PARADIGM INITIATIVE

Digital Policy Digest

Digital Policy Digest

No. 4 of 2024

This Digital Policy Digest (DPD) documents digital rights policies and laws and presents guidance on areas needing reform. This edition assesses Senegal's AI Strategy Horizon 2028, Nigeria's Cybercrimes Act, and its Implications for Digital Rights. It also analyzes Nigeria's AI Strategy 2024: Addressing Gaps in Digital Rights Protection for a Fair and Inclusive Future. Additionally, it includes an analysis of Burundi's Law No. 1/10 of March 16, 2022, on the Prevention and Repression of Cybercrime, examining its impact on digital freedoms and cybersecurity governance.

This publication is not for sale. It is provided as a part of Paradigm Initiatives mission to "Connect African youth with digital opportunities and ensuring digital rights for all". The Digital Policy Digest is published quaterly by Paradigm Initiative.

Researchers: Sarra Hannachi, Joseph Akoli, Sapni GK (Digital Rights and and Inclusion Learning Lab 2024 Fellows)

Editorial Designer: David Chima

An Assessment of Senegal's AI Strategy Horizon 2028

By Moussa Waly Sene

01

Introduction

Senegal has set an ambitious goal to become an African leader in artificial intelligence (AI) by 2028. A National AI Strategy was adopted in 2023, based on six strategic directions to achieve this. The strategy aims to harness AI's capabilities to stimulate economic growth, enhance national competitiveness, and provide concrete solutions to the country's social and economic challenges. However, while the roadmap is ambitious, certain areas need adjustments to ensure its success. Senegal aims to become an African AI leader by developing a robust and inclusive national framework. The goal is to use AI to improve economic competitiveness while ensuring ethics, responsibility, and trust in its use, serving citizens, businesses, and the state.

Strategy

Senegal's AI strategy outlines six strategic directions to position the country as a leading AI hub in Africa and a pioneer in applied AI across key sectors such as health, agriculture, and finance. The plan emphasises creating an AI ecosystem through clusters, incubation programmes and international partnerships while fostering innovation through flexible regulations, data governance and ethical frameworks. It prioritises workforce development with national training programmes, certifications and research partnerships, promoting inclusivity by addressing the digital divide. Ensuring ethical and responsible AI use through normative frameworks and a National Ethics Committee is central to the strategy's vision of leveraging AI for sustainable and equitable development.

Cross-cutting Issues and Implementation

The success of this strategy will depend on collaboration among stakeholders who include the government, private sector, universities, civil society organisations and international partners. Cross-cutting leadership (Action 6.5) and establishing a dedicated regulatory body (Action 6.7) will ensure that the strategy aligns with Senegal's ethical and economic objectives.

Senegal's short-term AI implementation plan is structured into two waves over 18 months. The first wave focuses on launching the strategy by creating a National AI Team (Campus Sen AI), organising a national consultation, and establishing a governance structure for AI oversight. The second wave prioritises building momentum through AI awareness seminars, modernising digital infrastructure, creating an AI observatory, adapting startup regulations, and forging regional and international alliances. Key actions also include setting an international AI training standard. This phased approach aims to establish a robust institutional framework, align with global standards, and strengthen Senegal's AI capabilities and infrastructure.

Strategic Directions Analysis

1. **Positioning Senegal as an African AI Hub:** The main objective is to create a competitive digital ecosystem. Setting up an AI cluster (Action 1.1) and incubation programs for startups (Action 1.4) are critical steps in structuring the ecosystem and attracting talent. However, the success of this endeavor

relies on the country's ability to attract foreign investment and foster international partnerships. Rwanda, for instance, has positioned Kigali as a regional tech hub through similar initiatives[1] supported by Google[2] and other tech giants.

