OCTOBER 2025

POLICY PAPER

# DIGITAL SOVEREIGNTY AND DATA COLONIALISM: SHAPING A JUST DIGITAL ORDER FOR THE GLOBAL SOUTH

MARCUS VINÍCIUS DE FREITAS

POLICY CENTER FOR THE NEW SOUTH

PP - 38/25

POLICY CENTER FOR THE NEW SOUTH

*This policy paper examines digital colonialism as a defining structural challenge of the twenty-first century and argues for the urgent pursuit of digital sovereignty in the Global South. While digitalization holds immense potential to foster inclusion and bridge development gaps, current dynamics reproduce historical patterns of dependency: data is extracted from Southern populations, routed through infrastructures owned by Northern corporations, processed by algorithms trained on foreign datasets, and monetized abroad. These asymmetries in infrastructure, knowledge, and economic power entrench global hierarchies, undermining sovereignty and perpetuating inequality.*

*The analysis situates digital dependency within broader theoretical frameworks, including dependency theory and surveillance capitalism, showing how informational empires now shape behavior, politics, and markets in ways that compromise autonomy. Case studies from Africa, Latin America, Asia, and the Middle East illustrate both vulnerabilities and opportunities—from Kenya's M-Pesa and Brazil's PIX to India's UPI and South Africa's POPIA.*

*The paper concludes by advancing a normative agenda for a just digital order, centered on regional cooperation and investment in indigenous infrastructures. It highlights the need to safeguard community data rights and proposes the convening of a Digital Bandung as crucial steps in the journey of the Global South from digital consumer to digital co-author. Taken together, they will help ensure dignity, autonomy, and multipolarity in the digital age.*

**MARCUS VINÍCIUS DE FREITAS**

## Introduction

The twenty-first century is increasingly defined by the immaterial, the intangible, and the invisible. Unlike the industrial age—when steel, oil, and railways set the tempo of nations—today's era is driven by flows of data, algorithms, and artificial intelligence. Digitalization is not only transforming economies; it is also redefining sovereignty, reshaping power dynamics, and generating new forms of interdependence.

For the Global South, the digital era embodies both promise and peril. Its promise lies in the potential to bridge developmental gaps and to include previously marginalized populations. Its peril lies in the reproduction of colonial hierarchies, as the digital order siphons resources, concentrates wealth, and entrenches dependence.

This tension crystallizes in the central paradox of our time: while digital technology promises democratization and decentralization, the lived reality has been one of radical concentration. A handful of corporations—predominantly from the United States and, increasingly, China—control the infrastructures of the digital economy. The outcome, described by scholars as data colonialism, is the extraction of personal, communal, and societal data from the Global South without fair return, creating a new form of asymmetrical dependency that echoes the colonial past.

This Policy Paper contends that the Global South should not accept such asymmetry. The fight for digital sovereignty—the ability to control, govern, and utilize digital infrastructures and data in accordance with one's own needs and values—is as crucial in the twenty-first century as the struggles for political independence were in the twentieth. A just digital order requires more than resistance to exploitation: it demands the proactive construction of alternatives—regional data governance frameworks, open-source technological stacks, and shared innovation—pursued through sustained cooperation and normative creativity. To grasp the full significance of this struggle, one must acknowledge its profound parallels with the colonial past.

## From Colonialism to Digital Colonialism

History provides sobering lessons. Classical colonialism rested on the extraction of natural resources—such as gold, silver, spices, and rubber—from Africa, Asia, and Latin America. These resources were shipped to European metropoles, fueling industrialization and wealth accumulation. Today, the extracted resource is data: the behavioral traces, communications, and personal information of billions of users. As with raw materials in the past, data is appropriated with little or no compensation for the societies that produce it. It is monetized abroad, with limited reinvestment in local societies. This is not merely a historical echo, but a pressing issue of our time.

Colonial powers imposed physical infrastructure—railways, ports, and plantations—designed primarily to serve export economies and the needs of the colonizing metropole. Similarly, the infrastructures of the digital age—submarine cables, cloud servers, and social media platforms—are often designed to prioritize the data-harvesting and profit-making imperatives of transnational corporations. The asymmetry is stark: while the Global South contributes a vast and growing share of the world's internet users, most of the economic benefits accrue to a handful of technology firms headquartered in the United States.

International relations theorists like John Mearsheimer warn that structural competition between great powers is inevitable. Yet today's struggle extends beyond traditional interstate rivalry: it is also a contest between corporations and nations for control of the defining strategic resource of our time—data. Unlike finite resources such as oil or gold, data is continuously generated. Its immense value, however, is realized only through concentration, processing, and algorithmic control. In this paradigm, those who monopolize the means of processing—algorithms and computing power—effectively monopolize future innovation and influence.

This dynamic has been theorized as data colonialism, in which the logics of extraction in the digital age reproduce imperial practices of the past.[1] Closely linked is the notion of surveillance capitalism, which describes how behavioral surplus is monetized to predict and shape human behavior.[2] Together, these dynamics underscore a disturbing reality: digital colonialism is not a metaphor. It is a structural phenomenon that entrenches dependencies, erodes national and individual autonomy, and perpetuates the very global inequalities that formal decolonization was meant to abolish.

## The Global South and the Digital Divide

The digital asymmetry experienced by the Global South is a complex issue that unfolds across three interconnected dimensions: infrastructure, knowledge, and economic power. These dimensions are mutually reinforcing, creating a web of digital inequality.

First, **infrastructural dependency**. The physical architecture of the internet—submarine cables, data centers, and cloud servers—is largely owned and controlled by corporations headquartered in the Global North. This creates neocolonial pathways for data; for instance, internet traffic between two African nations is often routed through European exchange points, introducing latency, costs, and vulnerabilities to external surveillance. Similarly, Latin America's reliance on foreign-owned platforms for commerce and finance mirrors the dependency of colonial economies on external shipping lanes and financial capital.

Second, **epistemic injustice**. Artificial intelligence systems that increasingly shape digital life are trained predominantly on datasets generated in the Global North. These datasets embed specific cultural values and biases, producing algorithmic discrimination that systematically disadvantages much of the world's population. The effects are tangible: voice recognition systems that fail to process diverse accents, facial analysis technologies that misidentify non-white features, and recommendation algorithms that erode local cultures. This constitutes a new hierarchy of knowledge, where the Global South is once again defined by, and subjected to, a foreign epistemological framework.

Third, **economic extraction**. The vast user bases of the Global South generate significant revenue, yet this wealth flows overwhelmingly to a small cluster of corporations in the North. Digital advertising spending in cities like Lagos, Nairobi, and Jakarta ultimately enriches shareholders in Silicon Valley, while local economies struggle to capture value through taxation or homegrown innovation. This creates a persistent net outflow of capital, establishing a 21st-century economic

1. See, Couldry, Nick and Mejias, Ulises A., The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism (Stanford, CA: Stanford University Press, 2019).

