SPECIAL EDITION OF THE CALABAR HISTORICAL JOURNAL (PROCEEDINGS OF THE 4TH INTERNATIONAL MULTIDISPLINARY CONFERENCE 27TH-30TH OCTOBER, 2024)
Vol. 14 (Special Edition), No. 1, June 2025 p140-162 ISSN: 2315-8816
https://thecalabarhistoricaljournal.com/

DIGITAL SOVEREIGNTY AND GLOBAL GOVERNANCE: THE DILEMMA OF AFRICA'S DATA SECURITY IN THE AGE OF GLOBALISATION

By

Boypa **EGBE**
Department of History and International Studies
University of Calabar
Calabar – Nigeria
boypaegbe@gmail.com
ORCID: 0009-0007-8079-2966

&

OTORA, Osmond Agbor
Department of History and International Studies
University of Calabar
Calabar – Nigeria
agbor02@gmail.com
otoragbor@unical.edu.ng
ORCID: 0000-0001-5886-3798

Abstract

This paper examines the future of sovereignty in a digital and geopolitically contested age and explores the conceptual and empirical development of digital sovereignty in the governance of the digital space. It is argued that digital sovereignty has emerged as a critical concept in international relations, challenging the traditional doctrine of sovereignty and the ability of state actors to exercise control in global governance. Using data from textual content analysis and anchored on the theoretical construct of political realism, the complex nature of digital sovereignty, relating to the intersectionality of several variables, including security, politics, economy, sociocultural, legal, environmental, and human rights, is highlighted. The paper further examines the different interests that motivate digital sovereignty, including the protection of citizens' rights, competitiveness in cyberspace for strategic public interests, and the dilemma of data colonialism in Africa. The paper concludes that there is a need for an all-encompassing framework to regulate the digital sphere while preserving individual liberties and national sovereignty, given the increasing power of non-state actors.

Keywords: *Digital sovereignty, global governance, national security, data colonialism, political realism*

Introduction

The debate about digital sovereignty cannot be divorced from wider debates about sovereignty in international relations. The question of sovereignty is itself a complicated one and

one that has long been a central, contentious issue in international affairs, as it structures the core character of a nation-state. Since the Westphalia Treaty in 1648, the concept of sovereignty has been shaped, refuted, and evolved over historical conjunctures.[1] The concept of sovereignty has also been largely discussed by scholars with different theoretical orientations, ranging from Realism, Liberalism, Constructivism, and Critical Theory etc. Over time, the arguments have also been influenced by empirical processes of international politics such as the rise of nation-states, decolonization, and the emergence of globalisation (the UN) and regionalism like the EU, AU, ASEAN, OAS, etc, thereby raising unprecedented political economy questions that to some extent have pooled national sovereignties into the supranational regional institution.

Similarly, the emergence of non-state actors has also driven new debates that questioned the extent to which state actors can exercise their sovereignty.[2] Lately, modern science and technological innovations have also prompted the conceptual development of sovereignty into question. By the end of the 1990s and early 2000s, the debate on whether a state's sovereignty is being eroded by the internet prevailed as one of the most discussed ideas in international politics. Since the 2000s, the paradigm has shifted from technological threats to statehood to the questions that revolve around sovereignty in cyberspace.[3]

Intensive digital globalization has a strong impact on states' sovereignty in the international system. Due to the increasing interconnectedness of the global system, the digital realm has become a critical domain for states, international organisations, and non-state actors to exercise power, influence, and control over the international system. The rapid growth of digital technologies has created new opportunities for economic development, communication, and innovation, but also

[1] Abid A Adonis, "Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy." *Global: Jurnal Politik Internasional,* 21(6), 2019: 262-282

[2] Juned, Mansur, et al. "Kekuatan Politik Media Sosial: Uji Kasus pada Revolusi Mesir 2011." *Global: Jurnal Politik Internasional,* 15(1), 2013: 68-83.

[3]Anggoro, Kusnanto. "Kedaulatan, Teritorialitas, dan Keamanan Pasca Westphalia." *Global: Jurnal Politik Internasional,* 6(2), 2004:1-14.

raises concerns about security, privacy, and governance.[4] As the global digital landscape continues to evolve, the concept of digital sovereignty has emerged as a central problem in international relations, and most importantly, the place of developing countries in the digital global governance.

While delving into conceptual definitions, the debate turns into an interesting discussion due to the inherent complexities in digital sovereignty. Thus, cyberspace, in which digital information is situated, is located in a non-physical territory, yet it has the potential of affecting the physical domain, and vice versa. Given this background, this paper discusses approaches to digital sovereignty and data governance with a particular focus on the dilemma of Africa's data security in the digital age. This is an important imperative because the issue revolves around statehood and its political consequences, especially as the subject of digital sovereignty raises questions on the fundamentals of a nation-state: territory (since it has no physical territory), people (whom to govern in cyberspace), and government (how to govern cyberspace).