2. **Positioning Senegal Among Leaders in Applied AI:** The strategy emphasizes AI applications in key sectors such as health, agriculture, and finance. AI could play a crucial role in enhancing telemedicine services, facilitating agricultural forecasting, and promoting financial inclusion. However, these initiatives need to be adapted to local needs and available infrastructure. A success story is Kenya's use of AI in the agricultural sector to improve weather forecasting, helping farmers better plan their harvests (KAOP)[3].
3. **Fostering Innovation:** To support innovation, an AI code (Action 3.1) and regulatory sandboxes (Action 3.4) are proposed, allowing companies to test solutions in a controlled environment. However, existing laws must be adapted to the current realities of big data and AI. Senegal will need to modernize its regulations to accompany this technological revolution, similar to the European Union's General Data Protection Regulation (GDPR)[4], which serves as a model for managing sensitive data.[5]
4. **Strengthening AI Expertise:** Training 90,000 Senegalese in AI skills is a central pillar of the strategy. While commendable, the initiative cannot succeed without a robust and adapted educational infrastructure. Senegal must avoid a brain drain by creating local opportunities for young graduates, a challenge the country already faces in other sectors. Partnerships with African and international universities, as seen in South Africa with research centers, could strengthen these capacities.
5. **Promoting Digital Inclusivity:** The strategy acknowledges that AI should not exacerbate digital divides but rather provide opportunities for all. Initiatives like AI awareness for rural and disadvantaged populations are crucial to ensure that AI adoption does not widen existing inequalities. However, more efforts are needed to ensure access to technological tools in remote areas, where internet access remains limited.
6. **Encouraging International AI Cooperation:** The last strategic axis emphasizes the importance of international collaboration in positioning Senegal on the global AI stage. The country aims to develop partnerships with AI-leading nations and actively participate in international bodies on AI norms and regulations (Action 6.2). However, this cooperation must genuinely address

[1] https://www.africa.engineering.cmu.edu/about/living-in-rwanda/kigali-innovation-city.html

[2] https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Press_Release/Government_of_Rwanda_and_Google_Collaborate_to_Accelerate_Digital_Transformation.pdf?utm_source

[3] https://kaop.co.ke/?utm_source

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[5] https://www.cnil.fr/en/ai-system-development-cnils-recommendations-comply-gdpr

local needs and priorities, focusing on capacity building and technological independence.

Analysis of the Strategic Directions

1. **Position Senegal as an AI Hub in Africa**
   The main objective is to create a competitive digital ecosystem. Establishing an AI cluster (Action 1.1) and incubation programs for startups (Action 1.4) are important steps in structuring the ecosystem and attracting talent. However, creating an environment conducive to innovation depends on the country's ability to attract foreign investments and foster international partnerships.
2. **Position Senegal Among Leaders in Applied AI**
   The strategy focuses on the application of AI in key sectors such as health, agriculture, and finance. AI could play a decisive role in improving telemedicine services, facilitating agricultural forecasting, and promoting financial inclusion. However, these initiatives must be tailored to local needs and available infrastructure. An example is Kenya's use of AI in agriculture to improve weather forecasting, helping farmers better plan their crops.
3. **Framework for Innovation**
   To support innovation, an AI code is proposed (Action 3.1), along with regulatory sandboxes (Action 3.4), which would allow companies to test solutions in a controlled environment. However, it is crucial to adapt existing laws to the current realities of big data and AI. Senegal must revise its regulations to accompany this technological revolution, similar to the European Union's General Data Protection Regulation (GDPR), which serves as a model for managing sensitive data.
4. **Strengthening AI Capabilities and Expertise**
   Training 90,000 Senegalese citizens in AI skills is a central pillar of the strategy. While this initiative is commendable, it

cannot succeed without a robust and adapted educational infrastructure. Senegal must prevent brain drain by creating local opportunities for young graduates, a challenge the country already faces in other sectors. Partnerships with African and international universities, like those in South Africa with European research centers, could strengthen these capabilities.

5. **Promote Digital Inclusivity**
   The strategy recognizes that AI should not widen the digital divide but serve as an opportunity for everyone. Initiatives such as AI awareness for rural and disadvantaged populations are essential to prevent AI adoption from exacerbating existing inequalities. However, efforts must be made to ensure that technological tools are accessible in remote areas with limited internet access. Google's Project Loon, which used balloons to provide internet access to remote populations, is an example of an innovative initiative to improve internet access in hard-to-reach areas. For Senegal, it will be crucial to implement solutions adapted to local realities, such as expanding mobile networks and affordable connectivity solutions (Action 5.2). This also includes strengthening telecommunications infrastructure in rural areas and subsidising access to digital devices and services for low-income households.