2. See, Zuboff, Shoshana, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (New York: PublicAffairs, 2019).

dependency that functions as a form of digital colonialism.

Despite these stark asymmetries, emergent counter-currents offer pathways toward sovereignty. Africa's pioneering success with mobile money, epitomized by Kenya's M-Pesa, demonstrates the potential of context-specific innovation. By bypassing traditional Northern-dominated financial infrastructures, it provides a model for the Global South to assert digital sovereignty. In Latin America, countries are developing regional data protection frameworks—drawing inspiration from the General Data Protection Regulation (GDPR)[3]—to safeguard digital rights and resist unchecked data extraction. Even China's investments in African digital infrastructure highlight the potential of alternative alliances and South-South cooperation to recalibrate, if not yet fully dismantle, the entrenched power dynamics of the digital age.

## The Case for Digital Sovereignty

Digital sovereignty has emerged as a critical objective for nations worldwide. It can be defined as the capacity of a state—or a collective of states—to control its digital infrastructure, govern data flows within its jurisdiction, and establish technological governance norms aligned with its own legal, cultural, and strategic interests.

For many nations, digital sovereignty is not a regulatory luxury but a strategic necessity. The European Union, with its pioneering regulations like the GDPR, has set a precedent. Yet for the Global South, the imperative is both broader and more fundamental. It requires actively reducing external dependencies by investing in local data centers and digital public infrastructure, fostering indigenous technological platforms, and negotiating from a position of strength to secure equitable terms of engagement with global tech corporations.

Digital sovereignty, however, is not about isolationism or autarky. The objective for the Global South is not to disconnect from global networks but to engage with them on its own terms. This may involve negotiating data-sharing agreements that respect local laws and cultural norms, or developing homegrown platforms that serve local needs. The principle is one of mutual benefit and conscious choice, rather than imposed dependency. In this sense, digital sovereignty represents a pursuit of strategic autonomy in the digital realm, a goal that closely parallels historical quests for energy or food security.

Furthermore, the principle of digital sovereignty extends beyond the state to the community level, fostering a sense of empowerment. A compelling case exists for community data sovereignty. Indigenous peoples and local communities, for instance, argue that data generated from their knowledge, territories, and cultural practices is a vital resource that must not be extracted without their free, prior, and informed consent. This perspective aligns with and strengthens the broader critique of digital colonialism, asserting a fundamental right—that those who generate data must retain agency over its use and benefit from its value.

3. The European Union has been a pioneer in articulating digital sovereignty, most notably through the General Data Protection Regulation (GDPR), which enshrines data protection as a fundamental right. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), Official Journal of the European Union L119 (May 4, 2016): 1–88.

## Surveillance Capitalism and Informational Empires

The unprecedented concentration of wealth and influence wielded by a handful of digital corporations has led many analysts to dub them the new empires of the 21st century.[4] Whereas historic empires expanded across continents with armies, flags, and treaties, these new empires expand invisibly through algorithms, platforms, and predictive analytics. They command no navies, yet their capacity to monitor, influence, and shape human behavior is arguably more formidable than that of the territorial empires they succeed.

The term surveillance capitalism encapsulates this dynamic: a business model pioneered by corporations like Google, Meta, and Amazon, which accumulate the so-called behavioral surplus—the exhaustive data trails of our daily lives. This "behavioral surplus" refers to the data beyond what is needed for the service provided, which is then used for other purposes. Unlike industrial capitalism, which extracted raw materials from the earth, surveillance capitalism extracts raw human experience, commodifying and monetizing it. This behavioral data is not a mere by-product; it is the central resource and primary source of profit in the digital economy.

The insidious power of this new empire lies in its disguise. It operates under the appealing guise of convenience and complimentary services. Users willingly, often unknowingly, surrender their data in exchange for connectivity, unaware that their personal information is the actual commodity being sold. Every Google search, Facebook/Instagram like, and Amazon purchase is harvested, analyzed, and used to fuel a vast predictive marketplace—a system where companies use collected data to predict and influence future actions and decisions. In this light, the "free" digital economy is, in fact, the most expensive in history, as its currency is the very essence of human autonomy: our private choices, preferences, and identities. This calls for a cautious and vigilant approach to digital interactions.Bas du formulaire

The consequences are profound and extend far beyond targeted advertising. Surveillance capitalism does not merely predict behavior; it is engineered to shape and modify it. Recommendation engines dictate what we watch and buy, while social media algorithms influence what we believe. The capacity for political manipulation was starkly revealed in the Cambridge Analytica scandal, which demonstrated how voter sentiment could be exploited and democratic processes subverted through the weaponization of personal data in elections from the United States to Kenya.[5]

For the Global South, the implications are particularly grave. Populations with minimal regulatory protection are uniquely vulnerable to data exploitation and algorithmic manipulation. Governments lacking the technical capacity to oversee these complex systems risk becoming dependent on the very corporations whose interests are fundamentally misaligned with national sovereignty and public welfare. In this way, surveillance capitalism functions as a potent form of informational imperialism, where external actors can exert profound influence over domestic affairs without a

4. Google, Facebook, and Amazon are often described as infrastructural monopolies, exercising power akin to that of empires by shaping communication, commerce, and governance at a global scale. See, van Dijck, José, Poell, Thomas, and de Waal, Martijn, The Platform Society: Public Values in a Connective World (Oxford: Oxford University Press, 2018), 3–7.

5.The Cambridge Analytica scandal brought to light the unauthorized harvesting of personal data from millions of Facebook users. This data was then used to create psychographic profiles for targeted political advertising, a manipulation that was linked to the 2016 U.S. presidential election, the Brexit referendum, and elections in countries such as Kenya. The widespread implications of this scandal underscore how digital tools can be weaponized to distort democratic processes. See Cadwalladr, Carole and Graham-Harrison, Emma, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," The Guardian, March 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

single soldier crossing a border—through the control and manipulation of information and data.

The analogy to a historical empire is thus more than a mere metaphor. Just as European powers extracted natural resources from colonies under the guise of a civilizing mission, digital empires extract data under the banner of connectivity and progress. Similarly, while empires imposed foreign legal and administrative institutions, digital empires impose proprietary algorithmic architectures that govern social and economic life. The crucial difference lies in visibility: where imperial soldiers marched under identifiable flags, digital corporations operate under sleek brands—symbols no less potent in commanding global allegiance.

This new empire is also far more difficult to resist. Historic imperialism could be challenged through military force, popular resistance, and the renegotiating of treaties. But how does one resist an empire woven into the fabric of daily life? To relinquish these platforms often entails facing social and economic isolation, as connectivity has become essential for modern existence. The empire of surveillance capitalism is therefore totalizing, penetrating every sphere of life—from the most personal to the overtly political.

