reliance between the authority responsible for appointments and the appointees raises a critical question: Can the independence of ARPTIC's leaders in making decisions, particularly regarding data protection, truly be ensured within such a framework?

Therefore, the independence of ARPTIC is vital to

© iStock

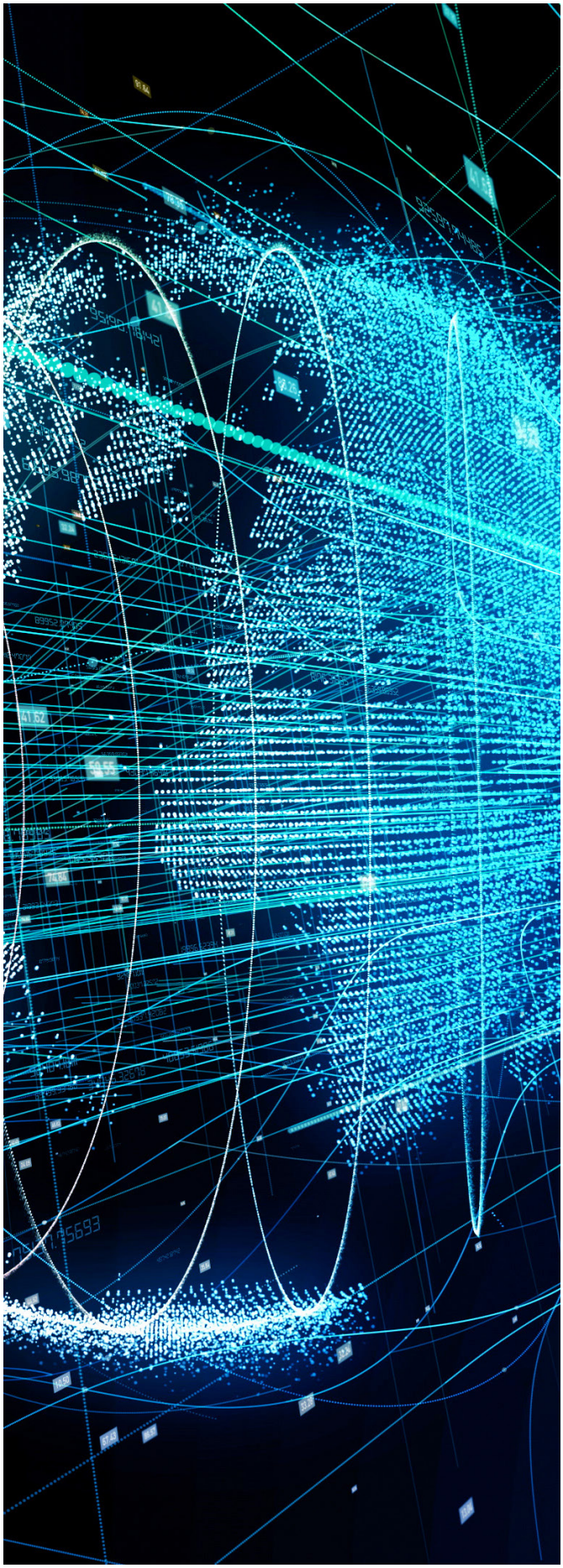
ensure impartial and effective regulation of personal data protection in the Democratic Republic of Congo. The stakes surrounding data protection are too high to be subject to political pressures. It is essential to implement concrete measures to ensure that ARPTIC can carry out its missions autonomously, free from external interference, pending the establishment of the APD.

B. ARPTIC: Balancing Economic Regulation and Data Protection

ARPTIC's primary missions involve regulating the telecommunications and information and communication technologies (ICT) markets. Its focus is mainly on economic objectives such as promoting competition, optimizing infrastructure, and improving service quality in these sectors. While these missions are essential for the development of the digital sector, they do not always align with the requirements of an authority dedicated to personal data protection.

Economic regulation often demands a more flexible and pragmatic approach, aiming to enhance market efficiency and encourage innovation. In contrast, personal data protection imposes strict obligations regarding confidentiality, security, and transparency. This requires constant vigilance, independence in oversight, and the ability to oppose abusive practices, even if doing so may have economic repercussions for industry players.

Lastly, ARPTIC is tasked with arbitrating sometimes conflicting interests, particularly in reconciling the promotion of competition with the need for data security and confidentiality. However, these goals may come into conflict, as initiatives designed to boost market competitiveness can sometimes undermine the protection of personal data. **B.K**



© iStock

WWW.AFRICADATAPROTECTION.ORG
INFO@AFRICADATAPROTECTION.ORG