Pre-print version of Belli L. and Galdino L. Editorial: Toward a BRICS stack? Leveraging digital transformation to construct digital sovereignty in the BRICS countries. Computer Law & Security Review. Special issue on Digital Transformation in the BRICS Countries. https://doi.org/10.1016/j.clsr.2024.106064

Toward a BRICS Stack? Leveraging Digital Transformation to Construct Digital Sovereignty in the BRICS Countries

Luca Belli and Larissa Magalhães

The past decade of digital transformation processes, enormously accelerated by the COVID-19 pandemic, have starkly exposed the benefits as well as the risks that the massive adoption of digital technologies may entail. In this period of intense and frequently turbulent technological evolutions, it has become commonly accepted that meaningful connectivity and well-functioning and inclusive and cybersecure digital (public) services are essential to unleash sustainable development. However, very few countries and stakeholders seem to have a clear vision and a sound strategy to achieve their digital transformation, understanding the need for a system approach to digital technologies, and being able to mitigate, and ideally avoid the risks that accompany the use of digital technologies.

Even fewer stakeholders have realised that such strategy and vision are not only instrumental to shape a sustainable digital transformation, they are the very essence of digital sovereignty. A concept that we define as the capacity to understand, develop and effectively regulate digital technologies, to retain agency, self-determination, and control over digital infrastructure, data, services, and protocols[1].

Over the past years, the CyberBRICS Project[2] has dedicated an increasing amount of attention to an ample range of initiatives and digital policy issues that compose and intersect with digital sovereignty narratives emerging in the BRICS countries (Brazil, Russia, India, China, and South Africa). The analyses featured in this special issue offers a critical perspective on these issues and needs to be read in conjunction with at least two other studies elaborated by the CyberBRICS Project, which are dedicated respectively to "Digital Sovereignty in the BRICS: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance"[3] and to mapping "How the BRICS Countries are Regulating their Digital Transformation"[4]. Indeed, our research findings seem to demonstrate that, although with important differences in their

[1] This definition is based on the previous works on digital sovereignty published in the context of the CyberBRICS project. See for instance Jiang, Min and Belli, Luca (Eds). Digital Sovereignty from the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge University Press. (2024); Belli, L. (2023). Building good digital sovereignty through digital public infrastructures and digital commons in India and Brazil. G20's Think20 (T20). https://is.gd/BDCXss ; Belli et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano. FGV (2023); Belli L. "Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, to build an AI Sovereignty Stack" in Belli, L. and Gaspar, W.B. (Eds.) The Quest for AI Sovereignty, Transparency and Accountability. Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition. FGV. (2023).

[2] Since 2018, the CyberBRICS project has been supported by the Open Society Foundations (OSF), the Getulio Vargas Foundation (FGV) and the Ford Foundation. The authors would like to express deep gratitude and praise the foresightedness of the founders, who have believed in the CyberBRICS project's potential to develop innovative research, exploring some extremely relevant areas of digital policy and regulation, from Global South perspectives. Detailed information about the CyberBRICS team, publications and events are available at www.cyberbrics.info

[3] Jiang, Min and Belli, Luca (Eds). Digital Sovereignty from the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge University Press. (2024).

[4] Belli, L. and Magalhães, L.(Eds). Smart BRICS: How the BRICS Countries are Regulating their Digital Transformation. Springer-Nature. Forthcoming.

approaches, BRICS countries have become leading players regarding digital transformation, leveraging a variety of processes to construct and assert their digital sovereignty.

As we discuss at length in this special issue and in other CyberBRICS publications[5], the BRICS countries' approaches to digital transformation and digital sovereignty have been motivated by numerous and heterogenous reasons. These span from being fully aware of the consequences of technological dependence, due to the colonial past of most of the group members; to being keen on fostering vibrant innovation ecosystems at the domestic level, in line with well-rooted developmental traditions; to the understanding that digital technologies can be leveraged either to undermine or to reassert existing constitutional frameworks, thus directly impacting state sovereignty and individual rights; and to the necessity to cope with increasingly relevant geopolitical tensions, which have led to mounting suspiciousness, protectionism, and explicit sanctions targeting digital products and services, and disrupting digital supply chains.