This reality raises a critical question for the Global South: can genuine digital sovereignty be achieved when these informational empires dominate the very infrastructures of daily life? The answer depends on the arduous but essential task of developing alternative platforms, negotiating from a position of collective strength, and building robust coalitions to challenge monopolistic control. The task is daunting, yet necessary if autonomy and self-determination are to hold meaning in the digital age. The emergence of alternative platforms provides a ray of hope in this struggle.

## The Digital Divide in the Global South

While surveillance capitalism is a global phenomenon, its impact is uneven. The Global South is particularly vulnerable due to the persistence of the digital divide—a complex constellation of inequalities in infrastructure, knowledge, economics, and governance—that reinforces dependency.

## Infrastructure Asymmetry

Surveillance capitalism, while global in scope, disproportionately affects the Global South due to the persistence and complexity of the digital divide. This divide is not a singular gap but a constellation of structural inequalities—in infrastructure, knowledge, economic power, and governance—that reinforce dependency and impede digital sovereignty. Addressing these inequalities is urgent.

The backbone of the digital economy—the physical infrastructure—rests on global cooperation. Submarine cables, data centers, cloud storage facilities, and satellite constellations underpin digital connectivity, yet the Global South remains structurally dependent on infrastructure controlled by entities in the Global North. A stark example is Africa, where an estimated 80% of intra-continental internet traffic is routed through servers in Europe,[6] introducing latency, higher costs, and critical vulnerabilities to surveillance and data interception.

Similarly, Latin America's digital connectivity exhibits structural dependence on hub cities such as

6. See, United Nations Conference on Trade and Development (UNCTAD), Digital Economy Report 2019: Value Creation and Capture—Implications for Developing Countries (New York: United Nations, 2019), 98–100.

Miami and São Paulo. These hubs, often reliant on foreign-owned infrastructure, centralize control over the region's digital architecture.[7]

Ownership of this core infrastructure is highly concentrated. Tech giants such as Google, Meta, and Amazon, have increasingly financed and deployed private undersea cables, effectively privatizing what is, in essence, a global public good. While these investments expand raw connectivity, they also entrench a neo-colonial dependency: access to the global digital economy becomes contingent on the commercial and strategic interests of a few corporations, directly challenging the regulatory sovereignty of states.

This dynamic mirrors the logic of historical colonial infrastructure. Empires built railways and ports not to develop colonies internally, but to efficiently extract raw materials for export. Similarly, today's digital infrastructures are often optimized to channel data from the Global South to Northern data centers, rather than fostering regional integration. The result is a 21st-century dependency that perpetuates longstanding asymmetries of power and wealth.

## Knowledge Asymmetry

Digital colonialism extends beyond physical infrastructure to the very architecture of knowledge. Artificial intelligence systems that increasingly govern digital life are overwhelmingly trained on datasets collected and annotated within the Global North.

To foster inclusivity, these datasets must be diversified to reflect the realities of the Global South. Current datasets embed cultural, linguistic, and racial biases that systematically marginalize the realities of the Global South. The consequences are tangible: voice recognition technologies misinterpret diverse accents, facial analysis systems exhibit higher error rates for darker skin tones, and content moderation policies on global platforms often enforce Anglo-American cultural norms, sidelining local knowledge and expression.

This epistemic injustice generates a new form of dependency: the Global South is relegated to a consumer of technologies built on assumptions it had no role in shaping. Mirroring colonial education systems that imposed European epistemologies and erased indigenous knowledge, modern algorithmic systems establish hierarchies of knowledge that privilege Northern perspectives and data.

The implications are profound and material. When biased algorithms determine creditworthiness, identify policing targets, curate news feeds, or rank search results, epistemic bias translates directly into concrete economic and social harm.

Communities are systematically excluded, misrepresented, and marginalized by systems they

7. Miami has long served as the primary digital gateway for Latin America, hosting the Network Access Point of the Americas (NAP of the Americas) and terminating multiple submarine cables linking the region to global markets, which are largely financed and operated by U.S. telecommunications carriers. See, TeleGeography, Submarine Cable Map, accessed May 2024, https://www.submarinecablemap.com/; and Hivelocity, "Miami: Gateway to Latin America's High-Speed Connectivity," Hivelocity Blog, April 12, 2023, https://www.hivelocity.net/blog/miami-gateway-to-latin-americas-high-speed-connectivity/. São Paulo, meanwhile, hosts IX.br São Paulo, the largest internet exchange point in the Southern Hemisphere, and serves as the main traffic hub for Brazil and neighboring countries. While nationally operated, it remains integrated into foreign-owned submarine cable systems such as Seabras-1—a private U.S.-owned cable connecting Brazil to New York. See, NIC.br, "IX.br São Paulo," Núcleo de Informação e Coordenação do Ponto BR, accessed May 2024, https://ix.br/; and Seaborn Networks, "Seabras-1 Subsea Cable," accessed May 2024, https://seabornnetworks.com/.

neither designed nor fully understand, often lacking the technical or legal capacity to contest them. Achieving digital sovereignty therefore requires not only control over cables and data centers but also meaningful participation in the creation of the algorithms and datasets that constitute the world's digital knowledge base.

## Economic Asymmetry

The economic dimension of the digital divide reveals a stark neocolonial dynamic. Despite contributing a massive and growing user base, the lion's share of revenue generated from digital activity in the Global South flows to multinational corporations headquartered in the North. Advertising spending in São Paulo enriches shareholders in Silicon Valley; e-commerce transactions in Rabat swell profits in Seattle boardrooms; and mobile payments in Jakarta are facilitated by platforms that extract value through fees and data monetization, with minimal reinvestment in local economies.

This system generates a persistent net outflow of capital and wealth. The Global South supplies the raw materials—users and their data—while the high-value products and profits accrue abroad. This environment stifles local innovation: domestic startups and tech firms struggle to compete with the vast economies of scale, network effects, and pre-existing data troves of established global giants. Governments also face significant hurdles in capturing fiscal value through taxation, as digital corporations adeptly exploit regulatory arbitrage and shift profits to low-tax jurisdictions.

This core-periphery dynamic, while disheartening, also presents an opening for change. It is a digital-age echo of the dependency theory articulated by economists such as Raúl Prebisch and Fernando Henrique Cardoso.[8] The periphery (the Global South) exports raw, unrefined data—the primary commodity—while the core (the Global North) processes it, develops proprietary algorithms and services, and re-exports these finished digital products back to the periphery at high margins. The promise of the digital economy as a great democratizer has thus been broken; yet, with concerted effort, it can still be recalibrated to overcome entrenched patterns of global inequality.

## Political and Governance Asymmetry

The most consequential aspect of the digital divide may be its political dimension. The foundational rules, standards, and norms of the global digital order are predominantly crafted in power centers like Washington and Brussels, while the voices and interests of the Global South remain largely marginalized in key international forums. Institutions governing critical internet resources, such as the Internet Corporation for Assigned Names and Numbers (ICANN), and standard-setting bodies like the International Telecommunication Union (ITU), continue to be disproportionately shaped by Northern governments and corporate interests. As a result, global standards for cybersecurity, data governance, and artificial intelligence are being established with insufficient input from the Global South, reflecting neither its needs nor its values.