Defining the Problem

A simplistic analysis of the current tensions between privacy and the security narrative of sovereignty prevalent in international relations indicates that states are spying on nationals and foreign citizens, and the trend is increasing as states acquire sophisticated technologies, proportional to their military power. Utilising the private sector, too, but with inherently political intents, the private sector is concerned about the experience of the user, the maximum capture of citizens' data, and how to offer the best products and services. The use of Facebook data, WhatsApp, Google, and other foreign tech firms to spy on citizens and other countries raises serious concerns about private information surveillance and their overall experience in cyberspace. Thus, despite the increasing privacy awareness and rules of data governance in some regions, especially in Europe, for example,

[4] Abid A Adonis, "Critical Engagement on Digital Sovereignty in International Relations…", p. 263.

after the entry into force of the General Data Protection Directive (GDPR), patching a broken system of systemic privacy erosion and data extractivism remains problematic.

Beyond this simplistic analysis, however, the situation is more complex in developing regions like Africa and involves an additional element that is often overlooked. The power of surveillance and the concentration of data gathered by both public and private mechanisms are focused on a small number of actors, public and private, based mainly in one jurisdiction, leading to a rapid erosion of state sovereignty. While much power is concentrated in a few centers overseeing the entire World that monitor and influence the behaviors of not just individuals, but also states. The problem is more alarming, considering how the public and private sectors are merging through joint ventures in a quest for global domination, penetrating state and citizens' movements, and mediating every connected citizen's private life through digital devices and data collection. Moreover, states' approach to the governance of their citizens' personal and non-personal data is seen as an extension of their sovereignty and an essential part of their digital sovereignty. States' approach has given states unique social, economic, and political environments, technological capabilities, domestic priorities, and digital foreign policy, indicating there is no one-size-fits-all.' Other factors, such as rising (digital) geopolitical tensions, risks of foreign government surveillance, and concerns about digital colonialism, also affect national data governance frameworks.

Conceptual and Theoretical Issues

The concept of sovereignty remains the fundamental and central theme in the analysis of international relations. The concept of state sovereignty in international relations has emerged from at least three thinkers.[5] Moreover, intensive digital globalization has had a strong impact on the sovereignty of individual states. Given the growing number of threats in the field of digital security, it becomes relevant to study the conceptual foundations of the formation of the state's digital

[5] Choucri, Nazli. *Cyberpolitics in International Relations.* (Cambridge: The MIT Press, 2012), p. 12.

sovereignty. Digital sovereignty and related concepts such as cyber sovereignty, technological sovereignty, and data governance are widely used by policymakers worldwide.[6] There is little consensus on what these concepts mean, and, indeed, they often carry very different connotations and policy consequences across different global actors. J. Westerman and V. Dhara were among the first to use the concept of digital sovereignty. Digital sovereignty is an orientation and strategic state policy that aims to reaffirm the authority of state actors over cyberspace, including over the development of digital technology. As such, this vision requires recognition of the rights of individual states to develop and use the policy instruments necessary to govern cyber activities within their legal territory.[7]

The Copenhagen School of Diplomacy defines Digital Sovereignty as the ability of states and other actors to exercise control over their digital territories, including the internet, data, and cyber-infrastructure. The concept encompasses a range of issues, such as internet governance, data privacy, cybersecurity, and e-commerce regulation.[8] The definition emphasizes that, as the global economy becomes increasingly digital, digital sovereignty has significant implications for economic development, social and cultural relations, political power, and human rights.

M.N. Dudin, S.V. Shkodinskii, and D.I. Usmanov explain digital sovereignty as the final stage of the state's digital reforms of the socio-economic system.[9] According to their approach, digital sovereignty characterizes the stability of socio-economic systems in the face of external challenges and threats, not only technological but also economic and political.

[6] Titilayo Aishat Otukoya. "The Securitization Theory." *International Journal of Science and Research Archive,* 11(1), 2024: 1747–1755.
[7] Soulé, Folashadé., *Digital Sovereignty in Africa: Moving beyond Local Data Ownership.* Policy Brief No. 185. (Centre for International Governance Innovation, June 2024.), p. 1.
[8] Dilmurad Iakhiaev et al, "Conceptual Foundations and Global Challenges in the Formation of Digital Sovereignty of the State." *Nexo: Revista Cientifica,* Vol. 36, No. 05 (Especial), 2023: 169-179/Noviembre.
[9] Dudin, M.N., Shkodinskii, S.V., Usmanov, D.I. "Digital Sovereignty of Russia: Barriers and New Development Directions." *Problemy Rynochnoi Ekonomik*i, 2, 2021: 30-49. https://doi.org/10.33051/2500-2325-2021-2-30-49

V.A. Nikonov, A.S. Voronov, V.A. Sazhina, S.V. Volodenkov, and M.V. Rybakova understand digital sovereignty as the state's independence in the use of digital technologies to realize national interests. This approach implies that the state is the main actor shaping the concept of digital transformation and the main regulator of the digitalization of economic sectors. Thus, the state determines both the level of external technological integration of solutions into domestic markets and the volume of exports of domestic innovations to foreign markets.[10] Digital reforms of the national economy are implemented with due regard to the existing technological potential and resources. Development strategies of large businesses are adjusted to align with government priorities as new players emerge in the digital space.