International AI Cooperation

The final strategic direction of Senegal's National AI Strategy emphasises the importance of international collaboration to position the country on the global AI landscape. Senegal aims to develop partnerships with leading AI countries while actively participating in international bodies on AI standards and regulations (Action 6.2). Indeed, to secure a place in the global AI economy, the country must collaborate with strategic actors and join multilateral initiatives, like the "Global Partnership on Artificial

[6] https://x.company/projects/loon/

Intelligence," which several African nations are already part of. However, it is essential that this cooperation truly benefits local needs and priorities, rather than being focused solely on top-down technology transfer. Acquiring know-how, strengthening local capacities, and achieving technological independence should remain central to these international partnerships. A good example of this dynamic is the cooperation between China and Ethiopia on AI, where centers of excellence were co-created to enhance local skills while benefiting from international technological advancements.

These six strategic directions of Senegal's National AI Strategy demonstrate a strong ambition to position the country as a key player in AI, not only on the African continent but also globally. Nonetheless, to realize this ambition, the strategy must be grounded in local realities that consider existing infrastructure, population needs, and Senegal's social and economic challenges. The absence of detailed financing, measurable KPIs, and attention to the country's sociocultural dimensions are gaps that need to be addressed for Senegal to fully exploit AI's potential and improve the daily lives of its citizens.

Critical Review of the Strategy

Strengthening Infrastructure and Developing Skills

Strengthening digital infrastructure and training a skilled workforce are two major pillars of this strategy. Modernising infrastructure, including adapting data centers and enhancing connectivity in rural areas, is essential to support AI projects. Initiatives like the creation of a national AI training programme and the establishment of certifications are notable advancements.

However, the large-scale rollout of these trainings faces major challenges, such as the lack of specialised educational infrastructure and the risk of brain drain. Without incentives to retain these newly trained individuals, Senegal could see its talent benefit foreign markets rather than strengthen the local ecosystem. Governance, Ethics, and Inclusion: An Essential Reflection

Ethical and Responsible AI

Ethics is another central point in Senegal's AI strategy. With the establishment of a legislative framework to regulate AI in line with international standards and the creation of a National Ethics Committee, Senegal aims to ensure the responsible use of AI. However, the current data protection law, dating back to 2008, is outdated and needs revision to adapt to the new realities of big data.

Respecting Senegalese societal values and aligning AI with human rights are fundamental principles, but remain largely theoretical. For example, the use of AI in telemedicine could revolutionize healthcare access in remote areas, yet the strategy lacks concrete details on implementing these initiatives in isolated regions.

A Digital Inclusion Effort

Digital inclusivity, particularly for women, youth, and disadvantaged populations, is another important aspect. Awareness programs on AI are planned to bridge the digital divide. However, the strategy must go further to ensure that these populations can not only access these technologies but also benefit from them in a sustainable way. Kenya's example, which launched digital training initiatives for youth in rural areas, shows that such actions can have a significant impact if well-structured.

AI in Priority Sectors - Agriculture, Health, Education: An Underexploited Strategic Axis

The application of AI in strategic sectors such as agriculture, health, and education is at the core of the strategy. In agriculture, for instance, AI could be used to optimize crop management, improve weather forecasting, and reduce post-harvest losses, contributing to food self-sufficiency. The potential for AI in precision agriculture is widely recognized, as demonstrated by Brazil[7], a leader in using AI to boost agricultural production.
However, this ambition remains underexploited in Senegal. The AI strategy has not adequately addressed the country's food

[7] /

dependency, and the proposed action plan has not provided concrete solutions to the high unemployment rate, particularly among the youth. For the training of 90,000 Senegalese in AI-related skills to have a meaningful impact, it must be accompanied by tangible job opportunities in these crucial sectors.

Challenges and Recommendations for Successful Implementation

Gaps in Implementation and Monitoring

One of the significant challenges in Senegal's AI strategy lies in its implementation. The lack of identified funding sources and key performance indicators (KPIs) to measure progress could jeopardize its success. To prevent this strategy from remaining a set of unfulfilled intentions, solid partnerships with private investors and international organisations must be established. Additionally, assigning responsibility for each action would allow for better coordination and rigorous progress monitoring.