The outcome is a profound governance asymmetry that starkly mirrors the political subordination of the colonial era. Digital sovereignty is fundamentally compromised when the regulatory frameworks

8. Dependency theory, initially formulated in the mid-20th century, argued that the global economy is structured in a way that locks developing countries (the "periphery") into unequal relationships with developed nations (the "core"), leading to chronic underdevelopment. See, Prebisch, Raúl, The Economic Development of Latin America and Its Principal Problems (New York: United Nations, 1950); Cardoso, Fernando Henrique and Faletto, Enzo, Dependency and Development in Latin America (Berkeley: University of California Press, 1979).

governing a nation's digital life are authored elsewhere.

Without meaningful representation and agency in global digital governance, the nations of the Global South risk remaining perpetual rule-takers rather than rule-makers. This enforced passivity not only undermines policy autonomy but also entrenches a new generation of structural dependency, threatening to extend digital subordination for decades to come.

## The Quest for Digital Sovereignty

Classically, sovereignty has been defined by territorial control, a monopoly on the legitimate use of force, and recognized political authority within defined borders. In the twenty-first century, however, this concept is being fundamentally challenged in domains where territory is irrelevant and boundaries are porous.

Digital sovereignty represents a modern extension of this principle: the ability of a state or region to control its digital infrastructure, regulate data flows within its jurisdiction, and govern platforms in accordance with its own laws, values, and national interests—not merely the capacity to exclude foreign military forces.

The European Union has been a pioneer in articulating this concept, most notably through the General Data Protection Regulation (GDPR),[9] which enshrines data protection as a fundamental human right. The GDPR, with its stringent data protection rules and hefty penalties for non-compliance, exemplifies the EU's commitment to digital sovereignty.

For the Global South, however, the imperatives are both broader and more foundational. For nations grappling with persistent developmental challenges, institutional weaknesses, and limited resources, digital sovereignty extends far beyond individual privacy; it is a prerequisite for national agency and survival. Without the capacity to govern their digital ecosystems, these countries risk permanent subordination within the global digital hierarchy.

This pursuit of sovereignty encompasses at least four critical dimensions: infrastructural sovereignty, data sovereignty, regulatory and governance sovereignty, and cultural and epistemic sovereignty. Each of these dimensions is indispensable to a nation's ability to control its digital destiny.

**1. Infrastructural Sovereignty:** This refers to ownership and control over the physical backbone of the digital world—submarine cables, data centers, satellite networks, and cloud computing services. These assets determine the terms of access, pricing, and security. Without infrastructural sovereignty, nations remain dependent on external providers, thereby replicating the dependency dynamics of the colonial era.

**2. Data Sovereignty:** This is the capacity of a nation to assert legal and technical control over data generated within its jurisdiction—dictating how it is collected, stored, processed, and transferred. Achieving this requires not only robust legislation but also the technical capacity to enforce it.

9 The GDPR, adopted in 2016 and enforced from May 2018, represents a landmark regulation that not only harmonizes data protection across EU member states but also affirms privacy and data protection as fundamental rights under Article 8 of the Charter of Fundamental Rights of the European Union. See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Official Journal of the European Union L119 (May 4, 2016): 1–88.

Crucially, it ensures that the value derived from citizen data benefits the local economy.

**3. Regulatory and Governance Sovereignty:** This is the ability to participate meaningfully in shaping the rules, standards, and norms of the global digital order at institutions like the ITU and ICANN. It also entails the domestic authority to effectively regulate powerful foreign tech firms. Without representation and agency in these forums, the Global South risks remaining a rule-taker rather than a rule-maker.

**4. Cultural and Epistemic Sovereignty:** This dimension is about safeguarding local languages, knowledge systems, and cultural values from algorithmic erasure. It requires resisting the homogenizing force of global platforms and ensuring that artificial intelligence systems are trained on diverse datasets that reflect the full spectrum of human experience—not just Western paradigms. Digital sovereignty here becomes a vehicle for preserving cultural diversity, which is a vital component of global human knowledge.

Digital sovereignty must not be conflated with digital autarky. No nation can, nor should, seek to disconnect from the global internet. The goal is strategic autonomy: the ability to engage with global networks on fair terms, to choose partners on the basis of mutual benefit, and to ensure that digital integration advances local development priorities. In this sense, it is directly analogous to food or energy security—a matter of resilience, not isolation.

Crucially, the concept extends beyond the state to encompass community data sovereignty. Indigenous peoples and local communities around the world affirm that data concerning their traditional knowledge, territories, and cultural heritage is a collective resource that cannot be extracted without their free, prior, and informed consent. This principle resonates with postcolonial critiques, affirming a fundamental right: those who generate value must retain agency over its use and share equitably in its benefits. The urgency of community data sovereignty cannot be overstated.

**Case Studies in the Global South**

The struggle for digital sovereignty is not an abstract theory but an immediate and concrete reality. Across Africa, Latin America, Asia, and the Middle East, governments and regions are experimenting with policies, forging new partnerships, and driving innovations to reduce external dependency and assert autonomy. These case studies illustrate the complex interplay of ambition, constraint, and possibility in shaping a more just digital order.

**Africa: Ambitions and Constraints**

Africa, home to the world's youngest population and among the fastest-growing digital adoption rates, embodies both the transformative promise and the profound perils of digital modernity. Mobile technology has been a revolutionary force: Kenya's M-Pesa, launched in 2007, became a global exemplar of mobile banking, driving financial inclusion for millions and inspiring similar innovations across the continent. Today, a vibrant startup ecosystem in hubs such as Nigeria, South

Africa, and Rwanda is pioneering context-specific solutions in fintech, health tech, and agriculture.[10] Yet, these grassroots innovations coexist with deep-seated structural vulnerabilities. The African Union's ambitious Digital Transformation Strategy for Africa 2020–2030 sets out a clear vision for inclusive growth, infrastructure development, and digital rights.[11] However, the continent's digital economy remains heavily dependent on foreign-owned infrastructure. Most international bandwidth is delivered through submarine cables financed and controlled by American, European, and Chinese consortia. Crucially, an estimated 80% of Africa's internet traffic is routed and stored overseas, primarily in Europe. This not only exposes African nations to external surveillance and creates latency issues but also severely undermines their capacity to enforce data protection laws, even when such laws are in place.[12]

China's role as a primary builder of African digital infrastructure is both significant and complex. Companies such as Huawei and ZTE have constructed much of the continent's telecommunications backbone, while Chinese financing underpins critical data centers and e-government systems. These investments provide essential alternatives to Western dominance, delivering immediate gains in connectivity and accelerating development.