S. V. Volodenkov's perspective focuses on the state's ability to utilize digital technologies, i.e., the level of skills and competencies required of government entities for the effective implementation of digitalization policies, relying on their technological solutions. Consequently, Volodenkov emphasizes the lack of a shared identity of digital knowledge across scientific schools, including applied ones, under rapidly changing conditions.[11]

For Couture and Toupin, the concept assesses the degree of autonomy and security of states' digital infrastructure from external challenges and threats. Inherent in this definition is the state institution's ability to respond to existential cyber threats and attacks.[12] Posch sees the concept as the ability of the individual or the state to have full knowledge and control over who can assess one's data and where such data is transferred.[13] Gourley conceptualized digital sovereignty through

[10] Nikonov, A. V., Voronov, A. S., Sazhina, V. A., Volodenkov, S. V., Rybakova, M. V. "Sovereignty of a Modern State: Content and Structural Components Based on Expert Research." *Vestnik Tomskogo Gosudarstvennogo Universiteta,* 60, 2021: 206 - 216. https://doi.org/10.17223/1998863X/60/18

[11] Volodenkov, S.V. "The Phenomenon of Digital Sovereignty of a Modern State in the Context of Global Technological Transformations: Content and Features." *Zhurnal Politicheskikh Issledovanii,* 4, 2020: 3-11. https://doi.org/10.12737/2587-6295-2020-3-11

[12]Couture, Stephane and Toupin, Sophie. "What Does the Notion of "Sovereignty" Mean When Referring to the Digital?", *New Media and Society,* 21(10), 2019:2305-2322.

[13] Posch, Reinhard. "Digital Sovereignty and IT-Security for a Prosperous Society", in *Informatics in the Future.* (Vienna: Springer, 2006), p. 77.

Vol. 14 (Special Edition), No. 1, June 2025 p140-162 ISSN: 2315-8816
https://thecalabarhistoricaljournal.com/

a state-based lens and argued that the cyber domain must encompass the land, air, sea, and space domains in accordance with sovereign territorial principles.[14] According to Gourley, there is a distinction between the cyber domain and cyberspace. The cyber domain refers to the physical network aspects, whilst cyberspace is the field in which the cyber domain operates.

Digital sovereignty denotes the need for control over the physical layer (infrastructure, technology), the code layer (standards, rules, and design), and the data layer (ownership, flows, and use). It is motivated by different interests, such as protecting individual citizens' rights (data protection), increasing the competitiveness of domestic firms (local content requirements or other industrial policy considerations), protecting core democratic values or strategic public interests, and maintaining sovereignty in critical infrastructure and national security.[15] Based on a comparative analysis of perspectives to determine the state's digital sovereignty, we formed our perspective. Digital sovereignty refers to the state's ability to independently create, develop, and maintain the security and sustainability of the national digital infrastructure across all sectors of its geo-political and economic spheres.

Arising from the above, therefore, realism considers that the international system of states is an anarchy of states. This does not mean there is chaos; rather, the defining characteristic is the absence of an overarching authority. Moreover, states are caught in the “security dilemma,” which means they must be ever-mistrustful of other states' intentions in the global system, must rely on self-help, and are likely to arm themselves pre-emptively.[16] While contingency thinking holds that international relations between states depend on, or are contingent on, history, the evolving

[14] Gourley, Stephen K. “Cyber Sovereignty” (8-24) in *Conflict and Cooperation in Cyberspace: The Challenge to National Security.* Ed. Panayotis A. Yannakogeorgos and Adam B. Lowther. Boca Raton: Taylor and Francis, 2014.
[15] Abid A Adonis, “Critical Engagement on Digital Sovereignty in International Relations…”, p. 268.
[16] Waltz, K. N. *Theory of International Politics*. (Waveland Press, 2010), p. 337.

identities of states, and the "socialization" between states, as developed over the years and across all forms of international relations.[17]

Although the interplay of contemporary international relations and technology is not yet a systematic corpus of knowledge in Africa, let alone established principles within either political or technological innovations in their global engagements. Over time, science and technology have been treated as exogenous factors in international relations scholarship, primarily as features of warfare. Writing was on the famous *Declaration of the Independence of Cyberspace,* Barlow states, "… as governments of the Industrial World ... you have no sovereignty where we gather."[18] Hence, the emergence of "techno-politics" has grown out of science and technology and takes a two-way interplay of technology and (international) politics seriously.[19]

Thus, digital sovereignty is centered around the humanistic perspectives that relate to the international system of states. Realism, therefore, considers states as primary actors and likely takes digital humanism into account only to the extent it fits with friend-or-foe perceptions. Digital humanistic sovereignty can then very well impact alliances among like-minded states, but becomes problematic when it extends beyond them.[20] Digital humanistic sovereignty would be expected to work in particular with state-related social constructs such as law, public education, and national institutions to protect citizens' rights and national security.

In an age where power is linked to control of technology and where global challenges transcend the powers of any individual state, it is imperative to take into account international corporations, such as Big Tech, and their influence on geopolitics. Similarly, international

[17] Timmers, P." The Technological Construction of Sovereignty." In *Perspectives on Digital Humanism* (pp. 213–218). Springer, 2022. https://doi.org/10.1007/978-3-030-86144-5_28.
[18] Barlow, J. P. *A Declaration of the Independence of Cyberspace*, 1996. Electron. Front. Found. Accessed 9.13.24, from https://www.eff.org/cyberspace-independence.
[19] Eriksson, J., & Newlove-Eriksson, L. M. "Theorizing Technology and International Relations: Prevailing Perspectives and New Horizons" (pp. 3–22). In *Technology and International Relations*. Edward Elgar, 2021.
[20] Timmers, Paul, "Sovereignty in the Digital Age." (pp. 571-592). In H. Werthner et al. (eds.), *Introduction to Digital Humanism,* https://doi.org/10.1007/978-3-031-45304-5_36.

collaborations, such as civil society activism, technology community standardization, and industrial alliances, as well as multistakeholder collaborations, are of great importance. These can be meeting places for the building of common opinion and voluntary action, but can also have power, either de facto or sometimes de jure under national, regional, or international law, to manage important assets of the economy, society, justice, or democracy.