Some BRICS countries, particularly China, Russia and India, have been consistent in considering digital transformation as an essential element for achieving their digital or "Internet sovereignty"[6], while Brazil and South Africa have been a fertile ground for less outspoken but equally relevant digital transformation initiatives[7] aimed at strengthening "technological autonomy", which is a constitutional objective for Brazil,[8] for more than two decades.[9] The proximity of Russia, China and India, not only in geographical terms, but

[5] CyberBRICS publications are available in open access at https://cyberbrics.info/cyberbrics-publications/

[6] Such terminology has been frequently adopted by the members of the Shanghai Cooperation Organization (SCO), which include the RIC countries. Since 2011, the SCO has adopted an International Code of Conduct for Information Security – which was updated in 2015 – recognising that "policy authority for Internet-related public policy issues is the sovereign right of States." https://digitallibrary.un.org/record/710973 For a comparison of the differences between the 2011 and 2015 versions of the Code, see https://openeffect.ca/code-conduct/

[7] For instance, in Brazil, South Africa and India numerous community networks have emerged as crowdsourced connectivity initiatives, built and operated as digitally sovereign commons by local community members, administrations and entrepreneurs. These initiatives play an increasingly relevant role to expand Internet access, while also giving rise to a large number of positive externalities, spanning from promotion of new content and services in local languages, new job opportunities in network maintenance, new governance models for the management of the network infrastructure and, ultimately, new forms of enjoying fundamental rights through a commons-based conception of digital sovereignty. Belli, L., & Hadzic, S. (2023). Community networks: Building digital sovereignty and environmental sustainability. Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity. https://is.gd/cB2VLm ; Belli, L. (2017). Network self-determination and the positive externalities of community networks. In L. Belli (Ed.), Community networks: The internet by the people for the people: Official outcome of the UN IGF dynamic coalition on community connectivity. FGV. https://is.gd/SuKDFg

[8] Critically, technological autonomy is a constitutional objective enshrined in article 219 of the Brazilian Federal Constitution, thus giving a constitutional law base to the pursuit of digital sovereignty in the country. The pursuit of strategic autonomy as regards digital technologies has been demystified and entered global discussions, since the European Union has started to herald it as an explicit policy goal. Michel, C. (2021, February 3). Digital sovereignty is central to European strategic autonomy – Speech by President Charles Michel at "Masters of digital 2021" online event. European Council. https://is.gd/mm4ysK

[9] Already in 2003, Brazil mandated the adoption of open software in federal public administration, to reduce national dependency from foreign software producers and promote technological autonomy. In a similar perspective, since 2016, the Brazilian Central Bank has promoted the establishment of the Pix system, a highly successful digital public infrastructure for electronic payments that entered in force in 2020 and, since then, has disrupted the previous e-payment monopoly of Visa and Mastercard, which were the only providers concentrating all consumer-facing digital payment – and the consequent data processing – before Pix. Brazil took inspiration from the Indian UPI, a similarly successful digital public infrastructure, which is an evolution of Mir, the Russian autochthonous card-based electronic payment system. Belli, L. (2023). Building good digital sovereignty through digital public infrastructures and digital commons in India and Brazil. G20's Think20 (T20). https://is.gd/BDCXss

also as members of the Shanghai Cooperation Organization[10], may explain the convergence in their explicit posture in favour of digital transformation as a leverage of digital sovereignty.