Yet challenges persist. Nigeria's 2021 suspension of Twitter, following a dispute over content moderation, became a flashpoint that exposed the tension between global platform power and national sovereignty.[13] Conversely, South Africa's robust Protection of Personal Information Act (POPIA) reflects growing recognition of the importance of data rights.[14] Still, the gap between legislation and enforcement remains wide: many states lack the technical expertise, financial resources, and institutional capacity needed to implement regulations effectively against powerful multinational firms.

**Latin America: Between Innovation and Dependency**

Latin America's historical struggle with dependency is now being replayed in the digital realm. The region illustrates a paradox of proactive regulation alongside deep structural vulnerability.

10. M-Pesa, introduced by Safaricom in Kenya, revolutionized access to financial services by enabling mobile money transfers without the need for traditional banking infrastructure. Its rapid growth to serve over 30 million users made it a global model for economic inclusion. The success of M-Pesa not only transformed the African financial landscape but also inspired digital entrepreneurship worldwide, with emerging innovation hubs in Lagos, Cape Town, and Kigali adapting technology to local needs in sectors from payments to agriculture. See, Mas, Ignacio and Radcliffe, Dan, "Mobile Payments Go Viral: M-Pesa in Kenya," Capco Institute's Journal of Financial Transformation 32 (2011): 169–182.

11. The African Union's Digital Transformation Strategy for Africa (2020–2030), adopted in 2020, sets out a continental framework to harness digital technologies for economic growth, job creation, and social inclusion. It emphasizes priorities such as universal access to broadband, development of digital infrastructure, digital literacy, and safeguarding digital rights. This commitment to protecting citizens' digital rights is a key aspect of the strategy, ensuring that the digital revolution benefits all. See African Union, Digital Transformation Strategy for Africa (2020–2030) (Addis Ababa: African Union Commission, 2020).

12. See, United Nations Conference on Trade and Development (UNCTAD), Digital Economy Report 2019: Value Creation and Capture—Implications for Developing Countries (New York: United Nations, 2019), 98–100.

13. In June 2021, the Nigerian government suspended Twitter after the platform removed a tweet by President Muhammadu Buhari for violating its policies. The ban, which lasted a significant seven months, severely restricted digital expression and commerce, and sparked international criticism, showing the fragile balance between national sovereignty, freedom of expression, and the dominance of global platforms over domestic digital ecosystems. See Maclean, Ruth and Satariano, Adam "Nigeria Bans Twitter After President's Tweet Is Removed," The New York Times, June 5, 2021, https://www.nytimes.com/2021/06/05/world/africa/nigeria-twitter-president.html

14. South Africa's Protection of Personal Information Act (POPIA), signed into law in 2013 and fully enforced from July 2021, is a testament to the global relevance of data privacy laws. Inspired by the European Union's GDPR, it establishes comprehensive rules on the collection, processing, and storage of personal data, affirming privacy as a constitutional right under Section 14 of the South African Constitution and imposing significant obligations on both public and private bodies. See, Republic of South Africa, Protection of Personal Information Act 4 of 2013, Government Gazette 581 (Cape Town: Government Printing Works, 2013), https://www.gov.za/documents/protection-personal-information-act.

On one hand, Brazil has emerged as a leader in digital governance: its General Law on Data Protection (Lei Geral de Proteção de Dados – LGPD) is widely recognized as one of the world's most comprehensive data protection frameworks. Mexico has launched ambitious digital inclusion programs, while Chile has invested significantly in national cybersecurity capabilities.

On the other hand, Latin America remains highly vulnerable to external digital domination. U.S. corporations control the vast majority of the region's cloud computing and data storage services. Much intra-regional internet traffic is routed through hubs in the United States, reproducing a core-periphery model that increases latency, raises costs, and creates strategic exposure to extraterritorial surveillance and control. Economically, this translates into a familiar pattern: value generated from Latin American users is extracted and repatriated abroad.

In response, the region has produced groundbreaking innovations that model digital sovereignty in action. A flagship example is Brazil's PIX instant payment system, launched by the Central Bank of Brazil in 2020.[15] Unlike private-sector models like M-Pesa, PIX is a public utility with over 140 million users. It enables real-time, low-cost digital payments, reduces reliance on international card networks, expands financial inclusion, and demonstrates how states can reclaim sovereignty by designing and controlling critical digital public infrastructure.

The path forward likely hinges on regional cooperation. Bodies such as MERCOSUR and the Community of Latin American and Caribbean States (CELAC) have explored digital market integration and shared data governance frameworks. While progress has been uneven, the strategic logic is compelling: only by pooling resources, harmonizing regulations, and negotiating as a bloc can these nations hope to counterbalance the influence of global tech giants and other powerful state actors. Without such cooperation, individual countries will remain outmaneuvered—rule-takers rather than rule-makers.

## Asia: Strategic Autonomy and Contestation

Asia presents a complex and contested digital landscape, marked by diverse strategies to assert strategic autonomy. India, with its massive population and dynamic technology sector, has emerged as both a consumer and producer of digital technologies. Its Aadhaar programme, the world's largest biometric identification system, demonstrates a formidable capacity to deploy digital tools at scale,[16] though it has also sparked significant debate over privacy and mass surveillance.

India has actively advanced data sovereignty through localization mandates requiring certain categories of data to be stored domestically. At the same time, it has successfully promoted indigenous platforms and digital public goods, most notably the Unified Payments Interface

15. PIX, introduced by the Central Bank of Brazil in November 2020, is a nationwide instant payment system enabling real-time transfers, available 24/7, and free of charge for individuals. By 2023, it had gained global recognition as one of the most widely used digital payment systems, significantly advancing financial inclusion and reducing reliance on cash transactions. See, Banco Central do Brasil, PIX: O Novo Sistema de PagamentosInstantâneos Brasileiro (Brasília: Banco Central do Brasil, 2020), https://www.bcb.gov.br/estabilidadefinanceira/pix.

16. The Aadhaar programme, launched in 2009, is the world's most extensive biometric identification system, enrolling over a billion Indians through fingerprint and iris scans. It showcases the state's formidable capacity to deploy digital tools at scale for welfare delivery, financial inclusion, and identity verification, bringing these benefits to a large population. However, it has also provoked intense debate over privacy, data security, and the potential for mass surveillance. Critics argue that Aadhaar risks enabling state overreach and exclusion, particularly where authentication failures prevent citizens from accessing essential services. See, Khera, Reetika, Impact of Aadhaar in Welfare Programmes (September 29, 2017). Available at SSRN: https://ssrn.com/abstract=3045235.

(UPI), which now facilitates billions of mobile transactions.[17] These initiatives reflect a deliberate effort to harness digitalization for national development while balancing economic openness with sovereignty.

Southeast Asia faces distinct challenges. Indonesia, for instance, has introduced regulations requiring foreign digital platforms to establish local offices and pay taxes. Vietnam has implemented data localization policies, insisting that data concerning its citizens be stored domestically. These measures reflect a growing awareness of the risks of dependency, though resource constraints and varying enforcement capabilities often complicate implementation.

