Pre-print version of BELLI, Luca. Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, towards an AI Sovereignty Stack. In Carnegie Endowment for International Peace. Digital Democracy Network Conference 2023 Essay Collection. (2023)

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

Luca Belli[1]

As a transformational technology[2], 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[3], 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. In this paper, I put forward a definition of this concept, building upon what I have previously described as "Good Digital Sovereignty,"[4] thus considering AI Sovereignty as the capacity of a given country to understand, develop and regulate AI systems. I argue that AI Sovereignty should be seen as essential to retain control, agency, and self-determination[5] over AI systems.

---

[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. The author would like to thank Steven Feldstein and the participants of the Carnegie Endowment for International Peace's Digital Democracy Network Conference 2023 for their valuable feedback to an earlier version of this paper presented at the Conference.

[2] Jarvenpaa, S. L., & Ives, B. (1996). Introducing transformational information technologies: the case of the World Wide Web technology. *International Journal of Electronic Commerce*, *1*(1), 95-126. https://www.jstor.org/stable/27750802

[3] Belli, L., Curzi, Y., & Gaspar, W. B. (2023). AI regulation in Brazil: Advancements, flows, and need to learn from the data protection experience. *Computer Law & Security Review*, *48*, 105767. https://www.sciencedirect.com/science/article/pii/S0267364922001108

[4] Belli L. (June 2023). Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil. G20's Think20 (T20). https://t20ind.org/research/building-good-digital-sovereignty-through-digital-public-infrastructures/ ; Belli, L. and Jiang, M. (Eds.). (Forthcoming). Digital Sovereignty from the BRICS Countries. Cambridge University Press.

[5] The right to self-determination is so-called a primary principle or principle of principles, as it plays an instrumental role to allow individuals to enjoy their human rights, thus being an enabler of other fundamental rights. For this reason, it is enshrined as the first article of both the Charter of the United Nations and the International Covenants of Human Rights. According to these three international-law instruments, states have agreed that "all peoples have a right to self-determination" and that "by virtue of that right they are free to determine their political status and to pursue their economic, social and cultural development." It is essential to emphasise the relevance of the internal dimension of self-determination, i.e. the right of peoples to freely determine and pursue one's economic, social and cultural development, including by independently choosing, developing and adopting digital technologies. Such conception is also corroborated by the recognition of the fundamental right to "informational self-determination" as an expression of the human right to have and develop a personality, first recognised by the German Supreme Court, in the 1983 Census case. The fundamental right to free development of personality is formally recognised internationally. Article 22 of the Universal Declaration of Human Rights affirms that "everyone is entitled to the realisation of the rights needed for one's dignity and the free development of their personality," while the International Covenant on Economic, Social and Cultural Rights consecrates this fundamental principle regarding the right of everyone to education and to participate in public life. Particularly, the Covenant's signatories have agreed that the right to education "shall be directed to the full development of the human personality and the sense of its dignity [...] and enable all persons to participate effectively in society" (Article 13.1). Moreover, the free development of personality is explicitly considered as instrumental to exercise the fundamental right "to take part in cultural life [and] to enjoy the benefits of scientific progress and its applications" (Article 15). See Belli, Luca. Network Self-Determination and the Positive Externalities of Community Networks. In L. Belli (Ed.) Community

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[6], regulation, 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 systems in a country, which would likely transform the recipient country into a digital colony. Importantly, the purpose of this paper is not to advocate for AI autarchy, nor to deny the ample range of benefits that digital trade and cooperation can produce, but rather to discuss how countries could achieve a sufficient level of strategic autonomy, diversifying their AI value chains, and being able to grasp the functioning of AI systems, develop such systems rather than being mere consumers, and regulate them effectively.

The paper also emphasises that the careful consideration of each of the KASE and the importance of their interconnection, through an integrated approach, may allow countries to build what I define as an "AI Sovereignty Stack". This layered structure may reduce the country's exposure to the technological choices of foreign (private or public) actors, and simultaneously increase their agency and self-determination over and though AI systems.

Such interconnection must be reflected in the necessary coordination of research and development, governance and regulation of the various KASE to be able to form a well-functioning AI Sovereignty Stack. Such stack should be organised through a dedicated governance system allowing the authorities in charge of overseeing each KASE to cooperate with other authorities from different sectors (including with regulators of transversal sectors such as competition, consumer protection, data privacy, financial services, energy, and telecom infrastructure) to facilitate smooth organisation and, particularly, information sharing.