Moreover, their traditional sensitivity towards potential US meddling in their internal affairs has motivated suspicion towards US information and communication technologies, perceived as a potential tool of digital colonisation[11], espionage, manipulation and control – suspicions that have been amply corroborated by the revelations of former National Security Agency (NSA) contractor Edward Snowden. In this context, we are reminded that (cyber) security and sovereignty may often rhyme with surveillance. Hence a critical approach to digital technologies and the transformations they enable, avoiding indulging in excessively confident "techno-solutionism"[12], is always needed to be able to truly understand their potential positive and negative impact.

Brazil and South Africa seem to have an approach to digital transformation driven primarily by developmental considerations, aimed at exploiting technological advancements to cut costs and increase the efficiency of oversized and lethargic administrations, while reinvigorating the national economies by promoting the establishment of domestic – and, ideally, autonomous – digital ecosystems. Such posture is evident in the recent South African National Policy on Data and Cloud that openly advocates for the use of data-intensive technology to foster national development and reassert digital sovereignty[13], as explored in this special issue article dedicated to data sovereignty. Brazil has long been a pioneer of technological sovereignty, experimenting with various strategies, spanning from the adoption of open-source software by the public administration to promote software autonomy in 2003, to the development of a national digital public infrastructure for electronic payment, called Pix, which has rapidly become the main tool for online payments, in less than 4 years.[14]

In the research we conduct, we decided to adopt an agnostic approach to digital sovereignty and digital transformation, to avoid preconceptions on whether these concepts should be considered as necessarily negative or positive, but letting our conclusion be driven by our concrete findings. Conspicuously, the study of the BRICS countries is also useful to illustrate that political stability and the consequent capacity to implement strategies in a consistent fashion, is one of the main ingredients necessary to unleash digital transformations that can achieve digital sovereignty. The political and policy instability that characterised the past decade of Brazilian and South African history tellingly demonstrate this point. The sensitivity of the countries to digital sovereignty arguments and the way in which their policies have been shaped, implemented, discontinued or altered seems to strongly depend on the political orientation of the

[10] The SCO is an intergovernmental organisation aimed at political, economic, and security cooperation. It covers three-fifths of the Eurasian continent and was established in 1996, in Shanghai, by China, Russia, Kazakhstan, Kyrgyzstan, and Tajikistan. India has been an observer since 2005 and joined as full member in 2017. See http://eng.sectsco.org

[11] For a telling accounts on digital colonialism, see Benyera, E. (2021). The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data. Routledge; Avila Pinto, R. (2018). Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies. SUR: International Journal on Human Rights, 15(27), 15-27; Couldry, N. & Mejias, U. (2019). The costs of connection: How data Is colonizing human life and appropriating it for capitalism. Stanford, CA: Stanford University Press.

[12] The term 'techno-solutionism" refers to the belief that every social and political problem can be solved through the development of new technologies. See Morozov, E. (2013). To Save Everything, Click Here: The Folly of Technological Solutionism. Hachette.

[13] Department of Communications and Digital Technologies of South Africa. National Policy on Data and Cloud. (2024:8).

[14] See note 7.

government in charge. On the other hand, the strong political stability that the RIC countries have enjoyed over the past decades may have been one of the most important factors enabling their digital transformation.

Lastly, it is important to emphasise that, besides having expressed clear interest in the potential of the digital economy, over the past few years all BRICS countries seem to have notably increased their cybersecurity concerns, which frequently overlap with digital sovereignty narratives, and now occupy a prominent place in both their domestic agendas and in the BRICS-grouping one.[15] Cybersecurity is not featured in this special issue, not because we underestimate the relevance of this all-important topic, but rather because we have decided to dedicate a specific stream of the CyberBRICS research to this issue, given its enormous significance.[16] In such complex scenario, this editorial aims at providing an overview of the strategies and core initiatives spearheaded by BRICS countries regarding digital transformation, connecting them with their emerging digital sovereignty narratives and approaches.

1. Terminology, Methodology, and a Layered Approach towards Digital Transformation

To offer more clarity to the reader, this section defines some key terms utilised in this special issue, such as digital transformation, governance, and regulation. Secondly, we propose a "layered approach" that can be used to frame digital transformation and digital sovereignty initiatives.