China, as a leading digital power, offers a model for the Global South. Its long-standing strategy of "cyber sovereignty" explicitly emphasizes state control over digital spaces, presenting a clear alternative to the Western-led vision of an open internet. China's approach is compelling because it demonstrates that rapid digital development can occur outside Western frameworks and under state guidance. Its rise is a key driver of the emerging multipolar digital order.

## Middle East: Ambition, Wealth, and Vulnerability

The Middle East offers a perspective defined by the strategic deployment of capital. Wealthy Gulf states have invested heavily in frontier technologies such as artificial intelligence, smart cities, and next-generation digital infrastructure. The United Arab Emirates and Saudi Arabia aspire to become global digital hubs, competing to host data centers and launching ambitious projects like NEOM. These investments are central to long-term economic diversification plans and broader geopolitical ambitions.[18]

Yet, this ambition coexists with deep-seated vulnerabilities. The region's core software, platforms, and underlying technologies are largely imported. Furthermore, advanced surveillance tools are often purchased from foreign vendors, raising serious ethical questions and potential human rights risks. Political instability in other parts of the region further hampers coherent digital development.

A stark illustration is Israel's targeting of communication infrastructure in Lebanon—notably the destruction of pagers and the killing of several political agents—which epitomizes the vulnerabilities inherent in the digital domain.[19] The incident demonstrates that, without robust and independent digital ecosystems, societies are exposed to surveillance, interception, coercive manipulation, and even lethal consequences by technologically superior actors. It also shows how control over seemingly "low-tech" instruments can serve as a gateway to broader systems of digital dominance,

17. Launched in 2016 by the National Payments Corporation of India, the Unified Payments Interface (UPI) integrates multiple bank accounts and payment services into a single mobile application, enabling seamless, real-time peer-to-peer and merchant transactions. By 2023, UPI was processing over 9 billion transactions per month, a staggering figure that underscores its status as one of the largest digital payment systems globally and a key driver of India's digital financial inclusion strategy.

18. Both the UAE and Saudi Arabia have positioned digital infrastructure as a cornerstone of their economic diversification strategies. The UAE has promoted itself as a regional leader in cloud services and artificial intelligence, while Saudi Arabia's Vision 2030 includes NEOM, a $500 billion mega-project envisioned as a smart city integrating advanced digital technologies, renewable energy, and high-capacity data centers. See Ulrichsen, Kristian Coates, Saudi Arabia and the UAE: Regional Powerhouses in the Gulf (London: Routledge, 2020), 145–150; and NEOM, What Is NEOM? (Riyadh: NEOM Company, 2023), https://www.neom.com/en-us/about.

19. In September 2024, thousands of pagers and walkie-talkies used by Hezbollah members were reportedly rigged with explosives and detonated simultaneously, killing and injuring dozens, including civilians. The incident highlighted how devices once considered secure could be weaponized, exposing the fragility of digital and quasi-digital infrastructures in modern conflicts. See Laila Bassam and Maya Gebeily, "Israel Planted Explosives in Hezbollah's Taiwan-Made Pagers, Say Sources," Reuters, September 20, 2024; "Hezbollah Device Blasts: How Did Pagers and Walkie-Talkies Explode and What Do We Know About the Attacks?" The Guardian, September 19, 2024.https://www.theguardian.com/world/2024/sep/18/hezbollah-pagers-what-do-we-know-about-how-the-attack-happened

where the capacity to disrupt information flows becomes a form of modern warfare and subjugation. This dynamic mirrors the logic of digital neocolonialism: asymmetrical dependency, vulnerability to external interference, and the perpetuation of power imbalances through technological means.

Gulf states illustrate how resource wealth can be leveraged to pursue digital sovereignty. By directing capital into education, infrastructure, and home-grown innovation, they aim to reduce long-term dependency and assert greater autonomy. The critical question remains whether these investments will forge genuine, sustainable sovereignty or create a new form of dependency on external tech providers and consultants. Their success will ultimately depend on cultivating indigenous talent and robust, independent regulatory institutions.

## Towards a Just Digital Order

If the Global South is to avoid repeating the patterns of dependency that marked its colonial past, it must advance a positive agenda for digital sovereignty. Resistance to exploitation, while necessary, is insufficient. A just digital order requires proactive construction: a vision of inclusivity, fairness, accountability, and multipolarity, underpinned by institutions and policies capable of delivering dignity and autonomy in the digital age.

## Inclusivity

Inclusivity must begin with representation. The rules of the digital world are currently shaped in fora dominated by the Global North: the World Trade Organization's debates on e-commerce, ICANN, the Organization for Economic Co-operation and Development (OECD), and the G7. The Global South, though home to the majority of the world's internet users, remains marginal in these arenas. A just digital order must include mechanisms for equitable representation, ensuring that Africa, Latin America, South Asia, and the Middle East are not mere observers but active participants in the rulemaking process.

This inclusivity must also extend to populations within nations. Digital gender divides, rural-urban disparities, and socioeconomic inequalities risk deepening unless addressed through deliberate policy. Women, rural communities, and people experiencing poverty are too often excluded from the benefits of connectivity. Bridging this divide requires investment in infrastructure, digital literacy programs, and accessible platforms. Inclusivity is not a charitable gesture; it is a strategic necessity. A digital order that excludes half the population cannot be just, nor can it be sustainable.

## Fairness

Fairness requires an equitable distribution of the value generated by data. Currently, the lion's share of digital wealth is concentrated in corporations headquartered in a handful of countries. Advertising revenue in Lagos or São Paulo flows to shareholders in California. E-commerce transactions in Jakarta enrich platforms domiciled in the North. This dynamic mirrors the colonial model: raw data flows outward, and wealth is repatriated, while local economies and innovators remain underfunded.

Correcting this injustice requires tax frameworks adapted to the digital economy. The OECD's efforts to create a global digital tax represent progress, but the Global South must articulate and advocate for its own demands to ensure they are met. Regional blocs such as the African Union,

MERCOSUR, and ASEAN could coordinate digital taxation to prevent a race to the bottom. Fairness also requires reinvestment in local infrastructure, support for start-ups, and policies that ensure the benefits of digital growth are shared broadly across society.

## Accountability

Accountability is indispensable for restraining the excesses of digital empires. Just as the industrial age required antitrust laws to break up monopolies, the digital age demands robust regulation to prevent abuse. Big Tech corporations must be subject to oversight regarding competition, data protection, content moderation, and human rights. Without accountability, the empire of surveillance capitalism will continue to expand unchecked.

Accountability also requires transparency. Algorithms that shape political discourse, economic opportunity, and cultural content must be open to scrutiny. The opacity of artificial intelligence systems allows bias to persist and manipulation to flourish. A just digital order must insist on algorithmic transparency, independent audits, and enforceable rights of redress.