Considering Socio-cultural Realities

Senegal's AI strategy must be adapted to local realities. AI can only succeed if it integrates harmoniously into citizens' daily lives. Initiatives must promote development seen in countries like India, where AI has been used to enhance traditional agricultural practices. Rather than imposing imported technological solutions, the strategy should draw inspiration from local needs and provide solutions tailored to the country's specific challenges.

Recommendations to Strengthen Senegal's National AI Strategy

1. **Creation of a Favorable Environment for Human Rights-Based AI**

   To support AI innovation while safeguarding digital rights, Senegal could adopt the following measures:

   - Inclusion of Digital Rights in AI Regulations: Integrate provisions on personal data protection, freedom of expression, and non-discrimination into national AI legislation.
   - Creation of a National AI Ethics Committee: Establish an independent body to assess AI projects based on their impact on human rights and recommend redress mechanisms.
   - Dynamic Regulatory Framework: Inspired by Regulatory Sandboxes, this framework allows companies to test innovations under strict supervision to prevent abuses.

2. **Prioritisation of Key Sectors: Agriculture, Health, and Education**

   Senegal must focus its AI efforts on key sectors while ensuring that technologies respect citizens' fundamental rights, including digital ones.

   - Agriculture: AI should improve agricultural resource management and climate forecasting while protecting farmers' data and rural communities. AI systems must adhere to informed consent and data transparency principles.
   - Health: In healthcare, the use of AI for telemedicine or medical data analysis must be accompanied by the confidentiality of sensitive data, protection against the misuse of biometric data, and the establishment of informed consent mechanisms for processing health data.
   - Education: AI solutions must respect students' privacy, avoid excessive data collection, and ensure special protection for children's data. AI could also help bridge the digital divide by providing content adapted to marginalised communities.

3. **Senegal's Strategic Positioning in Africa**
   To become a key player in AI in Africa, Senegal should adopt a Human Rights by Design approach from the conception of AI solutions by:
   - Development of Ethical Chips and Algorithms: Encourage research on bias-free algorithms tailored to African contexts, especially in sensitive sectors such as health or security.
   - Regulation of Public-Private Partnerships: Any international or private AI collaboration must comply with human rights clauses to protect privacy and freedom of expression.
   - Transparency in Automated Decision Processes: Require companies using AI to publish their decision-making models to prevent discrimination in areas such as credit access, employment, or public services.
4. Awareness and Capacity Building
   - Strengthen the capacities of data protection authorities, tech companies, and civil society organisations on AI ethics and digital rights protection.
   - Develop public awareness campaigns to inform citizens about their digital rights in an AI-powered environment.

These recommendations aim to maximize the impact of the National AI Strategy by aligning technological objectives with the country's real needs and positioning Senegal at the center of Africa's AI ecosystem.

Conclusion

Senegal's National Artificial Intelligence Strategy offers an ambitious roadmap to make the country a regional leader in AI by 2028. However, for this ambition to become a reality, the strategy must address the country's socio-economic challenges, ensure rigorous implementation monitoring, and fully integrate cultural and local realities. By strengthening efforts in key sectors such as agriculture, health, and education, and ensuring that AI is inclusive and ethical, Senegal can leverage AI as a tool for sustainable development.

Nigeria's AI Strategy 2024: Addressing Gaps in Digital Rights Protection for a Fair and Inclusive Future.

By Shorefunmi Bola-Saliu

02

AI
AI

Introduction

Artificial Intelligence is a welcome, transformative revolution that has come to stay. Recognising its continuing impact, governments and institutions across the globe are actively engaging in close and open dialogues to create regulations, laws, and strategies to guide its responsible use. In Africa, Nigeria stands out as a leading advocate for technological advancement and is at the forefront of AI strategy on the continent. The government of Nigeria together with the National Centre for Artificial Intelligence and Robotics (NCAIR) is committed to harnessing AI's potential for inclusive growth, economic growth, job creation, and technological innovation[8], Nigeria's approach not only reflects its ambition but also sets a foundational framework for responsible and ethical AI adoption across Africa.