1.1. Digital transformation: a broad and multifaceted term

Digital Transformation processes evoke incredible benefits and opportunities in terms of accessibility, efficiency, and productivity, but also convey enormous risks and challenges in terms of human rights, security, equality and control, depending on how such processes are framed and structured. Governments around the globe are embracing digital transformation as a tool to cut costs and streamline public services, reignite the economy and foster digitalisation of their countries. However, existing approaches generally fail to consider the interconnection between the various dimensions of digital transformation, the impact that such process may have on a wide array of stakeholders, and the intimate connection between the building blocks of digital transformation and the fundamental elements of digital sovereignty.

Digital transformation is a broad and multifaceted term. The International Telecommunications Union defines it as "a journey which started with technological innovation, digitalization, market liberalization since the dawn of mobile and the Internet. […] Digital transformation is about users, technologies and data."[17] Hence digital transformation should be seen as a process that, ideally, implies people-driven transformation of entire organisations or sectors, thus requiring far-reaching and cross-cutting changes that accompany and are leveraged by the adoption of digital technologies. However, with few exceptions, this definition ideal scenario is far from reality.

[15] See Belli, L. (Ed.). CyberBRICS: Cybersecurity Regulations in the BRICS Countries. Cham: Springer International Publishing. (2021); Belli, L. Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. The African Journal of Information and Communication, v. 28, (2021); Belli et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano. FGV (2023).

[16] *Idem.*

[17] See ITU-D. The BDT Wheel of Digital Transformation. (s.d.) https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/digital-transformation-wheel.aspx

Indeed, digital transformation "plans" frequently manifest in the form of a collection of sporadic, ephemeral, and unorganised initiatives – often linked to experimentation with "hype" technologies such as Artificial Intelligence (AI), Blockchain, or 5G – rather than being coordinated processes, resulting from well-informed, well-conceived and well-implemented strategies. Even official documents denominated as "digital strategies" frequently lack essential strategic elements such as a redistribution of tasks, responsibilities and resources, the identification of timeframes and potential risks, and the definition of specific budgets and metrics to evaluate whether the strategy is successfully implemented or not.

Importantly, digital transformation cannot be seen as the mere implementation of sporadic standalone projects, but rather a whole process encompassing the design and execution of well-studied and highly interconnected initiatives, which aim at triggering a structural change enabled by digital technologies. This is precisely why the concept of the "stack" lends itself well to visualise such structural evolution. As eloquently argued by Benjamin H. Bratton, the digital "stack" forms both the technical structure and the governance architecture that underpin digital transformation.[18]

As our research illustrates, in order to be successful, digital transformation requires a systemic vision, matched with solid coordination both during the preparation and implementation phases. To understand what we mean by digital transformation we need to identify the different elements that enable such transformation and how they interconnect and mutually influence each other.

1.2. A layered approach to digital transformation

This section identifies five types of enablers of digital transformation that can be seen as forming a layered architecture of digital transformation stack that, in turn, is instrumental to construct digital sovereignty. While digital sovereignty is an emerging and not-universally-defined concept, as noted above, we propose to consider it as the capacity of states, corporations or individuals to understand, develop and regulate digital technologies in order to exercise control, choice and self-determination over the digital assets they use.

The layered architecture that we deem as instrumental to underpin digital transformation and achieve digital sovereignty relies on the following five elements: governance, funding, infrastructure, services, and data. To be able to maximise the degree of success, sustainability and digital sovereignty of the digital transformation processes, each of the abovementioned elements must be considered as interdependent layers of a stack. Each of the layers must include dedicated strategies, policies and regulations, and implementation mechanisms allowing for the stakeholders that drive the digital transformation to be able to exercise oversight on the process, by understanding, steering and regulating it. The use of a layered approach intentionally aims at stressing the relevance and interconnectedness of each element as an essential component of a larger digital transformation stack.