## Multipolarity

Finally, a just digital order must be multipolar. Unipolar dominance is incompatible with justice. Multipolarity ensures that no single actor can dictate the rules, that diverse voices are heard, and that balance is maintained. For the Global South, multipolarity provides the strategic space to negotiate, cooperate, and innovate on its own terms.

This vision is not about building digital walls but about constructing bridges on a more equitable foundation. It calls for moving from a world where the Global South is a digital colony to one where it is a sovereign architect of its own future. The task is monumental, but the alternative—a future of perpetual dependency—is untenable. The struggle for a just digital order is the defining geopolitical struggle of the twenty-first century, and one the Global South cannot afford to lose.

Multipolarity does not mean fragmentation. A Balkanized internet, divided by national firewalls, would undermine the universality of digital space. Rather, multipolarity implies pluralism within unity: recognition that different societies may choose various models of digital governance, while all participate in shaping the standard rules of interaction on a shared global internet.

The digital age thus presents a fundamental question to the Global South: will it remain a consumer of platforms and norms designed elsewhere, or will it actively participate in shaping a fairer digital order? Choosing the latter is not just a rejection of the status quo, but an empowering step toward redressing colonial-era injustices in a contemporary form. Pursuing digital sovereignty is an affirmation of dignity, autonomy, and the right to self-determined development, offering a journey that inspires hope and agency.

As Taoist philosophy reminds us, the Earth is not a failed project but a school: civilizations, like individuals, must learn, correct, and grow. The critical lesson of our age is that freedom requires sovereignty in the digital realm. Just as twentieth-century struggles for political independence dismantled colonial empires, the twenty-first-century pursuit of digital sovereignty seeks to dismantle contemporary structures of informational dependency. This journey is not solely about dismantling; it is also about growth and learning, a prospect that should fill us with optimism and hope.

Historically, bridges between civilizations—forged through cultural exchange—fertilized epochs like the Renaissance and the Enlightenment. Today, the urgent task is to bridge the digital divide through cooperation, solidarity, and imagination to build a more just and multipolar world. For the Global South, the task is daunting, but the imperative is clear: to shape, rather than be shaped by, the digital future. This is not merely a task, but a testament to the significant role the Global South plays in the digital realm—a role that should inspire a sense of value and purpose.

Only through such determined action can we ensure that digital modernity is not merely the extension of a single dominant path, but the convergence of humanity's many diverse trajectories—a future truly worthy of our collective diversity and capable of sustaining our universal dignity.

## Policy Proposals for a Just Digital Order

To translate these principles into practice, the Global South must pursue concrete initiatives.

**1. Regional Data Centers and Cloud Services.** Africa, Latin America, and South Asia must invest in regional data infrastructure that reduces their dependence on external providers. Shared facilities, supported by South-South cooperation, could enhance sovereignty, improve security, and reduce latency.

**2. Digital Literacy and Education.** Sovereignty is not merely institutional; it is also a human concept. Investing in digital literacy, coding, and data science education is crucial for building a citizenry capable of critical thinking and engagement. Without these skills, sovereignty is hollow. Children should be exposed to Artificial Intelligence as early as possible, and universities should ensure that students increase their intellectual productivity levels.

**3. South-Centered AI Training Datasets.** Artificial intelligence reflects the data on which it is trained. To prevent epistemic colonialism, the South must create vast, representative datasets that reflect its linguistic diversity, cultures, and realities. Collaborative initiatives are crucial to ensuring genuine diversity in global AI systems.

**4. Taxation and Regulation of Big Tech.** Coordinated frameworks are necessary to ensure that digital value is taxed where it is generated, rather than where it is consumed. Regional blocs could establish standard rules, preventing corporations from playing states against one another in a regulatory race to the bottom.

**5. Community Data Rights.** Recognition of collective data ownership, particularly for indigenous and marginalized communities, would prevent the exploitation of cultural and biological resources. This extends the principle of sovereignty beyond the state to the community level.

**6. A Digital Bandung.** Inspired by the Bandung Conference of 1955, which articulated a vision of solidarity among newly independent states, the Global South should convene a "Digital Bandung" to establish shared principles for digital justice. Such a declaration would affirm autonomy, cooperation, and multipolarity in the digital age.

## Conclusion: A Multipolar Digital Future

History rarely repeats itself in exact form, but it often rhymes. The struggles of the present echo those of the past. Just as the peoples of Asia, Africa, and Latin America once fought for political independence, so too must they now fight for digital sovereignty. The stakes are no less existential. Without control over data, infrastructure, and governance, political independence remains incomplete.

The challenge is immense. Digital colonialism is subtle, pervasive, and entrenched. Unlike the colonial empires of the past, which could be resisted with armies and flags, today's digital empires infiltrate daily life. To disconnect from them would mean isolation from the global economy; yet to accept their dominance would mean subordination.

The path forward lies in cooperation, imagination, and courage.

Cooperation, because no single state can confront digital empires alone; imagination, because new models must be invented rather than imported; courage, because resistance will provoke significant pressure.

Civilizations across history have contributed distinctive visions of harmony, justice, and dignity. Confucianism speaks of harmony without uniformity; African Ubuntu affirms that one's humanity is realized through the humanity of others; Latin America's legacy of solidarity emphasizes emancipation from dependency; Western humanism highlights the dignity of the individual. These traditions are not mutually exclusive. Together, they provide a pluralist foundation for a digital modernity that is neither hegemonic nor monolithic, but genuinely multipolar.

A just digital order will not emerge spontaneously. It must be built through deliberate policies, regional integration, and international advocacy. The Global South must not be a passive consumer in a world designed elsewhere. It must be a co-author of the future.

The experience of Brazil during the Trump administration—when sudden tariff announcements were coupled with the implicit threat of suspension from GPS, social media networks, and e-commerce platforms—revealed the dangers of technological dependency. The collective fear across business, government, and society at the prospect of digital paralysis underscored that economic measures today are inseparable from technological coercion.

For the Global South, this episode serves as a stark reminder that sovereignty in the twenty-first century cannot be confined to territory, trade, or military capabilities alone. The capacity to develop and control indigenous technologies—from navigation systems to payment platforms and data infrastructures—is not a matter of prestige, but a matter of survival. Without such autonomy, nations remain exposed to external shocks, vulnerable to unilateral measures, and condemned to a form of digital tutelage that replicates the very hierarchies of dependency they have historically sought to overcome.

The spirit of Bandung must be revived for the digital age. In 1955, leaders of the Global South met in Indonesia to affirm their independence from both Western and Soviet blocs. Today, a Digital Bandung could declare intellectual independence from digital empires while articulating principles of cooperation, sovereignty, and justice. Such a vision would not only empower the Global South

but also enrich humanity.

For the digital future belongs to all, or it belongs to none.