However, an analysis reveals several limitations regarding its ability to fully address critical digital rights issues, particularly for vulnerable populations such as children, marginalised communities, and people with disabilities. Despite the inadequately identified solutions in the strategy, the strategy acknowledges the possible unprecedented challenges for governments, especially when it comes to ethical applications, algorithmic transparency, and data privacy.[9]

Background

Recognising AI as a transformative technology capable of driving economic growth, innovation, and social progress, the Nigerian government initiated NAIS to position the country as a leader in AI on the African continent. The Ministry of Communications, Innovation and Digital Economy(NITDA) hosted a 4-day workshop themed "Developing the High-level Strategy and Implementation

[8] https://techpoint.africa/2024/09/10/nigeria-launches-ai-fund/

[9] https://ncair.nitda.gov.ng/wp-content/uploads/2024/08/National-AI-Strategy_01082024-copy.pdf

Plan for a National AI Strategy for Nigeria" between April 15 and 18, 2024, to co-create a National Artificial Intelligence Strategy (NAIS).[10] This strategy is still in the draft stage and is yet to be gazetted. The current status is that it is a draft document awaiting finalisation and implementation. The National Artificial Intelligence Strategy (NAIS)[11] provides a comprehensive roadmap to harness AI's potential, guiding the nation's distinctive approach to maximising AI benefits across key sectors such as (e.g., healthcare, education, agriculture) for improved outcomes and citizen welfare. NAIS aims to address national priorities—such as improving healthcare, education, and infrastructure—while ensuring data privacy, transparency, and inclusivity. Through NAIS, Nigeria seeks to foster collaboration across sectors, ensure alignment with international standards, and prepare the nation for AI-driven advancements.

The Nigerian National AI Strategy (NAIS) is built around five strategic pillars, each addressing key components necessary for fostering a robust AI ecosystem and achieving AI-driven transformation. It also addresses critical areas like risk and impact assessments, AI red lines, oversight, transparency, and accountability, primarily under the pillars focused on ethical AI development and governance.

These strategic pillars are:

- Building Foundational AI Infrastructure
- Building and Sustaining a World-Class AI Ecosystem
- Accelerating AI Adoption and Sector Transformation
- Ensuring Responsible and Ethical AI Development
- Developing a Robust AI Governance Framework

As the global landscape of artificial intelligence (AI) continues to evolve, the need for a comprehensive National AI Strategy (NAIS) that prioritises digital rights becomes increasingly critical. Digital rights encompass various issues, including data privacy, access to information, freedom of expression, and protection against surveillance. In developing countries, and as seen in Nigeria, these rights are often underrepresented in national strategies, leading to potential misuse of AI technologies and widening inequalities.

[10] https://fmcide.gov.ng/ministrys-artificial-intelligence-strategy-workshop-to-attract-120-experts-from-across-the-world/

[11] https://ncair.nitda.gov.ng/wp-content/uploads/2024/08/National-AI-Strategy_01082024-copy.pdf

Identified Inadequacies in the strategy

1. **Lack of focus on the protection of vulnerable groups such as women, children, elderly, and the disabled.**
   The current approach to Nigeria's AI strategy shows a concerning lack of emphasis on the digital rights of vulnerable groups, including women, children, the elderly, and individuals with disabilities. It is imperative that vulnerable groups are adequately represented and protected in any AI framework developed.[12]

   As AI technologies, such as deepfakes, become more prevalent, they pose significant risks, particularly concerning issues like image-based gender abuse and child sexual exploitation. The emergence of deepfake technology has been linked to the creation of harmful content that exploits and victimises these vulnerable populations. With increased access and rapid adoption of AI-based technologies, there is a risk that deepfakes become a powerful and dangerous tool for this type of crime, as the perpetrator no longer needs authentic content but can generate it with a quality that increases the likelihood of people believing it is real. On the other hand, victims are left in a vulnerable position, as it is challenging to refute the authenticity of these videos and completely remove them from cyberspace. The repercussions at the social, professional, or health levels can be highly impactful. It becomes evident that the consequences of digital gender-based violence can extend beyond the cyberspace sphere.[13] Therefore, the strategy must draw from existing lessons and best practices to establish robust protections for vulnerable groups.