The concept of the stack, where elements can be added and layered on top of other building blocks, represents, at the same time, the strategic framework aimed at enabling digital transformations but also the structural change that the digital transformations is capable of enabling. The Indian example is telling in this regard: the country has been shaping its transformation for the past decade, based on the implementation

[18] Benjamin H. Bratton. The Stack: On Software and Sovereignty. MIT Press. 2016. This approach has been further developed in the context of AI Sovereignty in Luca Belli. "To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)." In Steven Feldstein (Ed). New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms. Washington, DC: Carnegie Endowment for International Peace, 2023. http://dx.doi.org/10.2139/ssrn.4465501

of its "India Stack." [19] This approach is based on leveraging interconnected building blocks of digital infrastructure as the driving force of digital transformation, proving that such digital infrastructure is in itself an enormously powerful tool of regulation.

The India Stack provides vivid expression of what Susan Strange defined as structural power and Lawrence Lessig called architecture.[20] Both authors argue that the ways in which we construct our infrastructures determine what specific behaviours are allowed or not by design, thus playing an extraordinarily effective regulatory function. In this perspective, we need to recognise that a "stack approach" to digital transformation is not, per se, a guarantee that the process will be people-centred, transparent and accountable, and checks and balances are of utmost importance, as explored in this special issue's contribution dedicated to India.

In this sense, the first layer is the governance one, which is particularly relevant, considering that digital transformation must rely on smooth coordination of multiple actors. We define governance as the set of processes and mechanisms that favour the communication, coordination and cooperation of different stakeholders, to define the best possible regulatory strategies to frame a specific issue.[21] Consequently, regulation is the set of tools – which may have very different natures, spanning from laws, to contracts, technical standards or software algorithms – aimed at fostering order in a specific system.[22] Different countries may opt for different governance models, especially regarding the engagement with nongovernmental stakeholders and, as we illustrate in the analyses that compose this special issue, BRICS countries' governance approaches are rather heterogeneous.

For instance, Brazil excels at convening stakeholders for policy discussion and proposal purposes, as demonstrated by its twenty-year-old Internet Steering Committee (CGI.br) and its newly created Brazilian Presidency's National Cybersecurity Committee (CNCiber), while India has been leading efforts to actively engage different stakeholders in the experimentation and implementation of concrete techno-regulatory solutions, as demonstrated by the India stack experience. China has pioneered a form of state-led multistakeholderism which aims at involving stakeholders in the full digital transformation cycle through an informatization and cybersecurity "xitong", which literally translates as "system", and acts as a large coordination council.[23] Interestingly, a similar administrative tool, also called national system, is utilised in Brazil to facilitate stakeholder coordination in specific sectors, such as consumer protection, cyber defence, or education.

[19] Tellingly, the official website of India Stack affirms it is "A vision for the world, a vision for India" https://indiastack.org/

[20] Susan Strange, States and Markets. (1st edn, Continuum 1988). Lawrence Lessig 'The Law of the Horse: What Cyberlaw Might Teach' [1999] Harvard Law Review 501; L. Lessig, Code: And Other Laws of Cyberspace Version 2.0, (Basic Books 2006).

[21] Governance can be seen as the set of processes and institutional mechanisms that stimulate facilitate and organise the interactions of different stakeholders in a political space, to confront different perspectives and interests regarding a specific issue and, ideally, achieve the proposal of effective regulatory solutions to frame such issues. See Belli, L. De la gouvernance à la régulation de l'Internet. Paris: Berger-Levrault. (2016 :17-132).

[22] 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. See *idem*.

[23] See Belli, L. New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a post-Western Model of Data Governance. Indian Journal of Law and Technology. (2022)

The second layer tackles the existing funding opportunities to incentivise and support the digital transformation process. Such funding opportunities include financing the expansion of access and usage of digital technologies for households; financing technology development and startups as a propellant of economic growth, as illustrated in the Russian example; supporting the digitisation of existing public and private services, as demonstrated by the case of China, Brazil and Russia; funding the development of digital public infrastructures as epitomised by India; or supporting the establishment and maintenance of digital public goods.