Importantly, this paper intends to adopt a pragmatic stance, stressing that achieving AI Sovereignty will be far from trivial, especially for Global South countries. However, in the perspective of the author, AI Sovereignty should be considered at least a policy priority. The KASE discussed in the next section require considerable planning, resources, and implementation capacity, but they should be – ideally – seen as a highly strategic objectives for the reinforcement of national sovereignty, allowing to resist possible adverse conditions,

---

Networks: The Internet by the People for the People: Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity. FGV. (2017: 35-64) https://www.intgovforum.org/en/filedepot_download/4391/1132 ; Belli, Luca *et al.* Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. FGV Direito Rio. (2023: 69-94). https://bibliotecadigital.fgv.br/dspace/handle/10438/33784

[6] For the purposes of this paper, governance is intended as the set of processes and institutional mechanisms that stimulate facilitate and organise coordinate the stakeholder interactions of different stakeholders in a political space, to confront different opinions and interests regarding a specific issue and, ideally, achieve the proposal of the best possible regulatory solution to frame such issues. Regulation is intended as the product of governance, consisting of an ample range of instruments that can foster the stability and proper functioning of complex systems, where the presence of multiple actors with varying or divergent interests can naturally lead to instability and dysfunction. Belli, Luca. De la gouvernance à la régulation de l'Internet. Paris: Berger-Levrault. (2016 :17-132).

spanning from extraterritorial effects of foreign regulation, to the imposition of foreign sanctions and the increasingly frequent disruption of supply chains.

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 (state or corporate[7]) entities' exercise of AI Sovereignty.

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[8], 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

[7] Luca Belli. Structural Power as a Critical Element of Digital Platforms' Private Sovereignty. In Edoardo Celeste, Amélie Heldt and Clara Iglesias Keller (Eds). *Constitutionalising Social Media*. (Hart 2022) https://lucabelli.net/2021/08/10/structural-power-as-a-critical-element-of-social-media-platforms-private-sovereignty/
[8] CPDP LatAm. (2023, July 18). Publications - CPDP LaTAM 2023. CPDP LatAm 2023. https://cpdp.lat/en/publications/

fair amount of complexity and need for regulatory compliance in the context of their processing. Hence, not only the availability of large volumes of heterogeneous data is essential to develop AI capabilities, but having control over such data, including how they are collected, stored, processed, and transferred to third countries is a critical aspect of AI sovereignty.

Countries with large and diverse populations together with consolidated data collection practices and well-structured data policies will indubitably have a competitive advantage, constructing their AI sovereignty. It is important to emphasise that few countries enjoy the privilege of having both large data pools and sound data policies at their disposal. In this context, countries should consider establishing shared data policy frameworks, at regional level or within existing international governance mechanisms,[9] so that national data assets can be shared under substantially equal norms. This strategy would allow usage of much larger and diversified data pools, providing at the same time juridical certainty for AI researchers and developers, while protecting the rights of personal data subjects, intellectual property right holders, and preserving the public interest.

Particularly, 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[10] and by adopting a last-generation data protection framework, the *Lei Geral de Proteção de Dados* or LGPD[11]. The enforcement of the LGPD, however, remains still very embryonic, especially as regards new generative AI systems[12].

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[13], 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[14] in the lack of a Cybersecurity law and given the lack of regulation on personal data security.

[9] The finest example of international cooperation regarding data policy are provided by European initiatives. The Council of Europe Convention 108 is the most renown instance – and until the recent entry in force of the Malabo Convention, the only one – of international treaty regarding personal data protection. The most refined example of coordinated approach to data policy is offered by the European Union data policy framework, spanning form the General Data Protection Regulation, the Open Data Directive, and the most recent Data Act. It is important to stress that a less ambitious, yet relevant framework could also be proposed at the Latin American level, where most countries have already adopted similar data protection laws. In this regard, see Luca Belli, Ana Brian Nougrères, Jonathan Mendoza Iserte, Pablo A. Palazzi and Nelson Remolina Angarita. Hacia un modelo latinoamericano de adecuación para la transferencia internacional de datos personales. Centro de Tecnologia y Sociedad de Universidad de San Andrés. (2023).

[10] De Magalhães Santos, L. G., & Dhaou, S. B. Open Data and Emerging Technologies: Connecting SDG Performance and Digital Transformation. https://cyberbrics.info/open-data-and-emerging-technologies-connecting-sdg-performance-and-digital-transformation/

[11] The Brazilian General Data Protection Law (LGPD) – Unofficial English Version https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/

[12] Belli, Luca. (2023, July 20). Why ChatGPT does not comply with the Brazilian Data Protection Law and why I petitioned the Regulator. *MediaNama*. https://www.medianama.com/2023/05/223-chatgpt-brazilian-data-protection-law-ai-regulation/

[13] See http://www.zerorating.info/

[14] Belli, L. (2021). The largest personal data leakage in Brazilian history. openDemocracy. https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history/

2.2. Algorithmic governance

Software algorithms are the foundation of AI systems, enabling them to perform tasks and make decisions. Importantly, algorithms can be the subject matter of regulation, but they can also play an instrumental role to elaborate regulation. On the one hand, the development and deployment of algorithms can – at least partly – give rise to risks and social problems triggering the need for regulatory intervention. On the other hand, algorithms can support the regulatory intervention itself, as they are increasingly useful and used to assist both the elaboration and implementation of regulation.

In this perspective, the development, deployment and regulation of or through algorithms are all equally important dimensions of algorithmic governance. 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.

