

Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, towards an AI Sovereignty Stack

*Luca Belli*¹

As a [transformational technology](#), Artificial Intelligence (AI) will have a global impact and considerable ramifications for national economies, democracies, and societies. While many countries are [developing AI governance frameworks](#), the main goal of this paper is to emphasise that the regulation of AI is only one of the essential elements that need to be considered to achieve AI Sovereignty.

AI Sovereignty is not a universally defined concept, and, for this paper, I define it as the capacity of a given country to understand, muster and develop AI systems, while retaining control, agency, and self-determination over such systems.

In this perspective, I propose a layered framework to analyse which elements are essential to establish a country's AI sovereignty, defining them as "Key AI Sovereignty Enablers" or "KASE". Subsequently, I will analyse the case of Brazil, using the proposed KASE framework, to understand whether Brazilian policy choices and governance arrangements can allow the country to assert AI Sovereignty or rather lead to AI dependency.

I argue that sound governance, research, and development in all the elements of the AI value chain are essential not only to achieve economic growth, social justice, and industrial leadership but, primarily, to assert AI Sovereignty, avoiding the implementation of exclusively foreign AI system in a country transform it into a digital colony.

Importantly, I also emphasise that the careful consideration of each of the KASE as well as their interconnection, through an integrated approach, may allow countries to build an AI Sovereignty Stack, i.e. a layered structure allowing reducing the country's exposure to the technological choices of foreign (private or public) actors, and simultaneously increasing agency and self-determination over and though AI systems.

1. Presenting the Key AI Sovereignty Enablers (KASE)

In this paper I posit that the achievement of AI Sovereignty relies on the adoption of a systemic approach to AI, understanding the relevance and the interconnectedness of the Key AI Sovereignty Enablers (KASE). These elements are instrumental for ensuring that a country can develop, regulate, and utilise AI systems according to its own national interests, values, and strategic objectives, rather than being subject to the unavoidable impact of other entities' exercise of AI Sovereignty.

¹ Dr Luca Belli is Professor of Digital Governance and Regulation at Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro, where he directs the Center for Technology and Society ([CTS-FGV](#)) and the [CyberBRICS](#) project.

Importantly, AI Sovereignty is likely to become an increasingly relevant and strategic topic as the development and adoption of AI technologies continue to advance, acquiring a significant role in various aspects of society and democratic governance, not limited to the (digital) economy. The impact of AI advancement, which has been already the object of considerable research, especially concerning its [interaction with data governance](#), includes a wide range of critical sectors such as defence, infrastructural management, healthcare, and justice.

It seems important to emphasise that the capacity to develop and muster AI technology, rather than being regulated through it, does not rely exclusively on the elaboration and enforcement of well-crafted AI legislation. On the contrary, the achievement of an AI Sovereignty Stack entails the capacity to control and exercise agency and self-determination regarding at least eight different KASE that, together, compose the IA Sovereignty Stack, allowing to build of a sustainable and strategically autonomous AI ecosystem.

The fundamental elements that I define as KASE include sound (personal) data governance and algorithmic governance, strong computational capacity, meaningful connectivity, reliable electrical power, a digitally literate population, solid cybersecurity, and last, but not least, an appropriate regulatory framework. The next section analyses them, in the context of Brazil.

2. Exploring the KASE of Brazil

In this section, I will briefly present the KASE that compose what I define as the AI Sovereignty Stack, analysing how Brazil is harnessing each of them.

2.1. Data Governance

Data is the lifeblood of AI systems. Access to diverse, high-quality data is essential for training and improving AI models. Importantly, depending on the type of AI at stake, the data utilised to feed AI systems can be personal, governmental, confidential, copyrighted, etc, thus including a fair amount of complexity and need for regulatory compliance in the context of their processing. Having control over data, including how they are collected, stored, processed, and transferred to third countries is a critical aspect of AI sovereignty.

Sound data governance allows a country to protect its citizens' data privacy, ensure national and informational security, and harness the value of data for national development. Brazil made considerable progress in terms of data governance, by structuring one of the most progressive and refined [open data policies](#) and by adopting a last-generation data protection framework, the [Lei Geral de Proteção de Dados or LGPD](#). The enforcement of the LGPD, however, remains still very embryonic, [especially as regards new generative AI systems](#).

Furthermore, personal data collection is considerably concentrated in the hands of a few foreign tech giants, primarily as a result of so-called [zero-rating mobile Internet plans](#), as discussed in the connectivity section below, thus frustrating the possibility to harness personal data as a national asset. Lastly, data security remains also [very patchy](#) in the lack of a Cybersecurity law and given the lack of regulation on personal data security.

2.2. Algorithmic governance

Software algorithms are the foundation of AI systems, enabling them to perform tasks and make decisions. Developing and owning proprietary software provides a considerable competitive advantage and allows for embedding normative values according to national specificities. Investing in research and development of AI algorithms, while also addressing the potential risks that they pose, can enormously enhance a country's technological capabilities, and reinforce AI Sovereignty.