The third layer concentrates on the establishment of appropriate and well-performing critical digital infrastructures, providing universal and accessible Internet connectivity[24] and facilitating data processing. Importantly, critical digital infrastructures should be considered not only in terms of Internet access but also in terms of cloud servers and software infrastructures and their combination for the provision of AI systems. Moreover, the experimentation with alternative connectivity infrastructures can lead to the establishment of new types of commons-based approaches to connectivity, as illustrated by the case of the community networks, discussed in the article dedicated to South Africa.

The fourth layer to be analysed is the digitalisation of services. Connected citizens are increasingly getting used to the benefits of technology and the value of user-friendly platforms, which increases their expectations of governments' ability to deliver high-value, easy-to-use digital services. These expectations, together with the widespread tendency to utilise ICTs as a tool to achieve efficiency, frequently lead governments to consider digital transformation as an opportunity to reorganise not only industry and productive sectors but also reshape the state organisation, starting from the structure of the public administration until the provision of public services, as highlighted in this special issue analysis dedicated to China. The way in which such digitalisation is achieved, though, is a vital concern, as such digitalisation can be a vector of digital sovereignty or digital colonisation depending on the choices in the previous layers that determine the extent to which control, agency and self-determination are maximised or reduced.

Lastly, the fifth layer is the data layer and encompasses the existing frameworks regulating the processing of personal as well as non-personal data, such as governmental data and industrial data. This layer interests three intimately intertwined and frequently overlapping policy areas: data protection, data openness, and data security.

The ways in which these areas are shaped and interrelate is essential not only for digital transformation purposes, but for the definition of the future of our economies, societies and democracies. In this perspective (personal) data acquire an essential economic and strategic value which can be maximised through the adoption of dedicated policies (e.g. data privacy, information security and open data[25]) but also through the development of dedicated infrastructure facilitating data processing, as discussed in the contribution on data sovereignty of this special issue.

[24] See Belli, L., Pahwa, N. & Manzar, O. (2020) (Eds.) (2020) The Value of Internet Openness in Times of Crisis. UN Internet Governance Forum. https://www.intgovforum.org/multilingual/filedepot_download/6114/2375 ; Belli L. (2021) (Ed.) (2021). CyberBRICS: Cybersecurity Regulations in the BRICS Countries. Springer-Nature. https://link.springer.com/book/10.1007/978-3-030-56405-6

[25] For an analysis of these three type of data policies and their tensions at the Brazilian level, see Belli L., Magalhães, L. et al. Governança de dados no setor público: dados abertos, proteção de dados pessoais e segurança da informação para uma transformação digital sustentável. Lumen Juris. (2024). https://hdl.handle.net/10438/35341

1.3. Methodology

This article relies on the research developed during the second phase of the CyberBRICS project.[26] Particularly, this phase has been dedicated to the mapping of digital transformation and connectivity policies of the BRICS grouping. Desk research has been complemented by a large number of issue-specific multistakeholder seminars, and participatory observation of multiple policy discussion processes.

The existing CyberBRICS research has shed light on the good and bad practices adopted by the BRICS countries in their efforts to shape their digital transformation, exploring a variety of approaches that can be replicated or should be avoided by other countries. Importantly, as very few countries in the world already have consistent, well-functioning and well-resourced digital transformation strategies, and most nations are only starting to discuss what digital sovereignty means, the findings of the CyberBRICS research might offer particularly useful experiences to be studied by both so-called "developed" and "developing" countries.

As our research highlights, challenges faced by BRICS countries, which are typically shared by all low and middle-income countries, include the need to reorganise enormously costly – and frequently ineffective – bureaucracies, the strive for automation and productivity enhancement, and the increasing mindfulness of the risks presented by the over-reliance on foreign digital technology.