2. **Lack of Comprehensive Privacy Protections**
   While the strategy mentions AI's potential for social good in its strategic aims and objectives, "social development and inclusion," it lacks concrete measures on data privacy and

[12] https://unesdoc.unesco.org/ark:/48223/pf0000381137/PDF/381137eng.pdf.multi

[13] https://blogs.iadb.org/igualdad/en/deepfakes-gender-based-violence-in-the-era-of-artificial-intelligence/

protection, especially for vulnerable groups. Effective digital rights protection would require stringent standards for data governance to prevent misuse, particularly for minors and marginalised communities who may be disproportionately impacted by data exploitation.

3. **Insufficient Measures Against Algorithmic Bias**
   The strategy emphasises AI-driven economic growth particularly under its third strategic pillar, “Accelerating AI Adoption and Sector Transformation.” This section highlights how AI will be leveraged to boost economic activities across various industries and promote sustainable development. However, it does not adequately and directly address algorithmic bias, a significant issue in digital rights. AI systems can unintentionally perpetuate biases present in training data, potentially discriminating against minority groups. Without clear guidelines on bias mitigation, Nigeria risks adopting AI applications that could inadvertently reinforce social inequalities.

Recommendations to Strengthen the Strategy

To effectively safeguard the digital rights of vulnerable populations within Nigeria’s AI strategy, several key measures should be implemented:

- First, the enactment of comprehensive AI-specific privacy laws is essential and not just relying on the Nigerian Data Protection Act which has its weaknesses too.
- These laws must focus on enforcing data protection measures tailored for vulnerable users, incorporating robust consent mechanisms, strict data anonymisation standards, and clear penalties for the misuse of personal data.

- Additionally, mandating fairness audits for AI algorithms is crucial, particularly for those deployed in sensitive sectors. These audits should evaluate algorithms for potential discriminatory impacts and provide recommendations for more inclusive AI design.

By implementing these recommendations, Nigeria can create a comprehensive AI strategy that fosters innovation and respects and protects the digital rights of all its citizens, especially the most vulnerable.

Conclusion

Nigeria's AI Strategy 2024 reflects a forward-thinking approach to leveraging artificial intelligence for economic growth, innovation, and societal development. However, the strategy's ability to build a fair and inclusive digital future depends on its approach to addressing gaps in digital rights protection. By incorporating clearer frameworks for risk and impact assessments, focusing on protecting vulnerable groups such as women, children, the elderly, and the disabled, and enhancing comprehensive privacy protections, Nigeria can position itself as a leader in equitable and transparent AI development.

The Nigeria Cybercrimes Act and Implications on Digital Rights

By Shorefunmi Bola-Saliu

03

Background

The Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act, 2024[14] establishes a comprehensive legal framework to address the growing challenge of cybercrimes in the country. The aim of the Act is to provide an effective, unified, and structured approach to the prohibition, prevention, detection, prosecution, and punishment of cyber-related offences. This legislation marked a significant step forward in Nigeria's efforts to regulate the digital space, as it introduced measures to counter threats such as identity theft, online fraud, cyberbullying, and unauthorised data access while supporting digital security and law enforcement capabilities.

The 2024 Act is an amendment to the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.[15] Some of the amendments include, allowing transactions to be valid by electronic signature if they are legally verified in Certified True Copies; establishment of the Sectoral National Computer Emergency Response Teams (CERTs), Sectoral Security Operations Centers (SOCs) and a requirement of National Identification Number (NIN) for Electronic Financial Transactions.

Implications on Digital Rights

The Cybercrimes (Prohibition, Prevention, Etc.) Act, 2024, establishes a legal framework in Nigeria geared at enhancing protection against cybercrimes for both individuals and organisations.

The Act, in Section 24, sets boundaries on harmful activities like cyberstalking, misinformation, and hate speech to foster safer online environments. However, ambiguity in defining these activities leads to overreach, infringing on free expression, as the government uses this provision to suppress the right to freedom

[14] https://cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2024.pdf
[15] https://www.nfiu.gov.ng/images/Downloads/downloads/cybercrime.pdf

of expression. This tension underscores the importance of clear guidelines to balance security with civic rights.

Section 38, addresses how data is collected, stored, and shared, particularly with law enforcement. This protects data privacy, but it also raises questions about government surveillance and the need for transparency.