Importantly, the promotion of multistakeholder cooperation to develop open-source software algorithms, rather than fostering the sole development of proprietary software, can allow for enhancing AI Sovereignty collectively. In this perspective, the first Lula Administration was a true [pioneer in terms of a collective approach to digital sovereignty](#), promoting free and open software (FOSS) as a strategic objective for national development, already in 2003. Unfortunately, this policy was reversed by the Temer administration in 2016, de facto unleashing the recent phenomenon of platformisation of the public administration primarily through the use of foreign software providers.

Despite political turbulence, over the past two decades, Brazil has developed several industrial policy instruments aimed at fostering the national software industry. However, the software development sector has not become as thriving as it could, primarily due to a lack of consistency in software-related policies and the absence of policies focused on stimulating national demand in an organic fashion. Particularly, Brazilian software policies have lacked complementary instruments able to stimulate demand and supply, for instance through public procurements of nationally developed software, as happens commonly in China, or through the establishment of digital public infrastructures, as India did with [the India Stack](#), or by organising capacity building efforts aimed at fostering demand, as South Korea did in the late 1990s.

2.3. Computational Capacity

It is well-known that AI can require substantial computational resources for tasks such as training complex models and processing large datasets. Particularly, the most recent AI systems, such as generative AI, can be remarkably computer-intensive due to their increased complexity. Ensuring the existence or continuous access to sufficient computational capacity should be seen as a key strategic priority. Importantly, the availability of high-performance computing infrastructure depends on multiple factors.

Such factors span from the availability of semiconductors and chips specifically designed for AI applications and last-generation Graphics Processing Units or GPUs, which are becoming particularly relevant to support (generative) AI, to specialised servers tailored to AI specificities that go into data centres. Moreover, it is essential to emphasise that the availability of cloud computing resources by itself is not enough to assert AI Sovereignty, which demands that cloud resources be not only available but fully compliant with national legislation. A telling example of how this is far from being the rule is provided by the [online education platforms](#) provided by two major US tech companies in Brazil, which are supplied nationally and do not even mention how they comply with the Brazilian LGPD, despite the law being fully in force since 2021.

2.4. Meaningful connectivity

Meaningful connectivity, allowing users to enjoy reliable, well-performing, universally accessible Internet infrastructure for an affordable price plays an instrumental role for AI systems to function optimally and be used by the largest possible portion of the population. Seamless connectivity facilitates data exchange, collaboration, and access to cloud-based AI services. It enables real-time applications and supports the development and deployment of AI technologies across various sectors, contributing to the construction of a country's AI Sovereignty.

Over the past ten years, Brazil has made enormous progress [in terms of Internet penetration](#). The cost of connectivity has considerably declined while the connected population has doubled in a decade. Yet, such a rosy picture hides less visible digital divides, which do not impinge on the quantity of but rather on the quality of Internet access. Most of the Brazilian “connected” population is considered so, but de facto only partially connected.

Indeed, more than 70% of the Brazilian connected population, and around 85% of the lower income population, has access primarily to [a reduced set of apps included in so-called zero-rating plans](#), based on not counting the data consumption of a few applications selected by the mobile internet operators. As such user attention and user data collection is concentrated in a remarkably limited number of services, which typically are dominant social media platforms, thus making it particularly challenging for any other business to develop complete personal data sets that can be used to train AI models.

2.5. Reliable electrical power

As AI systems grow in relevance and size, they require a stable and [increasingly relevant supply of electrical power](#) to operate effectively. Ensuring reliable power infrastructure and access to affordable electricity is necessary for maintaining uninterrupted AI operations. In this regard, it may be said that Brazil is probably one of the best-placed countries to support the expansion of AI infrastructure, as it is not only independent in energetic terms, but between 70% and 80% of its annual energy needs are satisfied via renewables, especially hydropower.

However, the national power grid is not exempted from criticism. In the short term, Brazil does not run the risk of a lack of energy supply thanks to the complementarity of various energy sources to hydropower, but the lack of structural planning and the possibility of adverse hydrology – which has been observed in recent years – can alter the cost of energy making it considerably higher. Hence, despite having developed a strong power infrastructure, the Brazilian capability to support the deployment of power hungry technologies requires a stronger focus on planning to prevent potential dependency on external sources.

2.6. Digitally literate population

Enhancing the digital literacy of the population, through capacity building, training, and multigenerational education is essential not only to achieve a skilled AI workforce, but also to foster [cybersecurity and, ultimately, national sovereignty](#). Investing in AI education, research and development helps nurture a pool of talented AI professionals, while spreading an understanding of how to make the best use of technology. A sound educational strategy is

therefore vital to allow the national population to gradually evolve from one being made primarily of consumers of digital technology into one composed of prosumers, i.e. individuals that can develop technology and produce innovation rather than being exclusively consumers.