Hence, the analysis of the BRICS approaches to digital transformation and digital sovereignty offers a remarkably useful "testbed", to understand how low and middle-income countries may shape their approaches to these issues in the near future, what type of obstacles they might find and what type of solutions they might adopt.

Besides the increasing global relevance of the BRICS grouping and the fact they represent approximately 42% of the world population, 23% of GDP, and 18% of the global trade,[27] their digital transformation strategies and digital sovereignty approaches may be particularly appealing to other countries facing similar challenges. As the recent expansion of the grouping tellingly demonstrates, the grouping is increasing its appeal to Global South countries,[28] who might be dissatisfied with existing global institutions and pragmatically understand that the global politics and policies of technologies are increasingly tending towards a Post-Western configuration.[29]

[26] Since 2018, the CyberBRICS project has been hosted by FGV Law School in Rio de Janeiro (FGV DIREITO RIO). It is the only existing initiative mapping digital policies and regulations of the BRICS countries with the valuable help of research fellows from all the BRICS countries. Over the past years, the CyberBRICS project has developed substantial research and promoted intense stakeholder engagement in its core policy areas, namely personal data protection, cybersecurity, Internet access, digital transformation, digital industrial policy and AI governance in the BRICS. Further information on the CyberBRICS project can be accessed at www.cyberbrics.info

[27] See e.g. https://brics2023.gov.za/evolution-of-brics/

[28] The 2023 BRICS summit accelerated the expansion of the group, by announcing that six more countries – Argentina, Egypt, Ethiopia, Iran, Saudi Arabia, and the UAE - had been officially invited to join the BRICS+ group, with more expected to join in the future. BRICS. (2023). XV BRICS Summit Johannesburg II Declaration. In Sandton, Gauteng, South Africa. https://is.gd/wbWiXA

[29] Stuenkel, O. (2016). Post-Western world: How emerging powers are remaking global order. London, UK: Polity; Stuenkel, O. (2020). The BRICS and the future of global order (2nd ed.). London, UK: Lexington Books.

2. Towards the construction of a BRICS digital stack

Our research highlights that BRICS countries are devising different ways to balance innovation and regulation in the context of digital transformation. Although the countries are experimenting with diverse approaches to address digital transformation, the members of the BRICS grouping share a common goal of strengthening technological autonomy and promoting local innovation as an essential leverage for national development.

In this context, the move towards digital transformation faces persistent challenges in each country, such as the need for a consistent and well-coordinated approach to governance and regulation, investments in research, development and infrastructure, and continuous capacity building. While not exempted from criticism, the initiatives led by BRICS countries that we will explore throughout this special issue are particularly relevant due to their capacity to leverage strong, sustainable, and sovereign development in the long term.

In the article on “Open government data in the Brazilian digital government: Enabling an SDG acceleration agenda”, Larissa Magalhães discusses how data-driven policies and solution should be embedded within digital government strategies in order to accelerate the sustainable development agenda. The study emphasises how open data initiatives should be aligned with digital policies and utilised to support the establishment of national data infrastructures, complemented by efforts aimed at building capacities and facilitating applicability. Furthermore, the paper emphasises that, in the long term, open government data ecosystems should be structured to facilitate the development of innovative services by companies as well as local governments.

The analysis dedicated to “Digital transformation of the public administration system in Russia: Turning from a service model to ensuring digital sovereignty”’ by Ekaterina Martynova and Andrey Shcherbovich, emphasises that the ongoing Russian digital transformation process offers two dichotomous but important perspectives that need to be considered when addressing digital transformation efforts.

On the one hand, regulatory initiatives and investments at both the federal and regional levels have borne important fruit, illustrating how digital technologies can be exploited for the substantial update of private and public sectors, as in the case of the "Smart City" project for Moscow. On the other hand, the narrative of human-oriented digitalisation of services and convenience through digital public services has been used to justify the trend toward strengthening the state's control through digital means and, particularly, the increase of the surveillance apparatus.