Sovereignty requires internal and external legitimacy. According to Bickerton et al., internal legitimacy is the acceptance by citizens of the government's authority. In contrast, external legitimacy is the acceptance of the state by other states in the global system. For Bickerton et al, sovereignty concerns three "assets" that need to be governed: (1) power, which is called foundational sovereignty; (2) physical and nowadays also digital assets which comprise above all territory and therefore are called territorial sovereignty; and (3) the institutional organization of economy, society, and democracy, which is called institutional sovereignty.[21]

The key notions of internal and external legitimacy map onto the foundational, territorial, and institutional forms of sovereignty. For instance, where state sovereignty concerns power arrangements, these need to be recognized both internally and externally. To be effective, the state needs authority over the organization of government and public services, and democracy needs to be an authoritative institution, for instance, with an organization to ensure free elections. "Territory" may be seen as any resources or assets that "belong to us" (i.e., not to "them"). These are of a geographic, natural, or digital origin and can also be taken to include the population, values, and culture. This territorial view requires internal and external recognition and thereby legitimacy.[22] Finally, the institutions of government need to be internally accepted, while their external legitimacy is a matter of sometimes disputed international relations, such as extraterritorial jurisdiction.

[21] Bickerton, C., Brack, N., Coman, R., and Crespy, A. "Conflicts of Sovereignty in Contemporary Europe: A Framework of Analysis." *Comparative European Politics,* 20, 2002: 257–274. https:// doi.org/10.1057/s41295-022-00269-6

[22] Klabbers, J. *International law* (3rd ed.). Cambridge University Press, 2021), pp. 106-108.

SPECIAL EDITION OF THE CALABAR HISTORICAL JOURNAL (PROCEEDINGS OF THE 4TH INTERNATIONAL MULTIDISPLINARY CONFERENCE 27TH-30TH OCTOBER, 2024)
Vol. 14 (Special Edition), No. 1, June 2025 p140-162 ISSN: 2315-8816
https://thecalabarhistoricaljournal.com/

Approaches to Data Governance

Digital governance, particularly data governance, has increasingly become an area of contention as the global digital economy's basic infrastructure has come under greater scrutiny. This has led to the alignment and realignment of major actors in the global system. Each of the actors is afraid of data colonialism – a process in which data is extracted by foreign technology firms from marginalized communities without their knowledge, for profit, and to feed their technological development. However, there is growing concern that states are seeking ways to protect citizens' data and ensure national security. Other motivations, such as spurring local innovations for economic development, have also made data governance a fundamental policy issue. Yet, approaches differ greatly amongst the global powers in contradistinction to the global south, from no control to strict data localisation. More so, a state's approach to digital sovereignty also depends on its economic and political interests, technological capabilities, national priorities, and foreign policy. Internationally, there are several interpretations of the concept of digital sovereignty, with variations across continents.

For instance, the interventionist approach engaged by the United States in the 1990s and 2000s under the pretext of liberal interventionism and the subsequent invasion of Iraq in 2003, as well as the Russian invasion of Ukraine in 2023, have raised significant questions about the concept of sovereignty in international geopolitical analysis. On digital technologies and internet governance, the liberal internationalism of the United States advocates and promotes a cyber world without borders, where information would flow freely across the world's borders without state interference. This vision has been viewed with suspicion by China, which holds that the doctrine of sovereignty should also apply in the digital space.

More recently, however, the United States's open, unregulated online practices have been viewed with unease by the United States's closest allies in Europe, Japan, Canada, and, indeed, globally. The suspicion arose from the emerging dynamics of global geopolitics following Edward

Snowden's 2014 revelations about the United States government's practices under its Cloud Act. The emphasis surveillance capitalism, whereupon the United States' hi-tech firms harvest citizens' data and monetize such data through advertising to influence the behaviour of states in the international system. The United States' laissez-faire approach to unrestricted data flows is meant to benefit its tech companies, which control the largest share of the global markets. However, under the Cloud Act, the United States maintains its sovereignty by requiring United States entities to disclose data upon request for national security purposes, regardless of location.