Building a robust talent pipeline of AI researchers, engineers, and data scientists enables a country to develop and maintain its AI capabilities, increasing the possibility of being an exporter of technology and reducing the likelihood of becoming a digital colony. It is highly promising that the recently elected federal government has already adopted a new [National Policy for Digital Education](#). However, it is still problematic to note that digital literacy keeps on being considered a priority only for the new generations of students, forgetting that literally no one in Brazil – as in most other countries – has received this type of education, thus remaining digitally illiterate. Such a situation is particularly risky in a context of accelerated digital transformation and automatization, in which understanding the functioning of technology becomes a primary necessity not only for the youngest generation but especially for all the individuals, whose labour, social and economic conditions are likely to be affected by the deployment of AI systems.

2.7. Strong cybersecurity

AI systems are susceptible to cybersecurity threats and can be used to perpetrate cyberattacks. Robust cybersecurity measures are vital for any county but become even more so in the context of increasingly accelerated digital transformation and deployment of AI systems. Particularly, protecting AI critical infrastructure, from cyberattacks is essential. Brazil has recently enacted a [considerable number of sectoral cybersecurity regulations](#), spanning the telecom sector, the banking sector, the electricity sector, and the personal data protection laws. While much progress has allowed the country [to climb the International Telecommunications Union's Cybersecurity Index](#), it must be noted that this positive advancement must be considered again with a grain of salt.

Indeed, Brazil still lacks a Cybersecurity Law and a National Cybersecurity Agency, although they have been recently proposed by a study produced by the [Center for Technology and Society at FGV](#) and by a [Draft Bill formulated by the Brazilian Presidency](#). The existence of a highly fragmented approach to cybersecurity, driven by the initiatives of sectorial agencies with no general competence in cybersecurity, and frustrated by the lack of coherent national strategies on cybersecurity is probably one of the main vulnerabilities of the countries, which have not yet managed to create a solid governance framework to connect, coordinate, and leverage the incredible amount of talent that Brazil produces in terms of cybersecurity.

2.8. Appropriate regulatory framework

A comprehensive governance framework that encompasses ethical considerations, data protection laws, and AI regulations is crucial for AI sovereignty. Establishing clear guidelines and standards for AI development, deployment, and usage ensures responsible and accountable AI practices. In this perspective, the Brazilian Congress is discussing a new [Bill for an AI Regulatory Framework](#) to help protect citizens' rights, promote fairness, and prevent discrimination and other potential risks, thus aiming at steering the development, deployment, and use of AI technologies sustainably.

It is important to note that, while this initiative is surely laudable, even if still ongoing, it is not yet clear to what extent it will be able to effectively address the regulation of AI. The latest version of the proposed Bill includes many terms which provide a necessary level of flexibility on key issues such as AI systems transparency, data security, data governance or risk management. However, such flexibility, which is welcome to craft a law that can adapt to technological evolution, must be matched with a mechanism that allows the specification through regulation or standardisation.

In the absence of such specifications, the law risks being highly ineffective. In this regard, it is necessary to consider the recent Brazilian experience regulating data protection to understand that the adoption of modern law and the establishment of a new regulatory authority is only the beginning of the regulatory journey, which risks being considerably jeopardised when the enormously pressing task of specifying the law is attributed to a regulator that seems to be purposefully created being “[ineffective by design](#)”.

3. Conclusions

It is important to reiterate that the abovementioned AI Sovereignty enablers are interconnected and mutually reinforcing. This consideration is particularly relevant in a moment where legislators and governments around the world are studying the regulation of AI, frequently ignoring the utmost importance of the other fundamental elements that I define as KASE.

Considering the interconnectedness of the KASE and leveraging their interdependence through an integrated approach is essential to achieve AI Sovereignty and avoiding digital colonialism. However, such an approach seems to be absent from the current Brazilian “strategic” vision for AI. Indeed, anyone analysing the 2021 [Brazilian Artificial Intelligence Strategy \(EBIA\)](#) will immediately notice the lack of strategic elements in the strategy. The document has been the object of unanimous critiques from observers as it merely includes general considerations about how AI could be implemented in several sectors, without defining either the elements that may allow coordinating the implementation of the strategy, not those that can allow assessing such an implementation, or who would be responsible for such implementation.

By providing a preliminary understanding on what are the essential elements that countries need to consider in their strategic approach to AI, this paper also aims at offering some food for thought that could inspire the revision of the Brazilian strategic approach to AI by the current administration. As noted, an integrated approach considering the KASE is instrumental to achieve AI Sovereignty, developing indigenous AI capabilities, increasing the digital literacy of the population, fostering strategic investments and partnerships, and safeguarding the security of critical AI infrastructure.

Countries that possess strong capabilities in these areas are not only better positioned to maintain control over their AI technologies, policies, and data, but they will likely increase their technological relevance, reducing dependence on external sources and preserving their national interests and autonomy in the AI landscape. Countries lacking such capability need to reconsider thoroughly their strategic approaches to AI, to minimise the considerable risk of dependency that the already ongoing phenomenon of digital colonisation is likely to exacerbate.