Under Section 12, the Act stipulates grounds for unlawful data interception, highlighting the importance of clear, rights-respecting guidelines to prevent privacy infringement.

The Act also places obligations on Internet Service Providers (ISPs) and digital platforms to collaborate with law enforcement. Provisions like Section 38 require ISPs to retain customer data for 2 years and to provide access to this information upon lawful request. This encourages accountability and transparency among service providers.

Inadequacies of the Act

1. **Vagueness and Overreach:**
   As previously mentioned, certain provisions in the Act are vaguely worded. For example, Section 24 uses words like "annoyance," "inconvenience," or "insult." These words are subjective and open to interpretation, making it easy to misuse this section to target legitimate expressions or dissent and potential overreach by law enforcement. This can infringe on individuals' rights to freedom of expression and privacy, as vague laws are usually used by governments as justification to suppress dissents or legitimate online activities in opposition to them.

2. **Insufficient Safeguards for Privacy:**
   While the Act aims to protect data, and stricter measures

have been put in place in the 2024 Amendment Act, it still lacks sufficient safeguards for individual privacy rights. The requirement in Section 38 subsections 2 and 3, for service providers to disclose user data to law enforcement on account of only a request without adequate protection mechanisms, can lead to privacy violations.

3. **Disproportionately Severe Penalties:**
   The penalties prescribed under the Cybercrimes Act are already creating an environment of fear and caution, with some penalties for certain offences considered disproportionately severe. This has led to instances of self-censorship among internet users, as individuals fear facing strict legal consequences. The case of Socio-Economic Rights and Accountability Project (SERAP) v. Federal Republic of Nigeria in the ECOWAS Court of Justice underscores the challenge of balancing cybersecurity laws and freedom of expression, especially when laws may be broadly interpreted to silence journalists and activists.

4. **Exclusion of Marginalised Groups:**
   There is insufficient consideration for the digital rights of marginalised groups, including women, and children. For instance, provisions that address data privacy and cyber harassment lack explicit protections or procedures that prioritise the unique vulnerabilities of these groups. Women, who are often targets of gender-based cyber violence, may find the legal avenues to address their grievances under this Act limited. Similarly, children’s exposure to online exploitation is a growing concern globally, yet the Act does not provide targeted measures that address the specific digital rights and protections necessary to guard against child exploitation and abuse online.

Recommendations

Several improvements are recommended to ensure the Act better aligns with digital rights:

- Lawmakers should clarify ambiguous terms, especially in areas related to hate speech and cyberstalking, to prevent misuse that could stifle free expression. Second, enhanced privacy safeguards are necessary, such as stricter oversight and guidelines to monitor data requests from law enforcement.
- By also incorporating considerate protections for marginalised groups, like women and children, the Act could offer better safeguards against gender-based and child exploitation online. Finally, establishing regular audits for service providers would promote accountability and transparency, protecting against inappropriate surveillance.

These and future recommendations, which should be periodically amended to keep pace with the evolving threat landscape and the protection of digital rights, will foster the creation of a more comprehensive and balanced Act. This will not only strengthen the prevention and prohibition of cybercrimes but also ensure that the rights of citizens whom the Act seeks to safeguard are adequately respected.

Conclusion

In conclusion, while Nigeria’s Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act, 2024 amendment represents a significant step in regulating cyber activities, captious gaps remain in adequately safeguarding digital rights. The Act’s amendments to preventing cybercrime, such as mandating electronic signatures, requiring NIN for electronic transactions, and establishing response teams, are well-intentioned. However, some aspects of the law such as ambiguous language around cyberstalking, no strict monitoring in data sharing requirements, and overly severe penalties, need to be looked into urgently.

Analysis Of Law N°1/10 Of March 16, 2022, On The Prevention And Repression Of Cybercrime In Burundi

By Avit Ndayiziga

04

RITY

Introduction

Burundi faces the pressing need to embrace digital technologies like many other states. Digital tools have become essential in Burundians' daily lives. Out of a total population estimated at 13,097,400 in 2023, the Regulatory and Control Agency for Telecommunications (ARCT) reports that 2,960,563 people, or 22.6% of the population, were connected to the Internet, generating an average monthly revenue of 13,683,296,664 BIF in March 2024. Mobile telephony subscriptions reached 8,289,139 users, representing 63.29% of the population, with an average monthly turnover of 7,102,876,457 BIF during the same period. Burundi still lags behind compared to other countries, but it is gradually adopting digital technologies to benefit from them fully.