Meanwhile, China maintains tight control over domestic and international operations. This approach results in surveillance-oriented data regulation and strict data transfer requirements. The Chinese government has privileged access to all data originating in China and requires tech companies in China to transfer critical information to state servers. Chinese tech companies are also required to provide access to their data for national security reasons when the state submits a request through its concept of *Wanglou Zhuguan* to preserve a strong idea of state sovereignty. For China, therefore, cyber sovereignty means the right it enjoys as a state to shape its digital domains without foreign interference. Creemers persuasively argued that:

> … with territorialization, Beijing seeks to delineate its national boundaries in cyberspace, ensuring that Chinese online processes affecting important Chinese interests take place within those boundaries, and that unwanted activities are barred from entering its national space.[23]

China is also blocking major United States tech companies from emerging as local champions by providing identical services in the process of indigenization. China has established markets for its technology abroad through its digital Silk Road project. Thus, China and Russia are increasingly

[23]Creemers, R. *China's Approach to Cyber Sovereignty.* (Berlin: Konrad-Adenauer-Stiftung.2020), p. 10

adopting more proactive cyber diplomacy at international institutional engagements that align with their domestic visions vis-à-vis cyber sovereignty and state control.

In the European Union, the strategy has been to assert digital sovereignty by establishing global legal standards and promoting European technologies. The General Data Protection Regulation (GDPR)[24] is a notable example. The European strategy is designed to impose strict standards on data governance and extend the European Union's authority over data processing beyond its continental borders. The European Union focuses on individual sovereignty and emphasizes fundamental values such as human rights, press freedom, democracy, equality, the rule of law, and respect for human dignity. The European Union explicitly wants to be the leader in creating global norms and standards in the regulation and standardization of digital technologies. Globally, the European Union hopes to capitalize on the famous 'Brussels Effect', the *de facto* process of unilateral regulatory globalisation of European Union laws outside its borders through market processes. By setting these standards, the European Union encourages other regions to adopt laws similar to the GDPR.

In Latin America, early steps towards digital sovereignty were initiated in the early 2000s to replace foreign providers with local technologies. Latin American countries such as Brazil and Venezuela blazed the trail by enacting laws that established free software migration of government data in 2004.[25] Similar initiatives followed in Ecuador, Uruguay, and Bolivia. In all of these countries, the shift was accompanied by strategies to increase free software literacy among primary school children, such as the *Plan Ceibal* in Uruguay and *Canaima* in Venezuela.[26] The Latin American countries have developed sufficient human capacity to produce domestically at least part

[24] E. C, General Data Protection Regulation, (2016) OJ, L 119/1, online: www.consillium.europa.eu/en/poilicies/data-protection/data-protection-regulation Accessed 10.10.2024.
[25] Renata Ávila Pinto, "Digital Sovereignty or Digital Colonialism? - New Tensions of Privacy, Security and National Policies." *SUR 27*, 15 (27), 2018: 15 – 27.

[26] Renata Ávila Pinto, "Digital Sovereignty or Digital Colonialism..., p. 17.

of the software they need, both for local use and for export, while simultaneously investing in human capital and infrastructure development. For instance, to circumvent the United States embargo, Cuba has developed its operating system, *Nova.* Cuba did this not only because of the embargo but also as a way to control their systems. Such adoption was vital, as the country has restrictions on accessing software licenses and security updates provided by the mega providers. Similarly, Russia recently announced a full migration to free software as a way to pre-empt the impact of current and upcoming sanctions.

In Africa, African governments are also trying not to be left behind in the digital revolution, as they were in the previous three Industrial Revolutions (31Rs). Still, there is no common approach to achieving this objective, as each country designs and governs its data differently. Thus, the common concern among African countries is the lack of homegrown digital products and tools. This is complicated because cloud markets in Africa are dominated by foreign actors who host African data on servers based abroad. In the long run, African governments have little or no control over where African data is hosted or how the data is used. To this end, African leaders have expressed fears and concerns over the threats of data colonialism - a process where foreign tech companies extract African citizens' data and commercialise it without sharing the benefits with Africa. Therefore, if Africa does not spearhead how African data is governed and how data governance frameworks align with African continental development needs, then foreign actors will continue to shape and manipulate Africa's digital space.

The categorical issues inherent to digital sovereignty are cross-cutting, encompassing political, sociocultural, economic, and normative dimensions. However, these cross-cutting issues can be analyzed with an emphasis on specificity, grounded in realities on the ground and the interactions among them. There are four major issues intertwined in digital sovereignty: security-politics, economy, social and civil rights, and normative-legal imperatives. These may seem

arbitrary in their location and separation into distinct categories, as some are intersectional in their analysis. Nonetheless, the most fundamental issue in digital sovereignty rests on security-politics, which focuses on national and international security on the one hand, and on national and international politics and its implications on the other.

First, as indicated earlier, digital sovereignty became a crucial subject of discourse for nation-states in the wake of Edward Snowden and the National Security Agency (NSA) revelations, as well as amid cybercrime, terrorism, and data protection. These four variables are situated as background and contextual issues, which state actors refer to as securitized digital sovereignty. Second, each actor has varying capabilities to exercise power and define the concept of digital sovereignty in their interests. Power capabilities are diffused across private business firms (e.g., Google, Apple, Facebook, WhatsApp, Amazon), with enormous resources and activism in the digital realm against other state actors. Third, geopolitical rivalry remains a prima facie factor for states' political behaviour. Recurring antagonistic relations in the digital realm between the Western bloc against the Russia-China bloc demonstrate that geopolitical rivalry is well translated into techno-political rivalry—fourth, profit-making and economic dimension. Digital sovereignty has economic and commercial elements that enable tech companies to shift interest through a logic that often shapes the normative and legal perspectives on digital sovereignty.