As discussed in the previous sections, the India Stack initiative has driven the country’s transformation, through the adoption of new digital public infrastructure and legislation. In her paper on “Stack is the New Black?: Evolution and Outcomes of the ‘India-Stackification’ Process”, Smriti Parsheera presents the socio-technical imaginaries around the brand “India Stack” and the strong vision of outcome-driven digital transformation.

The paper critically examines the extent to which India has been able to translate its transformative visions into outcomes. Importantly, it depicts a less rosy picture compared with common narratives around the India stack, emphasising reliance on coercive digital adoption strategies, lack of participative decision-making, and insufficient accountability safeguards as some of the fault lines in India's path to fair and equitable digital transformation.

Wayne Wei Wang's article on "Contextualizing Personal Information: Privacy's Post-Neoliberal Constitutionalism and Its Heterogeneous Imperfections in China" provides a rich overview of the complex data privacy narratives in China and how they relate with the county's constitutional framework. The article reveals a heterogeneous system that combines economic rationality, trust in technological advancement, and social experimentation.

The trajectory goes from a collectivist vision to judicial inequality due to the lack of formalization of privacy. The article argues that personal information reflects a post-neoliberal economic logic, balancing economic freedom with market efficiency. It also discusses the need to strengthen privacy constitutionalism to address imbalances between public and private interests, promoting greater protection of rights in the Chinese digital ecosystem.

In her analysis on "South Africa's Digital Transformation: Understanding the Limits of Traditional Policies and the Potential of Alternative Approaches" Senka Hadzic highlights that the country's excitement with the Fourth Industrial Revolution has translated into a powerful support for the implementation of digital transformation in recent years. The article discusses South Africa's information and communications technology infrastructure and the need for policymakers to prioritise bottom-up policy development.

While connectivity infrastructure is the backbone of digital transformation, many South Africans struggle to access decent connectivity and afford the cost of connectivity, while the government prioritises the implementation of emerging technologies to the detriment of infrastructural upgrade. The article provides examples of complementary and important initiatives, such as community networks, for digital transformation policy ambitions that maintain a commitment to equity, inclusion, and sustainable development.

In the final paper of this special issue, Luca Belli, Walter B. Gaspar and Shilpa Singh Jaswant explore "Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries". The papers offers an important contribution to the emerging theoretical discussions on digital sovereignty by defining data sovereignty as the capacity to understand how and why (personal) data are processed and by whom, develop data processing capabilities, and effectively regulate data processing, thus retaining self-determination and control. T

he paper highlights that data sovereignty considerations and data transfers cannot be excluded from digital economy and digital transformation discussions, given the quasi-certainty that digital technologies we utilise will collect and process a large amount of (personal) data, and transfer the collected or generated information in multiple jurisdictions.

This last paper argues BRICS countries have long recognised that the future of their economies and societies depends on mustering digital transformation but have also been amongst the first countries to realise that digitalisation processes can create new types of systemic vulnerabilities that can be exploited by foreign actors. In this perspective, data is considered a critical asset and data flows must be secure and trustworthy, so that control over data can be exercised effectively. The paper considers the various dimensions that compose the concept of data sovereignty and utilises a range of examples from the BRICS grouping to back some key considerations with empirical evidence.

The analyses of this special issue demonstrate that the approaches of the BRICS countries offer some particularly relevant case studies to appreciate what benefits and what risks digital transformation processes

may present. While none of the BRICS models can be deemed as a golden formula for success, their technological, policy and governance experimentations provide valuable learning experiences that should be considered by both developing and developed countries, in their quest for digital transformation and digital sovereignty. Particularly, BRICS experiences – both in terms of successes and failures – tellingly illustrate that a systemic approach to digital technologies, understanding how each element is interconnected and might be dependent form the others is key to design and implement successful, sustainable and sovereign digital transformation processes.