## Bibliography


- African Union. The Digital Transformation Strategy for Africa (2020–2030). Addis Ababa: African Union Commission, 2020.
- Banco Central do Brasil. PIX: Brazil's Instant Payment System. Brasília: Banco Central do Brasil, 2020. https://www.bcb.gov.br/estabilidadefinanceira/pix.
- Bassam, Laila, and Gebeily, Maya. "Israel Planted Explosives in Hezbollah's Taiwan-Made Pagers, Say Sources." Reuters, September 20, 2024.https://www.reuters.com/world/middle-east/israel-planted-explosives-hezbollahs-taiwan-made-pagers-say-sources-2024-09-18/
- Brautigam, Deborah. The Dragon's Gift: The Real Story of China in Africa. Oxford: Oxford University Press, 2009.
- Brazil. Lei Geral de Proteção de Dados Pessoais (Law No. 13.709/2018). Brasília: Presidência da República, 2018.
- Cadwalladr, Carole, and Emma Graham-Harrison. "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." The Guardian, March 17, 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
- Cardoso, Fernando Henrique, and Enzo Faletto. Dependency and Development in Latin America. Berkeley: University of California Press, 1979.
- Couldry, Nick, and Ulises A. Mejias. The Costs of Connection: How Data Is Colonising Human Life and Appropriating It for Capitalism. Stanford, CA: Stanford University Press, 2019.
- Creemers, R. (2016). Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century. Journal of Contemporary China, 26(103), 85–100. https://doi.org/10.1080/10670564.2016.1206281.
- European Union. General Data Protection Regulation (Regulation (EU) 2016/679). Adopted April 27, 2016. Official Journal of the European Union L119 (May 4, 2016): 1–88.
- Hivelocity. "Miami: Gateway to Latin America's High-Speed Connectivity." Hivelocity Blog, April 12, 2023. https://www.hivelocity.net/blog/miami-gateway-to-latin-americas-high-speed-connectivity/.
- Khera, Reetika, Impact of Aadhaar in Welfare Programmes (September 29, 2017). Available at SSRN: https://ssrn.com/abstract=3045235
- Kukutai, Tahu, and John Taylor, eds. Indigenous Data Sovereignty: Toward an Agenda. Canberra: Australian National University Press, 2016.
- Maclean, Ruth, and Adam Satariano. "Nigeria Suspends Twitter After President's Tweet Is Removed." The New York Times, June 5, 2021. https://www.theguardian.com/world/2021/jun/04/nigeria-suspends-twitter-after-presidents-tweet-was-deleted
- Mas Ribo, Ignacio; Radcliffe, Daniel E., Mobile payments go viral : M-PESA in Kenya (English). Washington, DC: WorldBank.

- http://documents.worldbank.org/curated/en/638851468048259219
- Mearsheimer, John J. The Tragedy of Great Power Politics. Updated edition. New York: W. W. Norton, 2014.
- NEOM. What Is NEOM? Riyadh: NEOM Company, 2023. https://www.neom.com/en-us/about.
- NIC.br. "IX.br São Paulo." Núcleo de Informação e Coordenação do Ponto BR. Accessed May 2024. https://ix.br/.
- OECD. Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy. Paris: Organisation for Economic Co-operation and Development, 2021.https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.pdf
- Prebisch, Raúl. The Economic Development of Latin America and Its Principal Problems. New York: United Nations, 1950.
- Seaborn Networks. "Seabras-1 Subsea Cable." Accessed May 2024. https://seabornnetworks.com/.
- Sullivan, Nicholas P. You Can Hear Me Now: How Microloans and Cell Phones Are Connecting the World's Poor to the Global Economy. San Francisco: Jossey-Bass, 2007.
- TeleGeography. Submarine Cable Map. Accessed May 2024. https://www.submarinecablemap.com/.
- UNCTAD. Digital Economy Report 2019: Value Creation and Capture—Implications for Developing Countries. New York: United Nations, 2019.
- ———. Digital Economy Report 2021: Cross-border Data Flows and Development. New York: United Nations, 2021.
- van Dijck, José, Thomas Poell, and Martijn de Waal. The Platform Society: Public Values in a Connective World. Oxford: Oxford University Press, 2018.
- Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

# ABOUT THE AUTHOR

## MARCUS VINÍCIUS DE FREITAS

Marcus Vinicius De Freitas is Senior Fellow at Policy Center for the New South, focusing on International Law, International Relations and Brazil, and is currently a Visiting Professor of International Law and International Relations at China Foreign Affairs University in Beijing, China. Previously, he was a Professor of The Armando Alvares Penteado Foundation in Sao Paulo, where he served as the coordinator of their International Relations Program from December 2012 until December 2013. He was president of the Sao Paulo Directorate of the Progressive Party, having run for vice governor of the State of Sao Paulo in 2010, where his party polled in third place with more than 1.2 million votes. He also served as the Administrative Director of the Sao Paulo Metropolitan Housing Company until December 2015. Early in 2017, Mr. De Freitas, was a Visiting Fellow of Practice at the Blavatnik School of Government at the University of Oxford. Prior to his current appointment, he was advisor to several investment companies investing in Brazil and Latin America, with particular emphasis on export financing, crypto- assets, crypto-currencies and Blockchain technology. Mr. De Freitas holds an LL.B. (Bachelor of Laws) degree from the University of Sao Paulo, a master of laws from Cornell University and a master of arts in economics and international relations from The Johns Hopkins University School of Advanced International Studies (SAIS).

# ABOUT
# THE POLICY CENTER FOR THE NEW SOUTH

The Policy Center for the New South (PCNS) is a Moroccan think tank aiming to contribute to the improvement of economic and social public policies that challenge Morocco and the rest of Africa as integral parts of the global South.

The PCNS pleads for an open, accountable, and enterprising "new South" that defines its own narratives and mental maps around the Mediterranean and South Atlantic basins, as part of a forward-looking relationship with the rest of the world. Through its analytical endeavours, the think tank aims to support the development of public policies in Africa and to give the floor to experts from the South. This stance is focused on dialogue and partnership and aims to cultivate African expertise and excellence needed for the accurate analysis of African and global challenges and the suggestion of appropriate solutions.

As such, the PCNS brings together researchers, publishes their work and capitalizes on a network of renowned partners, representative of different regions of the world. The PCNS hosts a series of gatherings of different formats and scales throughout the year, the most important being the annual international conferences the "Atlantic Dialogues", the "African Peace and Security Annual Conference" (APSACO), and the "Africa Economic Symposium" (AES).

Finally, the think tank is developing a community of young leaders through the Atlantic Dialogues Emerging Leaders program (ADEL) a space for cooperation and networking between a new generation of decision-makers from the government, business, and civil society sectors. Through this initiative, which already counts more than 450 members, the Policy Center for the New South contributes to intergenerational dialogue and the emergence of tomorrow's leaders.



**Policy Center for the New South**

Rabat Campus of Mohammed VI Polytechnic University,
Rocade Rabat Salé - 11103
Email : contact@policycenter.ma
Phone : +212 (0) 537 54 04 04
Fax : +212 (0) 537 71 31 54

**www.policycenter.ma**

POLICY CENTER FOR THE NEW SOUTH