However, to implement the basic principle of digital sovereignty (independence), the state needs its own digital technologies, equipment, and other solutions. Thus, it is important to emphasize systemic import substitution to increase the digital economy's independence from external supplies.[27] Also, under protectionist policies, states with low levels of digital economy and technological development would remain dependent on the progressive states. For technologically underdeveloped regions like Africa, the threat of introducing artificial restrictions is, on the one

[27] Astapenko, P. N. "Digital sovereignty as a condition for the implementation of state sovereignty in the Internet era". *Zakon i Pravo,* 9, 2022: 27-33.

hand, a mechanism to restrain the digital transformation of their economies and, on the other hand, an instrument of manipulation that has a major impact on socio-economic and political processes.[28] Therefore, ensuring data security is an element of information security in cyberspace.

Status of Africa and the Dilemma of African Data Governance

The digital acceleration attributable to COVID-19 served as an often-forgotten tale of the digital divide, acutely manifesting in Africa, where a large population lives without access to the benefits of digitization. The Continent has not been spared from the elitist technological domination of the West, bounded by the narratives of techno-solutionism. This, alongside the constant struggle for influence, power, and domination in the digital space by big technology companies, has been a risk referred to as digital colonialism.[29] While issues of digital colonialism are habitually amplified in academia, actions by African governments, either through crafted state policies or inaction alike at the regional level, have so far not inspired confidence in this new fight for technological domination of the continent.

Unremitted signatories to the 1991 African Union Convention on Cybersecurity and Data Protection, otherwise known as the *Malabo Convention,* are one such example. Perhaps therein lies hope, as the African Continental Free Trade Agreement (AfCFTA) includes a proposal for an e-commerce protocol.[30] This also raises the question: "Can the AfCFTA and/or Regional Economic Communities (RECs) help reset the balance of domination in the changing architecture of power between states and tech behemoths in the attainment of digital sovereignty in Africa"? Unfortunately, treaty adherence in Africa is marred by a deficiency in political will, as well as by multiple and overlapping memberships to trade agreements, RECs progressing at different paces,

[28] Dilmurad Iakhiaev et al, "Conceptual Foundations and Global Challenges in the Formation of Digital Sovereignty of the State." p. 170
[29] Megan Kathure, "Africa's Digital Sovereignty: Elusive or a Stark Possibility through the AfCFTA?" in *Afronomicslaw,* 2021, p. 1.
[30] Megan Kathure, "Africa's Digital Sovereignty…, p. 2.

insufficient competitiveness, economic transformation, industrialisation, and production diversification.

The African Union Digital Transformation Strategy for Africa (AUDTS), 2020-2023, has identified the need for respect for data sovereignty by localising data through Africa's Data Centre Infrastructure, designed to host missions' critical servers and computer systems. This is supported by the Program for Infrastructure Development in Africa (PIDA), which focuses on the development of regional and continental infrastructure, with an emphasis on ICT, transport, and energy. Rwanda and Kenya have taken the lead—Rwanda, for instance, through its Smart Africa Alliance program —to lead in the digital economy. Kenya is collaborating with the European Union to develop its data protection framework. Still, it seems relaxed about the need to protect its interests under the Kenya–United States Free Trade Agreement (FTA).

Generally, African governments do not have the financial resources to independently finance much of their digital infrastructure projects. Foreign actors, including China, the EU, and the US, fund many digital infrastructure projects. Hence, African states lack the political and financial capabilities to pursue an independent approach to digital sovereignty and data governance. For instance, since 2005, China has invested over USD 7.19 billion in Africa's digital infrastructure to build Africa's 3G and 4G networks and lay fiber optic network cables across Africa. The United States' big Tech companies control much of Africa's cloud computing infrastructure and dominate Africa's digital economy platforms. In the same way, too, the European Union plans to invest up to €150 billion in Africa by 2027. Thus, the digital sovereignty of African states suffers from high-tech threats, i.e., it becomes an object and a means of influence of world technological leaders, which has led to the digital colonization of underdeveloped regions.

Analysts have highlighted the threat of growing digital colonialism in Africa due to the extractive practices of US big tech companies, together with growing Chinese influence through

digital investments. Gravett argues that China's influence in Africa is giving rise to digital neo-colonialism, a term which means the application of economic and political pressure by China through technology to control and influence how African governments act.[31] Husami is of the view that any country that signs up to China's version of the internet can expose its people to the same levels of control as those exercised in China.[32] The concern is that if African governments fail to advance their values and interests with equal boldness, the 'China model' of digital governance may become the 'Africa model' by default. Interestingly, to argue that China will influence African states to adopt its approach to digital sovereignty creates an impression that African governments lack the sovereignty to make decisions for themselves and have to wait either to adopt the China or the EU model.

It is imperative to note that simply adopting an approach is not enough for a state to build a comprehensive policy that guarantees digital sovereignty over its communications. In attempting to replace either proprietary or dominant choices, governments and community initiatives are finding growing challenges to meet user expectations, in terms of both speed of delivery and quality of the user experience. Sustainability is also among the challenges, as is reaching mass adoption, unless dictated by law and a resourced public policy implementation, like in *Plan Ceibal,*[33] where the entire education system was migrated to open-source software (and hardware) development.

Sunil Abraham also identified the problem of developing technologies that consider human rights in their design, including code that cannot be restricted by copyright law or used as a tool of resistance against certain laws, which would lead to further tensions.[34] Abraham describes how

[31] Gravett, W. "Digital Neo-colonialism: The Chinese Model of Internet Sovereignty in Africa." *African Human Rights Law Journal,* 20 (1), 2020: 125-146.
[32] Husami, K. *China Splinternet, Is it a State-Controlled Alternative Cyberspace?* (London: Inside Telecom, 2022), p. 78.
[33] Renata Ávila Pinto, "Digital Sovereignty or Digital Colonialism..., p. 21.
[34] Sunil Abraham, "The Fight for Digital Sovereignty." *Economic and Political Weekly,* XLVIII, 42, (October 19, 2013), p. 3

"code could be used to resist regulation through law, thereby converting both the software and hardware layers of devices and networks into a battleground for sovereignty between the free software hacker and the state.

More so, as people gain access to the most sophisticated personal technology globally, access to a new generation of developers and creators is emerging. The next generation of technologies, produced outside the tech giants, might bring solutions to current challenges, insofar as they are designed, developed, and distributed taking into consideration a different set of values, societal behaviours, and dynamics. However, such creative power might be blocked if the current direction of technology architecture restricts creativity rather than enabling it, encourages consumption, and centralizes unregulated power.

Once technological autonomy is achieved, individuals and communities can develop their principles in ways they choose to communicate them. According to Tania Wolfgram, when considering the urgent need for indigenous people to develop their own ICT policy, "...the deliberate replacement of local technologies with Eurocentric values-laden, profit-driven technologies has been part of the colonising agenda for many centuries."[35] Therefore, constant innovation plays a key role in resisting and defeating technological domination. Thinking beyond the market is something that developed nations are already doing. As Francesca Bria submits:

> Alternative forms of public and common ownership for platforms will help to create a more democratic economy, transcending the logic of market-based, rent-seeking, privatised network systems. Too often, this leads to decisions based on short-termism, value extraction, and the appropriation of common resources for private gain. A much longer-term approach to technology, the economy, and politics is required, in which public resources and assets are owned, managed, and distributed for the collective good. This task is about building the Twenty-first-century democracy.[36]

[35] Tania Wolfgram, Re-Claiming our Technological Sovereignty, *Planet Maori,* 2015.
[36] Francisca Bria, *Public Policy for Digital Sovereignty.* (New York: OR Books, 2015), p. 23

For low-income countries and developing regions like Africa that are still struggling to catch up and realize the potential of new technologies, and at the same time to avoid violations of their citizens' rights, some options need to be deployed with urgency. Most of these options are part of medium- and long-term national and regional commitments at multiple layers and involve fluid collaboration among governments, citizens, and national companies.

At the constitutional level, countries must ensure that they innovate the ability to legislate and regulate emerging technologies and their impact on the fundamental rights of their citizens. Existing laws should be amended so as not to permit the executive's engagement in international commitments that would strip the government of its ability to enforce rights domestically. Enabling laws should also guarantee that the state exercises autonomy and control over critical technology infrastructures and key positions in important assets and industries.

In parallel, it is necessary to develop a state-funded strategy for digital sovereignty. This should cover all aspects, including modifying the curricula to develop the human resources needed for the next 50 years; investing heavily in funding research and development initiatives so that local experiments can be conducted; taking into consideration the specific needs, skills, and vision of each country; and proactively investing resources in social applications of technology. The exchange of skills, information, and research within the Global South could be encouraged and funded.

In the meantime, the simple regulation of open standards, free software, openly available hardware, and transparency of algorithms could be developed, at least for state purchases and practices. Achieving equal rights for all and effective remedies against mass surveillance for citizens in the Global South will only be achieved with funded, long-term, and comprehensive changes in policy, technology, and politics towards autonomy and sovereignty. This will gradually enable a

culture of digital dignity with human rights standards embedded in protocols at the regional and international levels.

Conclusion

The paper examined the complexities of applying the concept of digital sovereignty in international relations in the digital era. It questioned the rationale for the concentration of global power in a few centers and the merger of public and private mechanisms in the quest for global domination. It indicated its various perspectives and the categorical issues inherent in the concept. The various approaches to digital sovereignty in global geopolitical security dynamics and the dilemma of African data security were also analyzed based on humanistic realist considerations. However, global leaders, especially those advocating for equality and social justice, must be aware of the dangers that rapid digital commodification poses to vulnerable people around the world and of its impact on human rights and dignity.

In addressing global digital inequalities and embracing a future that places digital autonomy and human dignity at its core, social innovation should be encouraged and institutionalized at the community and citizen levels to ensure data security and foster socio-economic development. Interestingly, homegrown and autonomous/linguistic technologies should be encouraged to develop digital content to preserve and export their cultures to the digital domain. Perhaps it could be an opportunity to rescue and develop new local knowledge, firmly rooted in the local decentralized digital commons logic, as a strategic mechanism to defeat digital colonialism.

Bibliography

Abraham, S. "The Fight for Digital Sovereignty." *Economic and Political Weekly,* XLVIII, 42, (October 19, 2013).

Adonis, A. A. "Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy." *Global: Jurnal Politik Internasional,* 21(6), 2019: 262-282.

Anggoro, K. "Kedaulatan, Teritorialitas, dan Keamanan Pasca-Westphalia." *Global: Jurnal Politik Internasional,* 6(2), 2004:1-14.

Astapenko, P. N. "Digital sovereignty as a condition for the implementation of state sovereignty in the Internet era". *Zakon i Pravo,* 9, 2022: 27-33.

Barlow, J. P. *A Declaration of the Independence of Cyberspace*, 1996. Electron. Front. Found. Accessed 9.13.24. https://www.eff.org/cyberspace-independence.

Bickerton, C., Brack, N., Coman, R., and Crespy, A. "Conflicts of Sovereignty in Contemporary Europe: A Framework of Analysis." *Comparative European Politics,* 20, 2002: 257–274. https:// doi.org/10.1057/s41295-022-00269-6.

Bria, F. *Public Policy for Digital Sovereignty.* (New York: OR Books, 2015).

Choucri, Nazli. *Cyberpolitics in International Relations.* (Cambridge: The MIT Press, 2012).

Couture, Stephane and Toupin, Sophie. "What Does the Notion of "Sovereignty" Mean When Referring to the Digital?", *New Media and Society,* 21(10), 2019:2305-2322.

Creemers, R. *China's Approach to Cyber Sovereignty.* (Berlin: Konrad-Adenauer-Stiftung.2020).

Dilmurad Iakhiaev et al, "Conceptual Foundations and Global Challenges in the Formation of Digital Sovereignty of the State." *Nexo: Revista Cientifica,* Vol. 36, No. 05 (Especial), 2023: 169-179/Noviembre.

Dudin, M.N., Shkodinskii, S.V., Usmanov, D.I. "Digital Sovereignty of Russia: Barriers and New Development Directions." *Problemy Rynochnoi Ekonomik*i, 2, 2021: 30-49. https://doi.org/10.33051/2500-2325-2021-2-30-49.

EC. General Data Protection Regulation, (2016) OJ, L 119/1, online: www.consillium.europa.eu/en/poilicies/data-protection/data-protection-regulation Accessed 10.10.2024.

Eriksson, J., & Newlove-Eriksson, L. M. "Theorizing Technology and International Relations: Prevailing Perspectives and New Horizons" (pp. 3–22). In *Technology and International Relations*. Edward Elgar, 2021.

Gourley, Stephen K. "Cyber Sovereignty" (8-24) in *Conflict and Cooperation in Cyberspace: The Challenge to National Security e*dited by. Panayotis A. Yannakogeorgos and Adam B. Lowther. (Boca Raton: Taylor and Francis, 2014).

Gravett, W. "Digital Neo-colonialism: The Chinese Model of Internet Sovereignty in Africa." *African Human Rights Law Journal,* 20(1), 2020: 125-146.

Husami, K. *China Splinternet, Is it a State-Controlled Alternative Cyberspace?* (London: Inside Telecom, 2022).

Juned, M. et al. "Kekuatan Politik Media Sosial: Uji Kasus pada Revolusi Mesir 2011." *Global: Jurnal Politik Internasional,* 15(1), 2013: 68-83.

Kathure, M. "Africa's Digital Sovereignty: Elusive or a Stark Possibility through the AfCFTA?" in *Afronomicslaw,* 2021.

Klabbers, J. *International law* (3rd ed.). (Cambridge: Cambridge University Press, 2021).

Nikonov, A. V., Voronov, A. S., Sazhina, V. A., Volodenkov, S. V., Rybakova, M. V. "Sovereignty of a Modern State: Content and Structural Components Based on Expert Research." *Vestnik Tomskogo Gosudarstvennogo Universiteta,* 60, 2021: 206 - 216. https://doi.org/10.17223/1998863X/60/18.

Otokoya, T. A. "The Securitization Theory." *International Journal of Science and Research Archive,* 11(1), 2024: 1747–1755.

Posch, R. "Digital Sovereignty and IT-Security for a Prosperous Society", in *Informatics in the Future.* (Vienna: Springer, 2006): 60-81.

Renata, Á. P. "Digital Sovereignty or Digital Colonialism? - New Tensions of Privacy, Security and National Policies." *SUR 27*, 15 (27), 2018: 15 – 27.

Soulé, F. *Digital Sovereignty in Africa: Moving beyond Local Data Ownership.* Policy Brief No. 185. (Centre for International Governance Innovation, June 2024).

Tania Wolfgram, Re-Claiming our Technological Sovereignty, *Planet Maori,* 2015.

Timmers, P." The Technological Construction of Sovereignty." In *Perspectives on Digital Humanism* (pp. 213–218). Springer, 2022. https://doi.org/10.1007/978-3-030-86144-5_28.

---------- "Sovereignty in the Digital Age." (pp. 571-592). In H. Werthner et al. (eds.), *Introduction to Digital Humanism,* https://doi.org/10.1007/978-3-031-45304-5_36.

Volodenkov, S. V. "The Phenomenon of Digital Sovereignty of a Modern State in the Context of Global Technological Transformations: Content and Features." *Zhurnal Politicheskikh Issledovanii,* 4, 2020: 3-11. https://doi.org/10.12737/2587-6295-2020-3-11.

Waltz, K. N. *Theory of International Politics*. (New York: Waveland Press, 2010).