Hence, the promotion of multistakeholder cooperation to develop software algorithms can allow for enhancing AI Sovereignty either when domestic players are stimulated to develop proprietary software, or when software is developed in open-source through a collaborative process embraced – or even led – by national stakeholders. In this latter perspective, the first Lula Administration was a true pioneer in terms of a collective approach to digital sovereignty[15], promoting free and open software (FOSS) as a strategic objective for national development, already in 2003. Such policy allowed not only to be strategically autonomous from foreign software producers but also to increase national understanding and development of software. 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 software development and implementation in an organic fashion, including by facilitating access to capital to jumpstart the domestic algorithm industry. 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[16], 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

[15] Belli, L. (2023, March 1). Brasil precisa reconstruir sua soberania digital. Estadão. https://www.estadao.com.br/politica/blog-do-fausto-macedo/brasil-precisa-reconstruir-sua-soberania-digital/

[16] See https://indiastack.org/

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.

The availability of high-performance computing infrastructure depends on multiple factors, spanning from the accessibility 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. In this respect, it is interesting to note that some of the first policies adopted by the Lula 3 administration have been the reintroduction of the national support programme for the development of semiconductors (known as "PADIS", in its Portuguese acronym) as well as the suspension of the previous Bolsonaro administration decision to sell the National Center for Advanced Electronic Technology (Ceitec), which is the only semiconductors producer of Latin America.[17]

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 offered by the online education platforms[18] 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[19]. 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-

[17] Decree No. 11,456, of March 28, 2023. Amends Decree No. 10,615, of January 29, 2021, which provides for the Support Program for Technological Development of the Semiconductor Industry. https://www.in.gov.br/en/web/dou/-/decreto-n-11.456-de-28-de-marco-de-2023-473390191

[18] Pacotes "education" do Google e da Microsoft não contemplam lei brasileira de proteção de dados. (n.d.). https://aberta.org.br/pacotes-education-nao-contemplam-lgpd/

19 TIC domicílios. (n.d.). Cetic.br - Centro Regional Para O Desenvolvimento Da Sociedade Da Informação. https://cetic.br/pt/pesquisa/domicilios/publicacoes/

rating plans[20], based on not counting the data consumption of a few applications selected by the mobile internet operators. As such user attention ad 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[21] 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 angry 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[22]. 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[23].

[20] IDEC (2021). Barreiras e limitações no acesso à internet e hábitos de uso e navegação na rede nas classes C, D e E. https://idec.org.br/sites/default/files/pesquisa_locomotiva_relatorio.pdf

[21] Luccioni, S. (2023, April 12). The mounting human and environmental costs of generative AI. Ars Technica. https://arstechnica.com/gadgets/2023/04/generative-ai-is-cool-but-lets-not-forget-its-human-and-environmental-costs/

[22] CyberBRICS. (2023, February 24). Cybersecurity and digital sovereignty: a new path for Brazil. CyberBRICS. https://cyberbrics.info/cybersecurity-and-digital-sovereignty-a-new-path-for-brazil/

[23] Law No. 14.533 - Brazil, Jan. 11, 2023. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14533.htm

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[24], 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[25], 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[26] and by a Draft Bill formulated by the Brazilian Presidency[27]. 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[28] 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.

[24] Belli, L. *et al.* (2023). Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. CyberBRICS. https://cyberbrics.info/ciberseguranca-uma-visao-sistemica-rumo-a-uma-proposta-de-marco-regulatorio-para-um-brasil-digitalmente-soberano/

[25] Brazil rises in international cybersecurity ranking. (2022, June 24). Serviços E Informações Do Brasil. https://www.gov.br/en/government-of-brazil/latest-news/2022/brazil-rises-in-international-cybersecurity-ranking

[26] Belli, L et al. (2023).

[27] PNCiber Draft Bill https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf

[28] PL 2338/2023 - Senado Federal. (s.d.). https://www25.senado.leg.br/web/atividade/materias/-/materia/157233

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"[29].

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)[30] 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 neither the elements that may allow coordinating the implementation of the strategy, nor 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, diversifying supply chains, increasing the digital literacy of the population, fostering strategic investments and partnerships, and safeguarding the security of critical AI infrastructure.

[29]New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a post-Western Model of Data Governance Luca Belli. (n.d.). IJLT. https://www.ijlt.in/journal/new-data-architectures-in-brazil%2C-china%2C-and-india%3A-from-copycats-to-innovators%2C-towards-a-post-western-model-of-data-governance

[30] Gaspar, W. (2022, March 28). Artificial Intelligence in Brazil still needs a strategy. CyberBRICS. https://cyberbrics.info/artificial-intelligence-in-brazil-still-needs-a-strategy/

It is important to be realistic and acknowledge that not all countries might be able to elaborate and implement the necessary strategic, policy and institutional changes allowing them to build an AI Sovereignty Stack. Such an effort might be especially herculean for Global South countries, which typically depend on foreign technologies. However, a careful mix of creative thinking and – much needed – political vision regarding technological development may allow to overcome some of the most burdensome obstacles for low-income countries, for instance by embracing the use of open software to overcome the considerable financial costs determined by dependency on foreign software. The elaboration of an AI Sovereignty Stack, therefore, should be seen as an ideal goal that all countries should strive to achieve but that may not be feasible for all countries.

Ultimately, countries that possess strong capabilities in the KASE 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 risks prompted by AI dependency that the already ongoing phenomenon of digital colonisation is likely to exacerbate.