The Evolution of ICT Requires Legal Regulation

The proliferation of electronic services in Burundi calls for legal instruments adapted to the rapid development of ICT, especially in areas such as personal data protection, cybersecurity, and consumer protection for digital services.

Prevention and Repression of Cybercrime in Burundi

To address these needs, the Government of Burundi enacted Law No. 1/10 of March 16, 2022, on preventing and repressing cybercrime in Burundi. This law aims to prevent and punish all cyber offenses committed within or outside Burundi, as long as the offense produces effects within the country. It also applies to any criminal offense requiring electronic evidence collection.

Furthermore, the law covers unauthorized access or complicity in hindering, altering, deleting, or modifying the functioning of an information system related to critical infrastructure. While the promulgation of this law is a welcome development, no law is without flaws. This law, in particular, is improvable and should be enhanced.

Analysis and Critique

The law comprises only 70 articles, and addresses just four categories of offenses. The first category concerns the confidentiality, integrity, and availability of data in information systems. However, these elements are insufficiently developed in the text. For instance, concepts like data confidentiality and integrity are complex and deserve broader treatment.

The law also touches on terrorism-related offenses, but only in a few brief articles. It fails to comprehensively address cyberterrorism, an increasingly relevant threat in the digital age.
Moreover, the law mentions offenses against state security, targeting violations involving state information systems. Arti-

cles 61 and 63 refer to privacy protection, but two short articles only briefly cover the matter.

The law should emphasize privacy and personal data protection by providing for a dedicated legal framework and institutional mechanisms to ensure enforcement and oversight.
Another major concern is the disproportionate severity of penalties, especially compared to Burundi's Penal Code. For example, fraud is punishable under Article 315 of the Penal Code with 2 months to 5 years of imprisonment and a fine of only 50,000 to 100,000 BIF. However, under the cybercrime law, a comparable fraud offense can carry 5 to 10 years of imprisonment and a fine of 10 to 20 million BIF — a dramatic increase in punitive measures.

Recommendations

If the law is ever revised, several elements should be reconsidered. For example, Title or Chapter 7, which provides a "special procedure" for cybercrime, is misleadingly titled. The chapter does not clearly define which procedures to follow or which authority is competent. Victims of digital offenses must still go through regular judicial police officers, whereas specialized cybercrime units and prosecutors would be more appropriate.

Another gap is the lack of provisions protecting intellectual property rights. The law also fails to protect digital consumers despite its objective of ensuring their security and sanctioning those who infringe upon their digital freedoms.

Conclusion

In conclusion, this law does not address international cooperation in the fight against cybercrime, whether in terms of procedures, extradition, prosecution of offenders, or victim compensation. The law must reference international frameworks, such as the African Union Convention on Cybersecurity and Personal Data Protection, and the Budapest Convention on Cybercrime, adopted in 2001.

More About PIN

Paradigm Initiative has worked in communities across Nigeria since 2007 and across Africa since 2017, building experience, community trust, and an organisational culture that positions us as a leading non-governmental organisation in ICT for Development and Digital Rights on the continent. Across our regional offices in Kenya, Nigeria, Senegal, Zambia, Zimbabwe, Cameroon, the Democratic Republic of Congo (DRC), and beyond, we have impacted youth with improved livelihoods through our digital inclusion and digital rights programs. The organisation's programs include Life Skills. ICTs. Financial Readiness. Entrepreneurship (LIFE) Training Program, a digital readiness workshop for girls, and Life@School Club Program. PIN has also built online platforms that educate and serve as safe spaces for reporting digital rights violations. These mediums, in the form of reports, short films, and educational online platforms, include Ayeta, Londa, and Ripoti. The organisation is also the convener of the annual Digital Rights and Inclusion Forum (DRIF), a pan-African platform where conversations on digital policy in Africa are shaped, policy directions debated, and partnerships forged for action. The forum has been held since 2013.

PARADIGM
INITIATIVE

Free download of this policy digest and past issues, visit www.paradigmhq.org or scan code: