Pre-print version of Belli L., Gaspar, W.B., Singh Jaswant, S. Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. Computer Law & Security Review. Special issue on Digital Transformation in the BRICS Countries (2024)

Data Sovereignty and Data Transfers as Fundamental Elements of Digital Transformation: Lessons from the BRICS Countries

Luca Belli, Professor at FGV Law School, Rio de Janeiro, Brazil

Water B. Gaspar, Researcher at FGV Law School, Rio de Janeiro, Brazil

Shilpa Singh Jaswant, Assistant Professor at Jindal Global Law School, India

Abstract

When talking about digital transformation, data sovereignty considerations and data transfers cannot be excluded from the discussion, given the considerable likelihood that digital technologies deployed along the process collect, process and transfer (personal) data in multiple jurisdictions. An increasing number of nations, especially those within the BRICS grouping (Brazil, Russia, India, China, and South Africa) are developing their data governance and digital transformation approaches based on data sovereignty considerations, deeming specific types of data as key strategic and economic resources, which deserve particular protection and that must be leveraged for national development. From this perspective, this paper will try to shed light on how data sovereignty and data transfers interplay in the context of digital transformations. Particularly, we will consider the various dimensions that compose the concept of data sovereignty and will utilise a range of examples from the BRICS grouping to back some of the key considerations developed with empirical evidence. We define 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. We have chosen the BRICS grouping for three reasons. First, research on the grouping's data policies and digital transformation is still minimal despite their leading role. Second, BRICS account for over 40% of the global population, or 3.2 billion people (which can be seen as 3.2 billion "data subjects" or data producers, depending on perspective, thus making them key players in data governance and digital transformation. Third, the BRICS members have realised that digital transformation is essential for the future of their economies and societies and have shaped specific data governance visions which must be considered by other countries, especially from the global majority, to understand why data governance is instrumental to foster thriving digital environments.

1. Introduction: Untangling data sovereignty, data transfers and digital transformation

Digital transformation is a complex process aimed at leveraging digital technologies to increase sustainability, efficiency, and innovation, thus transforming the organisation of the public and private sectors, and driving the social, economic, environmental, and political evolution of a nation. To be successful this process entails

the establishment of a solid governance mechanism, allowing proper design, implementation, and monitoring of the various phases leading to a successful outcome.[1] Importantly, to harness the potential of digital technologies, public organizations must rethink their traditional structures and understand the role that effective data processing plays in driving the update if such structures. Indeed, the integration of digital technologies requires both public and private sectors to reorganize for improved performance,[2] frequently involving a complete redesign of processes, structures, and modalities of service provision. [3]

When talking about digital transformation, data sovereignty considerations and data transfers cannot be excluded from the discussion, given the quasi-certainty that digital technologies deployed along the process will collect and process a large amount of (personal) data, and transfer the collected or generated information in multiple jurisdictions. In this context, an increasing number of nations, especially amongst the BRICS grouping (Brazil, Russia, India, China, and South Africa) are developing their data governance and digital transformation approaches based on the key role of data sovereignty, considering specific types of data as essential strategic and economic resources, deserving particular protection.

From this perspective, this paper will try to shed light on how data sovereignty and data transfers interplay in the context of digital transformations. Particularly, this paper will consider the various dimensions that compose the concept of data sovereignty and will utilise a range of examples from the BRICS grouping to back some of the key considerations developed with empirical evidence. We define 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. This conceptualisation is constructed upon the complementary definitions of digital sovereignty and artificial intelligence (AI) sovereignty, proposed in previous works, defining digital sovereignty as the capacity to "exercise agency, power and control in shaping digital infrastructure, data, services, and protocols" [4] and AI sovereignty as the "capacity of a given country to understand, develop, and regulate AI systems" [5].

[1] Idowu Lamid, L. et al. A Framework for Digital Government Transformation Performance Assessment and Toolkit for Developing Countries. ICEGOV '21: Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance. (October 2021) Pages 203–215; Belli L. and Magalhães L. (Eds). SmartBRICS: How Brazil, Russia, India, China, and South Africa Are Shaping Their Digital Transformation into Smart Countries. Springer. (2024).

[2] Ashaye, O.R, Irani Z. (2019) The role of stakeholders in the effective use of e-government resources in public services. International Journal of Information Management 49. https://doi.org/10.1016/j.ijinfomgt.2019.05.016.

[3] Tangi, Luca, et al. (2021) Digital government transformation: A structural equation modelling analysis of driving and impeding factors. International Journal of Information Management 60. https://doi.org/10.1016/j.ijinfomgt.2021.102356.

4 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).

5 Belli, L. "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). Belli, L. and Gaspar, W.B. The Quest for AI Sovereignty, Transparency and Accountability. Springer (2024).

1.1. Why focus on the BRICS?

The BRICS grouping has been chosen for three reasons. First, the study of the grouping's data policies and digital transformation initiatives reveal the existence of specific thinking regarding data sovereignty that, in different yet compatible ways, blends developmental, strategic and cybersecurity considerations. Exploring the BRICS data sovereignty rational might be particularly useful to understand how these leading emerging economies leverage data to increase their capacity to develop, regulate and control, and to what extent they diverge or converge in their approaches and interests. However, research on BRICS data governance is still very limited[6] despite the leading role of these countries both in their regional environments and, to an increasingly relevant extent, at the global level, as demonstrated by the recent expansion[7] of the grouping and the ample number of countries who expressed interest in joining it.[8]

Second, it is always useful to remember that BRICS account for over 40% of the global population, or 3.2 billion people (which can be seen as 3.2 billion "data subjects" or data producers, depending on perspective), and they account for more than 26% of global GDP and over 16% of global trade, having acquired an enormous economic and geopolitical weight[9] Conspicuously, over the past decade, BRICS countries have evolved from being largely disconnected or poorly connected at best, to some of the most connected countries in the world[10] becoming global leaders in multiple data-intensive sectors such as ecommerce, online banking and instant online payments.[11] Despite many critics, especially regarding the unrestricted governmental access[12] to personal data that some BRICS countries may enjoy and the extent to which

[6] One of the few existing studies on the matter is Belli L. and Doneda D. Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence. International Data Privacy Law. Oxford University Press. (2022). Several comparative studies dealing with various data governance issues in the BRICS grouping have also been developed by the CyberBRICS project and are available at https://cyberbrics.info/.

[7] At the 15th BRICS Summit, the grouping heads of state "have decided to invite the Argentine Republic, the Arab Republic of Egypt, the Federal Democratic Republic of Ethiopia, the Islamic Republic of Iran, the Kingdom of Saudi Arabia and the United Arab Emirates to become full members of BRICS from 1 January 2024." Due to a change of government, Argentina withdrew its candidature, while Saudi Arabia has not confirmed its adhesion at the time of this writing. BRICS. XV BRICS Summit Johannesburg II Declaration. Sandton, Gauteng, South Africa. (23 August 2023). Paragraph 91. https://brics2023.gov.za/wp-content/uploads/2023/08/Jhb-II-Declaration-24-August-2023-1.pdf.

[8] Reuters. What is BRICS, which countries want to join and why? (21 August 2023). <https://www.reuters.com/world/what-is-brics-who-are-its-members-2023-08-21/> ; Julian Borger. Brics to more than double with admission of six new countries. The Guardian. (24 August 2023). <https://www.theguardian.com/business/2023/aug/24/five-brics-nations-announce-admission-of-six-new-countries-to-bloc>.

[9] See the official website of the Indian 2021 Presidency of BRICS <https://brics2021.gov.in/about-brics>.

[10] See the country reports on "Connectivity across BRICS Countries" developed by the CyberBRICS Project and included in Belli L. and Magalhães L. (Eds). SmartBRICS: How Brazil, Russia, India, China, and South Africa Are Shaping Their Digital Transformation into Smart Countries. Springer (2024). https://cyberbrics.info/connectivity-across-brics-countries/

[11] Particularly interesting and up-to-date data are available in the ACI Worldwide and Global Data reports on "Prime-Time for Real Time", which track and analyse real-time payments volumes, growth, and dynamics of 48 global markets. See ACI Worldwide, Global Data. Prime Time for Real-Time. (April 2022). https://www.aciworldwide.com/real-time-payments-report.

[12] See for instance, Czarnocki,, J. et al. Government access to data in third countries. Study prepared by Milieu under Contract No EDPS/2019/02-13 for the benefit of the European Data Protection Board (EDPB). (2019).

fundamental rights have been fully respected in the context of such digital transformations, the members of the BRICS grouping have become hallmarks of digital transformation.[13]

Third, for several years, the members of the BRICS grouping have realised that digital transformation is an essential element for the future of their economies and societies and that data governance must be considered as a key priority to foster thriving digital environments. On the one hand, data governance is deemed as a priority to guarantee individual rights, provide legal certainty to businesses, and revert the ongoing "data colonialism" typically driven by US-based tech giants[14]. On the other hand, 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.[15]

Indeed, one may contend that the revelations of former National Security Agency (NSA) contractor Edward Snowden did not only represent a global awakening moment, but acted also as a significant catalyst for the BRICS countries' digital policymaking.[16] Since 2013, the BRICS have developed and put into effect a wide range of data-related, cybersecurity, and digital sovereignty policies, to reassert their control over digital transformation and reap the benefits of such processes to bolster national industry and build new digital markets.[17]

In this context, data becomes a critical asset, and countries are recognising the need not only to facilitate flows but also to maintain control over data as a strategic resource, regulated effectively to safeguard its economic, social, and political value. Allowing states, individuals, or corporations to exert control and agency over their data is – or at least should be – one of the fundamental goals of data protection and represents a core dimension of the data sovereignty concept. Importantly, however, we must acknowledge that data sovereignty may have different meanings, depending on the context and actors at stake.

[13] The most recent example is the endorsement and promotion of the Indian concept of Digital Public Infrastructure by the 2023 Declaration of the G20. See G20 New Delhi Leaders' Declaration. New Delhi, India. 9-10 September 2023. https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf. See also Belli L. and Magalhães L. (Eds). SmartBRICS: How Brazil, Russia, India, China, and South Africa Are Shaping Their Digital Transformation into Smart Countries. *cit. supra*.

[14] 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.

[15] BELLI, L. BRICS Countries to Build Digital Sovereignty. Em: BELLI, L. (Ed.). CyberBRICS: Cybersecurity Regulations in the BRICS Countries. Cham: Springer International Publishing, 2021a. p. 271–280

[16] *Idem.*

[17] Belli L. and Doneda D. Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence. *cit. supra* pp. 5-9.

We may posit that, from an international relations perspective, it can refer to a country's capability to utilize in the national interest, and exert control over the data generated within its borders; in the corporate world, it is about protecting and being able to exploit and control the data assets generated in the context of business operations; at the individual level, data sovereignty is the right to have effective oversight and control over one's personal data, famously defined as "informational self-determination"[18]. This latter dimension becomes key for the exercise of individual autonomy and choice, in a context where the boundaries between people's physical bodies and their virtual selves are increasingly blurred.[19]

Additionally, one must recognize the role attributed to sovereignty concerns in internet governance and cybersecurity debates in the past. Described by Sukumar [20] as a divide between "like-minded" and "other-minded" states and by Barrinha and Renard [21] as a divide between those states that defend an "open and free internet" and those prioritizing "cyber sovereignty", there has been a rhetorical and analytical classification of Western states in the first groups and China, Russia and occasional others in the latter.

This stark division certainly describes aspects of the regulatory and diplomatic strategies implemented by these groups of countries, with China and Russia traditionally pushing for "information security" as a multifaceted concept that involves not only data protection and security measures, but also overall aspects of information flow on the internet, pointing to content control and censorship and network fragmentation efforts. However, this severe distinction also paints an overly simplified scenario of the actual concerns involved in current sovereignty debates. It sets an artificial division between "freedom/rights-respecting" and "authoritarian" States that fails to recognize the particular position of developing countries and emerging economies and of the complex "datafied" global value chains dominated by financialized transnational companies headquartered in central economies.

1.2. Rejecting oversimplifications and embracing complexity

[18] The right to "informational self-determination" enshrines the individuals' faculty to exert control over their personal data, as an expression of the human right to have and develop a personality, as famously stated by the German Constitutional Court in the highly influential Census case. See Judgment of 15 December 1983, BVerfGE 65, 1-71, Volkszählung The principle is considered to be a cornerstone of modern data protection and is explicitly enshrined by art. 2 of the Brazilian General Data Protection Law as one of the founding elements of the Brazilian data protection framework.

[19] Kovacs, A. & Ranganathan, N. (2019). Data sovereignty, of whom? Limits and sustainability of sovereignty frameworks for data in India. Data Governance Network. Retrieved from https://cyberbrics.info/data-sovereignty-of-whom-limits-and-suitability-of-sovereignty-frameworks-for-data-in-india/.

[20] 'The Pervasive Informality of the International Cybersecurity Regime: Geopolitics, Non-State Actors and Diplomacy', Contemporary Security Policy 45, no. 1 (2024): 7–44, https://doi.org/10.1080/13523260.2023.2296739.

[21] 'Power and Diplomacy in the Post-Liberal Cyberspace', International Affairs 96, no. 3 (1 May 2020): 749–66, https://doi.org/10.1093/ia/iiz274.

Recent digital sovereignty research has tellingly illustrated the inaccuracy of the abovementioned taxonomies counterposing supposed democratic and non-democratic fields, inevitably leading to gross oversimplifications of a multifaceted debate.[22] Indeed while it is undeniable that some BRICS countries have authoritarian tendencies and poor track records in terms of human rights protection and rule of law, it does not seem justified to adopt false dichotomies necessarily labelling every Western initiative as driven by democratic values and every non-Western one as mere autocratic experiments. Indeed, many developmental and cybersecurity considerations traditionally supported by BRICS countries have been recently embraced wholeheartedly by western countries, which were previously dismissing them.

The adoption of the sovereignty rhetoric by the European Union points at this, showcasing a regulatory strategy toward the digital economy that blends strategic autonomy, industrial and innovation policy, together with digital sovereignty rhetoric.[23] Other examples, eloquent albeit anecdotal, are set by the blockages, or attempts at it, in Western countries (and their former colonies and current "overseas territories", as per the recent block in New Caledonia[24]) of communication applications such as TikTok[25] and of commerce in strategic technologies such as chips and components for AI and quantum computing, based on national security grounds[26]. In addition, the subsequent judicial barriers to data flows between the EU and the US following the Schrems cases have highlighted the enormous risks and, ultimately, illegality of data transfers even towards countries that are traditionally categorised as "democratic"[27]. Hence, it seems that

[22] Jiang, Min and Belli, Luca (Eds). Digital Sovereignty from the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. *cit. supra.*

[23] Since 2020, the President of the European Commission Ursula von der Leyen has prioritized digital sovereignty, stressing that this concept is essential for Europe to be able "to make its own choices, based on its own values, respecting its own rules' in the field of tech" (von der Leyen, 2020). von der Leyen, U. (2020). A Union that strives for more My agenda for Europe: political guidelines for the next European Commission 2019-2024. https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf

[24] Le Monde. France blocking TikTok in New Caledonia sets an unfortunate precedent. (25 May 2024). https://www.lemonde.fr/en/politics/article/2024/05/25/france-blocking-tiktok-in-new-caledonia-sets-an-unfortunate-precedent_6672617_5.html

[25] Euronews, 'Which Countries Have Banned TikTok and Why?', euronews, 14 March 2024, https://www.euronews.com/next/2024/03/14/which-countries-have-banned-tiktok-cybersecurity-data-privacy-espionage-fears; Tom Gerken and Tom Singleton, 'TikTok Vows to Fight "unconstitutional" US Ban', 12 April 2024, https://www.bbc.com/news/articles/c87zp82247yo; Clothilde Goujard and Océane Herrero, 'French TikTok Block in Overseas Territory Sets "Dangerous Precedent," Critics Warn', POLITICO, 16 May 2024, https://www.politico.eu/article/french-tiktok-ban-new-caledonia-overseas-territory-dangerous-precedent-macron-eu/.

[26] Kana Inagaki, Demetri Sevastopulo, and Andy Bounds, 'US Wants Allies to Cut Chip-Related China Exports amid Huawei Alarm', *Financial Times*, 25 April 2024, sec. US-China trade dispute, https://www.ft.com/content/4ecea0a7-a5cd-40b0-8a24-b72c1c1a8996; Jenny Leonard, 'Biden to Sign Order Curbing US Tech Investments in China by Mid-August', *Bloomberg.Com*, 28 July 2023, https://www.bloomberg.com/news/articles/2023-07-28/biden-to-sign-order-curbing-china-tech-investments-by-mid-august; DigWatch Team, 'US Bans Chips, Quantum and AI Investment in China | Digital Watch Observatory', *DigWatch* (blog), 11 August 2023, https://dig.watch/updates/us-bans-chips-quantum-and-ai-investment-in-china.

[27] Caitlin Fannessy, 'The "Schrems II" Decision: EU-US Data Transfers in Question | IAPP', IAPP, 16 July 2020, https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

control of data flows must be considered as a fundamental tool for the realization of national interests, industrial policy and fundamental rights of citizens of Western and non-Western States alike.

This is a particularly dire scenario in the case of Global South countries, especially those of pre-industrial or early industrial economies. In face of global value chains which may be described as "platform capitalism"[28], "surveillance capitalism"[29] or similar concepts aimed at capturing the centrality of data to value production; and of digital markets structured as intellectual monopolies held by companies headquartered in central economies[30]; sovereignty concerns involve issues of industrial and innovation policy and strategy.

The policy space afforded to countries by the architectural choices of Big Tech companies is reduced, especially for developing countries and emerging economies, which are traditionally consumers rather than producers of the digital technologies that are essential for digital transformation. China serves as a prime counterexample, demonstrating how a least developed country – as the country was classified until the early 2000s – can leverage innovation and digitalisation for development with impressive results. Having implemented since the turn of the millennium efforts to foster national development via industrialization and innovation, including the endogenous digital economy, with significant success. Currently, the only Big Tech companies that truly compete with US-based GAFAM companies worldwide are Chinese[31].

Additionally, although the issues of surveillance, content control and censorship do pose actual and concerning threats to the functioning of the internet, these issues inhabit a much more nuanced field today than in the formative years of internet governance in the international system. It is now recognized that libertarian views preaching self-regulation and absolute freedom on the internet can serve as a deterrent of liberties. Telling examples are the "reverse" chilling effect of unmoderated spaces, triggering massive – online and offline – harassment of minorities and vulnerable groups and systemically persecuted peoples,[32] and the

[28] Nick Srnieck, *Platform Capitalism*, Theory Redux (London: polity, 2017).
[29] Shoshana Zuboff, *The Age of Surveillance Capitalism* (London: Profile Books, 2019).
[30] Cecilia Rikap, 'Amazon: A Story of Accumulation through Intellectual Rentiership and Predation', *Competition & Change* 26, no. 3–4 (1 July 2022): 436–66, https://doi.org/10.1177/1024529420932418; Cecilia Rikap, 'The Expansionary Strategies of Intellectual Monopolies: Google and the Digitalization of Healthcare', *Economy and Society* 52, no. 1 (2 January 2023): 110–36, https://doi.org/10.1080/03085147.2022.2131271; Cecilia Rikap, *Capitalism, Power and Innovation; Intellectual Monopoly Capitalism Uncovered*, Studies in the Economics of Innovation 5 (London & New York: Routledge, 2021).
[31] Cecilia Rikap and Bengt-Åke Lundvall, *The Digital Innovation Race: Conceptualizing the Emerging New World Order* (Cham: Springer International Publishing, 2021), https://doi.org/10.1007/978-3-030-89443-6; Shulin Gu and Bengt-Åke Lundvall, 'Introduction: China's Innovation System and the Move towards Harmonious Growth and Endogenous Innovation', *Innovation, Management, Policy and Practice* 8, no. 1–2 (July 2006): 1–26, https://doi.org/10.5172/impp.2006.8.1-2.1.
[32] Mary Anne Franks, 'Fearless Speech', *First Amendment Law Review* 17 (2019 2018): 294–342, https://heinonline.org/HOL/P?h=hein.journals/falr17&i=309; Jon Penney, 'Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study' (Rochester, NY, May 2017), https://papers.ssrn.com/abstract=2959611; Daniel Dias et al., 'Plataformas no Marco Civil da Internet: a necessidade de uma responsabilidade progressiva baseada em riscos', *civilistica.com* 12, no. 3 (29 December 2023): 1–24, https://civilistica.emnuvens.com.br/redc/article/view/931.

near-mandatory adoption of technologies structured around massive data hoovering practices, that are inherently antithetic to the fundamental rights to privacy and informational self-determination, and are typically shielded behind deceptive (dark) patterns and opaque legal structures implemented by Big Tech companies.

Thus, control over how digital technologies are designed, deployed and leveraged for digital transformation is essential to avoid the dire consequences of unchecked rule by algorithm, that can be implemented not only by authoritarian countries but also by unrestrained corporations. The complexities of these relations require regulation and intervention to reassert the capacity to foster national interest, which can only be enacted by sovereign State power.

These multiple conceptions of data sovereignty highlight the complexity of the issue as well as the need for a multifaceted approach to grasp how each one of these dimensions affects digital transformation, and which strategies, policies and institutional arrangements are more likely to deal with data sovereignty concerns effectively, while also fostering the data flows that are necessary for digital transformation.

On the other hand, digital transformation itself can also be considered as rather broad and multifaceted concept, utilised in remarkably elastic fashion by different stakeholders to encompass various forms of integration of digital technologies into organisational practices of institutions, entire market sectors, public administrations, or even democratic processes. Indeed, it can include policies and initiatives aimed at the digitalisation of business processes, provision of public services, or the production and distribution of digital products and services, considering frequently multinational supply chains and human resources. Digital transformation offers opportunities for increased efficiency, innovation, growth, and governmental accountability, but also creates new challenges related to security, data protection, digital colonialism, and centralisation of control in the hands of few entities.

1.3. Leveraging data and technology for sustainable development

Like most large economies, BRICS countries have adopted successive strategies to strengthen their industrial and technological capabilities through technology. The development of the digital economy has been a priority, resulting in the adoption of multiple national policies. Importantly, digital transformation relies on the collection and processing of large amounts of data. These activities are instrumental in allowing organizations to extract insights and make data-driven decisions. Businesses can use customer data to improve their services and governments can leverage data to enhance public services, including healthcare,

education, and transportation. In addition, data processing is instrumental for the development of new technologies, such as artificial intelligence and machine learning, which can revolutionise various sectors.

However, it is increasingly acknowledged that the mounting collection and use of multiple categories of information, including personal, confidential, and strategic data, can easily become a highly risky activity, revealing critical aspects of the institutions, corporations, and entire sectors to be digitised, as well as highly sensitive features of groups of individuals and entire populations. Indeed, the various digital transformation processes have increased the risks not only of data privacy violations, but also of cybersecurity breaches and the use of digital infrastructure for malevolent purposes by adversarial actors, imposing the adoption of solid cybersecurity measures.[33] Thus, data sovereignty, in its multiple dimensions, becomes a highly critical issue as, without control over data, countries, corporations and people risk losing their political and economic power, their autonomy and, ultimately, their fundamental right to self-determination.

In this respect, the recent South African National Policy on Data and Cloud aptly recognises that in "a global and digitally connected world driven by free data inflows and outflows, there is already a realisation that some countries establishing regulatory mechanisms to protect certain types of data regarded as critical for their security and sovereignty." [34] Hence, sound data regulatory frameworks are essential in protecting individual and collective rights, thus triggering sustainable digital transformation processes in the national interest, and facilitating data usage for legal and secure purposes.

Therefore, data sovereignty and digital transformation can be seen as mutually reinforcing concepts. The former plays a crucial role in enabling digital transformation by providing a foundation for data protection. The latter provides opportunities for countries to improve their data infrastructure and governance frameworks and, ultimately, build their data sovereignty. Striking a balance between the needs of digital transformation and data sovereignty seems instrumental to fostering sustainable economic growth while protecting individual rights and ensuring cybersecurity. Particularly, cross-border transfers of data, which are common practice when digital goods or services are provided by foreign companies in the context of many digital transformation processes, can result in multiple risks, including espionage, surveillance, personal data misuse, identity theft, fraud, and cyber-attacks.

These considerations are particularly relevant in the context of international transfers of both personal and non-personal data with critical value, such as information on the functioning of critical infrastructures. With

[33] Belli, L. et al. Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. FGV Direito Rio. (2023). Belli, L. (Ed.). CyberBRICS: Cybersecurity Regulations in the BRICS Countries. cit. supra.
[34] Department of Communications and Digital Technologies of South Africa. National Policy on Data and Cloud (2024). P 8.

the rapid advancement of technology and globalisation, data transfers have become an essential aspect of digital transformation, which typically relies on the adoption of multiple types of Information and Communications Technologies (ICTs) processing and frequently transferring data to foreign servers of subsidiaries, partners or of the same company providing the ICT solutions.

Hence, data transfers may give rise to a complex set of issues, giving rise to notable tensions with the abovementioned data sovereignty logic, requiring well-crafted regulation to protect individuals' rights, preserve national sovereignty, foster cybersecurity, and prevent illegal behaviours. As we will argue in this paper, to address these concerns, (personal) data transfers need to be carefully regulated, so that individual and collective rights are preserved, innovation, research and development are encouraged, markets remain open, and stable and foreseeable rules are clearly defined for businesses.

However, we need to acknowledge pragmatically that, while shaping their regulatory frameworks and digital policies, different nations can be driven by an ample spectrum of – frequently conflicting – regulatory goals, which can produce highly diverging incentives. The strategic policy goals that motivate digital transformation and the elaboration of data policies of each country typically include:

- promoting domestic innovation and stimulating national industries[35]
- developing new digital markets and attract investments[36]
- protecting fundamental rights[37]

[35] Bauer M, Erixon F, Krol M and Lee-Makiyama H (2013). The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce. European Centre for International Political Economy, Brussels. Available at: https://www.uschamber.com/sites/default/files/documents/ files/020508_EconomicImportance_Final_Revised_lr.pdf; Badran MF (2018). Economic Impact of Data Localization in Five Selected African Countries. *Digital Policy, Regulation and Governance*, 20(4): 337–357; Bagchi K and Kapilavai S (2018). Political Economy of Data Nationalism. 22nd Biennial Conference of the International Telecommunications Society (ITS): "Beyond the Boundaries: Challenges for Business, Policy and Society", Seoul, 24–27 June. Available at: http://hdl.handle.net/10419/190347; Taylor RD (2020). "Data localization": The internet in the balance. *Telecommunications Policy,* 44(8): 102003; Mitchell AD and Mishra N (2019). Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute. *Journal of International Economic Law*, 22(3): 389–416.

[36] Casalini F and López González J (2019). Trade and Cross-Border Data Flows. *OECD Trade Policy Paper*, No. 220, OECD Publishing, Paris; Daza Jaller L, Gaillard S and Molinuevo M (2020). The Regulation of Digital Trade: Key Policies and International Trends. World Bank, Washington, DC; Mattoo A and Meltzer JP (2018). International Data Flows and Privacy: The Conflict and Its Resolution. *Journal of International Economic Law*, 21(4): 769–789; Nguyen D and Paczos M (2020). Measuring the economic value of data and cross-border data flows: A business perspective. *OECD Digital Economy Papers*, No. 297, OECD Publishing, Paris; Spiezia V and Tscheke J (2020). International agreements on cross-border data flows and international trade: A statistical analysis. *OECD Science, Technology and Industry Working Papers*, No. 2020/09, OECD, Paris.

[37] Avila R (2020). Against Data Colonialism. In: Muldoon J and Stronge W, eds., *Platforming Equality: Policy Challenges for the Digital Economy*, Autonomy Research Ltd, Crookham Village, September: 47–57; Chander, A. & Lê U. P., Data Nationalism, 64 Emory L. J. 677 (2015). Available at: https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2; Bauer M, Erixon F, Krol M and Lee-Makiyama H (2013). The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce. European Centre for International Political Economy, Brussels; Hill R (2018). Why should data flow freely? Association for Proper Internet Governance (APIG), March. Available at: http://www.apig.ch/Forum%202018%20Policy%20statement.pdf.

- and increasing cybersecurity[38]

This article aims to cope with the complexity of these issues by providing an overview of the different dimensions of data sovereignty and how this concept relates to data transfers and underpins sustainable digital transformation. In the following sections, we will illustrate these points with concrete examples, referring to the approaches adopted by the BRICS countries while critically analysing the reasons for regulatory interventions. Lastly, in the concluding section, we will stress that BRICS countries should consider increasing the compatibility of their regulatory frameworks for intra-BRICS data transfers, to facilitate information flows, while preserving data security.

2. Balancing free data flows and data sovereignty

Ubiquitous connectivity, widespread monitoring and measuring of human activities and the digitalisation of industrial, commercial, social, civic, and political processes mean data flows are a constant phenomenon in today's information society. As stressed in the previous section, these flows become essential to drive digital transformations, and pose both opportunities and risks when one looks at adoption and implementations of specific ICTs.

This section provides an overview of the main benefits and challenges of transborder data flows and how they contribute to digital transformation processes. Subsequently, it will discuss the main dimensions and goals of data sovereignty, stressing the tensions that the promotion of this concept may trigger regarding the free flow of information. Indeed, we argue that the capacity to understand the value of data, how they flow transnationally, how they can be leveraged nationally and, ultimately, being able to effectively regulate the flows of specific types of data is instrumental to build data sovereignty.

2.1 Data flows: benefits and risks

Over the past decades, transborder flows of information have become essential for an increasing number of organisational processes, private and public services, and products, that are critical facilitators of the digital transformation of many different types of organisations. Cloud computing services, financial services, e-commerce and social networking, telecommunications, research, and even modern farming technology are

[38] Chander, A. & Lê U. P., Data Nationalism, 64 Emory L. J. 677 (2015). Available at: https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2; Chen L, Cheng W, Ciuriak D, Kimura F, Nakagawa J, Pomfret R, Rigoni G and Schwarzer J (2019). The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies. T20 Japan Task Force 8: Trade, Investment and Globalization. Available at: https://t20japan.org/policy-brief-digital-economy- economic-development/; Ciuriak D (2020). Economic Rents and the Contours of Conflict in the Data-driven Economy. CIGI Paper, No. 245, Centre for International Governance Innovation; Nussipov A (2020). How China Governs Data, Center for Media, Data and Society, The CMDS Blog, 27 April, available at https://medium.com/center-for-media-data-and-society/how-china-governs-data-ff71139b68d2;

frequently provided in a cross-border fashion, relying on several business functions that depend on free data flows. Such functions include (cyber) security services spanning from threat detection to fraud prevention or Know Your Customer (KYC) systems, to law-enforcement-related activities such as the fight against corruption, money laundering and terrorism. Manufacturing operations, customer services and human resources of most large corporations and a mounting number of small or medium-sized corporations willing to embrace digitalisation are also increasingly dependent on cross-border information transfers.

Data transfers have acquired an increasingly vital role for the global economy. According to the International Chamber of Commerce, the contribution of data transfers to global GDP is estimated to be around $2.8 trillion to global GDP and is expected to grow to $11 trillion by 2025[39]. The private sector is an essential beneficiary of mechanisms enabling trustworthy and secure data transfers. Indeed, companies rely on these flows to implement their digital transformation processes, digitalising their day-to-day business interactions with customers, suppliers, and partners; modernise their operations; detect cyber threats; and compete more effectively in a variety of sectors as diverse as agriculture, healthcare, manufacturing, banking, and shipping.[40] This is one of the main reasons why, since 2019, the G20, which includes all BRICS countries, agreed to foster the so-called Data Free Flow with Trust ("DFFT")[41], recognizing the need to improve legal

[39] International Chamber of Commerce. White Paper on Trusted Government Access to Personal Data Held by the Private Sector. (22 August 2022).
[40] *Idem.*
[41] G20, 'G20 Osaka Leaders' Declaration', June 2019, https://mofa.go.jp/policy/economy/g20_summit/osaka19/documents/final_g20_osaka_leaders_declaration.html; Aidan Arasasingham and Matthew P. Goodman, 'Operationalizing Data Free Flow with Trust (DFFT)', *Center for Strategic & International Studies* (blog), 13 April 2023, https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft.

interoperability[42] between national legislative systems to allow free and secure international data flows.[43] Such a priority has been also reiterated by the G7 that, since 2021, has started emphasizing the importance of cross-border transfers, including in the G7 Digital Ministers' Roadmap, which recognizes that the "ability to move and protect data across borders is essential for economic growth and innovation."[44]

One of the main benefits of facilitating data flows is that it promotes international cooperation and provision of services at the global level, allowing organising business enterprises in a multinational fashion while reducing costs and increasing efficiencies and scalability. For instance, most of the consumer applications and back-office tools we use daily, and the vast majority of generative AI systems and machine learning applications, rely on cloud computing resources provided by multinational providers – typically dominant US tech giants such as AWS, Google Cloud and Microsoft Azure – that can extract, transfer and generate data, while providing such services.

On the contrary, restricting data flows to keep specific categories of data inside the domestic jurisdiction is frequently deemed by policymakers as helpful to promote job opportunities, domestic production and the development of technology, [45] but that comes with its drawbacks. On the one hand, it can result in fragmentation of the Internet, which could lead to higher opportunity costs for small and medium-sized

[42] Interoperability is usually described as "the ability to transfer and render useful data and other information across systems, applications, or components". See International Telecommunication Union (ITU). GSR discussion paper: Interoperability in the digital ecosystem. (2015). Interoperability is therefore the property enabling the exchange and use of information across heterogeneous technologies and systems. This concept is increasingly important as interconnected technologies, continuously receiving and transmitting data, are becoming the norm. From a technical perspective, interoperability is fostered by adopting shared technical standards and protocols. that allow all Internet users to exchange information and to utilise services in a cross-border fashion. The concept of interoperability has been associated with different benefits, fostering openness, and positively affecting competition and innovation, while also increasing efficiency in the provision of a greater diversity of content and services. Interoperability is also associated with reductions in the cost of technologies, as it promotes scalability. Similar benefits may be achieved through the promotion of interoperability from a regulatory perspective – i.e. through legal interoperability – rather than from an exclusively technical one. In this perspective, legal interoperability is the property of fostering compatibility of rules concerning the same topic within different jurisdictions or different administrative levels within a state. Like technical interoperability, legal interoperability stimulates the exchange of information within different systems. As such, interoperability of both technical and legal systems allows individuals - and, particularly, Internet users - to access and provide services in a cross-border fashion and to enjoy equal right-protection within different systems thanks to compatible (or common) rules, principles, and procedures. Shared rules and principles amongst various juridical systems have the potential to reduce transaction costs, deflating barriers to cross-border trade, and foster non-measurable benefits, such as the protection of fundamental rights. See Weber, R. Legal Interoperability as a Tool for Combatting Fragmentation. Global Commission on Internet Governance Paper Series (4) (2014); Belli L. and Doneda D. Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence. Cit supra; Belli, L. and Zingales, N. "Interoperability to foster open digital ecosystems in the BRICS countries". in Chinese Academy of Cyberspace Studies. Shared Vision for the Digital World: Insights from Global Think Tanks on Jointly Building a Community with a Shared Future in Cyberspace. The Commercial Press. (2023).

[43] G20. "G20 Osaka Leaders' Declaration". (29 June 2019).

[44] G7 Digital and Technology Ministers. G7 Digital and Technology Track – Annex 2: G7 Roadmap for Cooperation on Data Free Flow with Trust. (28 April 2021). http://www.g8.utoronto.ca/ict/2021-annex_2-roadmap.html.

[45] Nigel Cory. The False Appeal of Data Nationalism, Why the Value of Data Comes From How It's Used, Not Where It's Stored. Information Technology & Innovation Foundation. (2019). https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where/

companies, reducing the entrance of potential service providers and competitors, which might increase efficiencies.[46] On the other hand, it is important to emphasise that the mere storing of data on national territory is not per se a guarantee of development or innovation, which need solid strategies, investments and definition of precise roles and responsibilities to be promoted. Additionally, fragmentation may reduce the options for local companies to use the most convenient data processing service provider and bear huge costs to transfer data outside their jurisdiction even for day-to-day activities like human resource management.[47,48]

It is important to acknowledge that, in most countries, a large number of business sectors, such as insurances, digital marketing, consumer electronics, etc. are quintessentially dependent on free data flows. While some categories of data need increased protection for a variety of reasons, spanning from cybersecurity to data privacy to national interests, we must stress that free and secure data flows can represent considerable gains. As an instance, analysing the growing expansion of connected objects in the context of the so-called Internet of Things, GSMA (2021) estimated that under conditions of open cross-border data flows, Brazil and South Africa are likely to increase considerably their respective GDPs, exports and employment rates.[49] Conversely, the establishment of restrictions on transnational data flows is likely to reduce economic gains in these areas,[50] unless such restrictions are defined int he context of a well-conceived, well-funded and carefully implemented strategy for data-driven development.

Of course, before harnessing data for any purpose, most countries require compliance with data protection obligations, including the need to assess the privacy and data protection risks of the operations involved. States recognise the utility of processing personal data and have created the means for data to flow legally. Any regulation on the flow of data will involve different interests: data privacy and security vs. and cross-border trade and cooperation. Both individuals and organisational actors may have conflicting priorities: they may consider data control – be it for privacy or confidentiality reasons – as a valuable criterion to choose a product or service; however, they might consider more valuable the financial gain derived from the

[46] UNCTAD. Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, United Nations Conference on Trade and Development, UNCTAD/DER/2021.
[47] Exploring International data flow governance- Platform for Shaping the future of Trade and Global Economic Interdependence, White Paper 2019 December, World Economic Forum. Available at https://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf.
[48] Taylor RD. 2020. "Data localization": The internet in the balance. Telecommunications Policy, 44(8): 102003
[49] Notably the Brazilian GDP could increase by up to 0.5 and the South African one by up to 2.6 per cent in South Africa; exports could increase by up to 2.4 per cent in Brazil, and up to 3.1 per cent in South Africa; and employment: could increase by up to 0.2 per cent in Brazil, and up to 1.3 per cent in South Africa. GSMA (2021). Cross-Border Data Flows: The impact of data localisation on IoT. Global System for Mobile Communications Association, London.
[50] *Idem.*

convenience of using digital services presented as "free" but de facto entailing the wavering of individual control over personal data.[51]

Since the early 80s, the current paradigm of data protection legislation has emerged, where the regulation is based not only on the protection of individuals' rights and on security considerations but also on the provision of legal certainty to businesses, allowing regulated flows of data, instead of prioritising closed systems where data flow is the exception. Yet, one interest must not be sacrificed for the other. It is clearly mentioned in the provision of Article XIV of the General Agreement on Trade in Services (GATS) that the agreement signatories are not prevented from adopting measures "necessary to secure compliance with laws or regulations [...] including those relating to: *the protection of the privacy of individuals in relation to the processing and dissemination of personal data*." The 'necessity' requirement does not mean picking one over the other but, in the lack of international consensus on what is tools are "necessary" to achieve data privacy and cybersecurity, one can only assume that the balance between these important priorities and trade can always be contested.[52]

Indeed, to balance the two interests, there is a need to determine the value of privacy, security and trade, which is an empirical exercise, since different stakeholders in different states at different moments may have radically different perceptions about them, motivated by valid and understandable considerations.[53] In response to this need, Chander and Schwartz suggest that negotiating a global agreement on data privacy, like the GATS, might be an ideal solution, although particularly hard to achieve, and running the risk to deprioritise privacy compared with trade concerns.[54]

In this context, it becomes essential to explore the different dimensions of the data sovereignty debate, their rationales and goals, to be able to assess the "necessity" of any restriction to free data flows that countries may be willing to implement.

[51] Solove, D. J., The Myth of the Privacy Paradox (January 29, 2021). 89 George Washington Law Review 1 (2021), GWU Legal Studies Research Paper No. 2020-10, GWU Law School Public Law Research Paper No. 2020-10; Belli. L, Schwartz. M. Louzada L. (2017). Selling your Soul while Negotiating the Conditions: From Notice and Consent to Data Control by Design. Health and Technology Journal. 7(4), 453-467. Topical Collection on Privacy and Security of Medical Information. Springer-Nature.

[52] In this sense, see Neha Mishra. (2020). Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation? 19 World Trade Review. 341, 356.

[53] Chander, Anupam and Schwartz, Paul M. (2023) Privacy and/or Trade. Georgetown Law Faculty Publications and Other Works. 2444. https://scholarship.law.georgetown.edu/facpub/2444.

[54] *Idem.*

2.2 Data Sovereignty and its goals

Data sovereignty debates have changed the understanding of international borders. Under international law, a sovereign state is the primary subject of international norms and has the competence to exercise the fundamental right to self-determination to make autonomous choices and decisions for its citizens.[55] Conceptualising this in relation to "data", data sovereignty can be defined as a state exercising its right to self-determination, in terms of development in the national interest, and obligation to protect fundamental rights, at least in terms of privacy, informational self-determination and (cyber)security, over the (personal) data of its citizens.

While the right to self-determination is typically associated with a collective dimension, exercised by the state, it is important to note that it also has a well-established informational dimension, which has been constructed by jurisprudence, doctrine, and legislation over the past four decades as a fundamental right of the individual, upon which relies personal data protection. The German Federal Constitutional Court was the first to recognise a fundamental right to "informational self-determination" in the landmark Census case, in 1983, constructing this right as an expression of the right to the free development of personality, underpinning "the capacity of the individual to determine the disclosure and use of his/her personal data."[56] As such, informational self-determination is considered as the individuals' right to exert control over their personal data, being entitled to know what information about them are collected, by whom, for what purposes and with what entities such data are shared. Similar considerations have led the Brazilian legislator, the Brazilian Supreme Court and, again, the Brazilian Congress to enshrine "informational self-determination" as a cornerstone of Brazilian data protection law.[57] The notion of informational self-determination can be seen as a bedrock of personal data protection from a Brazilian perspective, although the concept remains loosely defined in the Brazilian context.

The need for individuals' control over their personal data has also prompted the Supreme Court of India to recognise a new fundamental right to privacy as part of the Indian Constitutional framework in the landmark

[55] Peter Malanczuk, Akehurst's Modern introduction to international law, 7th edn., 77-78; Samantha Besson, Sovereignty, International Law and Democracy, *European Journal of International Law*, Volume 22, Issue 2, May 2011, Pages 373–387, https://doi.org/10.1093/ejil/chr029.

[56] See Judgment of 15 December 1983, BVerfGE 65, 1-71, Volkszählung.

[57] The principle is explicitly enshrined by art. 2 of the Brazilian General Data Protection Law as one of the key principles on which the Brazilian data protection framework relies. CyberBRICS. The Brazilian General Data Protection Law – Unofficial English version. CyberBRICS Project. (2020). https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/ The Brazilian Supreme Court explicitly considered it a cornerstone of a new fundamental right to data protection in Brazil in the IBGE case. This judgement led the Brazilian Congress to enshrine data protection as a new fundamental right, amending article 5 of the Federal Constitution.

Puttaswamy case, in 2017. [58] It is interesting to note that India has been pioneering the use of techno-legal tools to increase individual control over data, by establishing the Data Empowerment and Protection Architecture (DEPA)[59]. The DEPA framework was initially presented by the government think thank Niti Aayog and is based on the "electronic consent framework" proposed in 2017[60] and implemented in the financial sector since 2020 through the Account Aggregators system, established by the Reserve Bank of India. [61] This consent-based data sharing framework creates a software architecture based on public protocols, aiming at baking informational self-determination into Indian technology, "empowering all individuals with control over their personal data." [62]

Hence, when considering data sovereignty from a self-determination perspective, we can identify an individual dimension grounded on the data-subjects' capacity to exercise control over their data, as well as a collective dimension. This latter dimension consists in the state's capability to exercise the fundamental right of peoples to freely determine and pursue one's economic, social, and cultural development. Such prerogatives include the capacity to independently choose, develop, and adopt digital technologies and decide how (personal) data can be collected, processed, and stored, as well as having a say as to how and where data should generate value. [63]

More broadly, we must remember that the informational dimension of the right to self-determination is a recent evolution of the concept. Indeed, this right has been traditionally considered in its collective conception enshrined as the first article of both the Charter of the United Nations and the International Covenants of Human Rights, according to which "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." In this perspective, self-determination is deemed as a primary principle or principle

[58] The Supreme Court of India constructed the fundamental right to privacy based on three constitutional provisions: Article 14, guaranteeing the right to equality; Article 19, guaranteeing the right to freedom of speech, expression, and assembly; and Article 21 guaranteeing all persons right to life and personal liberty. Bhandari, V., Kak, A., Parsheera, S., Rahman, F. (2017). An analysis of Puttaswamy: The Supreme Court's privacy verdict. IndraStra Global, 11, 1-5.

[59] 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. Vol. 18 Issue 2 (2022); Belli & Doneda (2023). cit. supra.

[60] See Niti Aayog, Data Empowerment And Protection Architecture: Draft for Discussion (2020) <https://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf> accessed 13 October 2021

[61] See Reserve Bank of India, 'Account Aggregator Ecosystem API Specifications' (8 November 2019) <https://api.rebit.org.in/> accessed 14 October 2021

[62] See Niti Aayog (n 88) 26-27

[63] idem

of principles, as it plays an instrumental role to allow individuals and peoples to enjoy their human rights, thus being an enabler of other fundamental rights. [64]

Since the 1980s, various academic debates emerged in Brazil as regards the interest of regulating transnational data flows, noting that such flows were clearly asymmetric, tending to concentrate value generation only in the most developed countries. This asymmetry was already identified as evidence that information was (and still is) extracted in peripheral countries such as Brazil but processed to create innovation, jobs, and, critically, taxable income, where the multinational corporation extracting the information is headquartered, rather than in the country of extraction. [65]

Hence, when asserting sovereign control over the data extracted from their citizens, or empowering them with such control, nations can redefine their digital borders to stipulate how data can be shared, monetised, and used in the national interest. This seems to be one of the key concerns underpinning the digital transformation that China undertook over the past decades, with the aims to leverage the regulatory system in favour of domestic industries[66] focusing on key sectors where the government has strongly backed domestic players, including via huge public investments and subsidies in ICTs and facilitating the export of Chinese products and services[67].

As noted by Belli, since 2015, China has carefully blended industrial policy and regulation, adopting the ambitious "Internet Plus" and "Made in China 2025" plans with a large focus on the expansion of Internet access, the IoT and its enablers, followed by a National Plan for Artificial Intelligence Development and the AI Governance Principles, to reap the benefits of connectivity and datafication.[68] These strategic documents were accompanied by massive investments and by the adoption of an overarching Cybersecurity Law, in 2017, followed by two key documents setting the tone of future data-related legislation: the Personal Information Security Specification and the E-Commerce Law, in 2018.

[64] Luca Belli. "To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)." In New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms, ed. Steven Feldstein. Washington, DC: Carnegie Endowment for International Peace, 2023. http://dx.doi.org/10.2139/ssrn.4465501

[65] Marcos Dantas describes these dynamics in his work published in 1996, stressing that, during the Brazilian dictatorial period, some types of data flows were restricted for strategic and protectionist reasons, despite the ideological alignment of the Brazilian military dictatorship with the U.S. and the continuous support of the latter to the Brazilian regime. Dantas M. A Lógica do Capital-informação. Contraponto (1996).

[66] Made in China 2025: Global ambitions Built on local protections, 2017, US Chamber of Commerce, https://www.uschamber.com/assets/archived/images/final_made_in_china_2025_report_full.pdf.

[67] Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, United Nations Conference on Trade and Development, UNCTAD/DER/2021.

[68] 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 Chinese approach has led to a thriving domestic high-technology sector, able to produce national champions, such as Huawei which emerged as global leader in connectivity equipment, digital devices, and 5G technology.[69] At the same time, data harvested through ICTs is utilised to support national development and state control capabilities. The Chinese strategy tellingly exemplifies how national planning, strong investments and regulation, coupled with public-private implementation are key to promote development and digital transformation while asserting data sovereignty.

This seems to be also the ambition of the recent South Africa's National Policy on Data and Cloud, published on 1st June 2024. The document explicitly advocates for "data sovereignty" considering data as a resource to be used in the national interest, stressing that data transfer agreements "must promote national interests, including socio-economic development, security, and sovereignty" besides complying with data protection and data security laws. [70] In this context, the South African government seems to consider itself as the legitimate entity tasked with the construction of the South African data sovereignty.[71]

However, one must be mindful that, while all BRICS countries now enjoy data protection legislation, their national frameworks also include varying degrees of governmental access to personal data, which can be almost antithetic to informational self-determination.[72] It is important to acknowledge that the legitimate exercise of data sovereignty by national governments consist in the capacity to steer the use of data produced domestically to promote the national development and to enable individuals control over their personal data, but cannot be equalled to unchecked governmental access to personal data. While the former is clearly compatible with collective interest, the former may be hardly reconciled with rule of law, due process, and individual rights. In light of the above, we can argue that data sovereignty encompasses widely different purposes and meanings that reflect political preferences and cultural values of specific countries and regions.[73] It is important that we stress that the BRICS countries are not an exception to such heterogeneity of approaches.

[69] Matthew S. Erie & Thomas Streinz, 'The Beijing Effect: China's Digital Silk Road as Transnational Data Governance' (2021) 54 NYU J Int'l L & Pol 1

[70] In the same page, the Data and Cloud Policy also notes that "Government data that incorporates content pertaining to the protection and preservation of national security and sovereignty of the Republic shall be stored only in digital infrastructure located within the borders of South Africa." Department of Communications and Digital Technologies of South Africa. National Policy on Data and Cloud, p. 27 (2024).

[71] Calandro E. South African Digital Sovereignty at the Crossroad of Securitisation and Development. In Belli L. and Jiang M. Digital Sovereignty in the BRICS Countries cit. supra; Musoni M. et al. Global approaches to digital sovereignty: Competing definitions and contrasting policy. ECDPM Discussion Paper No. 344. (2023).

[72] See for instance, Jan Czarnocki et al. Government access to data in third countries. cit. supra.

[73] Couture S. and Toupin S. (2019). What Does the Notion of "Sovereignty" Mean When Referring to the Digital? New Media and Society, 21(10): 2305–2322.

Indeed, concerns prompting data sovereignty debates may span from the protection of individuals' fundamental rights and the increase of domestic firms' capacity to use data to catch up with foreign technology companies, to the governmental access to personal data for law enforcement and national security purposes. These latter objectives can easily mutate into surveillance. In this context a new dimension to data sovereignty is emerging, where data are considered as geopolitical assets. Some nations, like most of the BRICS grouping members, are increasingly considering the importance of guaranteeing "strategic autonomy"[74], where data and digital technologies are protected, under a national policy, as a core and strategic asset to be preserved by the government. Securing data, building domestic capacity as well as controlling critical digital infrastructure are also widely included in these policies, which are discussed below.

Most developed and developing nations have different priorities, with a strong embodiment of the social and cultural contexts of each group. A long link to histories of colonialism and dominance has raised the fear among developing nations of digital or data colonialism, which may be deeper than historical colonialism. Couldry and Mejias argue that the subject of this kind of colonialism is not just region-specific or foreign powers taking over domestic resources - data colonialism affects all. The authors call out the comparison of personal data to a natural resource as an appropriation of human lives in the hands of corporations. This ongoing phenomenon includes constant monitoring of individuals and data extraction from them during every social interaction that can be 'appropriated, abstracted, and commodified'.[75]

In this perspective, the capacity to have a clear understanding of how and why (personal) data are processed, and which entities are involved in the processing, becomes essential from both an individual and a collective perspective. Hence the transparency and explicability of processing plays a key role as enabler of data sovereignty understood as informational self-determination for individuals but also state capacity to understand and regulate who is extracting valuable insight from data, both in economic and strategic terms. These considerations play an essential role in terms of cybersecurity, developmental and economic policy, and strategic autonomy, as discussed in the following sections.

2.3 Cybersecurity dimension

Rising cybersecurity concerns are one of the main reasons for States' and individuals' interest in reasserting data sovereignty. Since the most egregious cybersecurity violations revealed by former NSA contractor Eward

[74] See Azmeh S and Foster C (2018). Bridging the Digital Divide and Supporting Increased Digital Trade: Country Case Studies. Discussion Paper, GEGAfrica, Global Economic Governance, Pretoria. Available at: http://www.gegafrica.org/item/862-bridging-the-digital-divide-and-supporting-increased-digital-tradecountry-case-studies; Aktoudianakis A (2020). Fostering Europe's Strategic Autonomy – Digital sovereignty for growth, rules and cooperation. European Policy Centre and Konrad-Adenauer-Stiftung, 18 December.

[75] Couldry and Meijas, p. 343

Snowden in 201376, several cases across different jurisdictions have demonstrated over the years the deep and widespread impact of cybersecurity violations over individuals' fundamental rights as well as on the functioning of public and private services.Platform companies like Yahoo, LinkedIn, Sina Weibo and Meta (through Facebook) have suffered some of the most impactful data breaches in the 21st century, with violations affecting the personal data of millions and even billions of their users.77

Other services, such as marketplaces (Alibaba), media companies (Adobe), credit scoring companies (possibly Serasa Experian, in the biggest data leak in Brazilian history, with 223 million people affected[78]) and others also make the roster[79]. Notable cases have also involved digital public services, such as India's national digtial identity infrastructure Aadhaar (815 million Indian citizens affected)[80] and Brazil's CADSUS[81], a digital registry system for users of the national public health system. Both systems have suffered various types of attacks that exposed personal and even sensitive data of users and citizens, exploiting vulnerabilities.By introducing solid cybersecurity governance frameworks, including mandatory data security measures and effective enforcement of such measures, nations may protect their citizens' data and infrastructure against potential risks.

Importantly, cybersecuurity must be seen as polyhedral concept aimed at covering several concerns, such as risks to personal or confidential information, critical infrastructure, democratic processes and institutions, and cybercrimes.[82] Hence, information security is only one dimension of the larger cybersecurity debate but

76 The Guardian. NSA Files. s.d. https://www.theguardian.com/us-news/the-nsa-files Margulies, P. Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy. Indiana Journal of Global Legal Studies. Vol. 24, No. 2 (2017), pp. 459-496. https://doi.org/10.2979/indjglolegstu.24.2.0459

77 For ad illustrative compilation of some of the most flagrant cybersecurity incident of the past decades, see Michael Hill and Dan Swinhoe. The 15 biggest data breaches of the 21st century. CSO Online. (8 November 2022). https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html

78 Luca Belli, 'The Largest Personal Data Leakage in Brazilian History', openDemocracy, 3 February 2021, https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history/.

79 *Idem.*

80 Prajeet Nair, 'Aadhaar Breach Report: Reactions on Freedom and Privacy', CSO Online, 11 January 2018, https://www.csoonline.com/article/567915/aadhaar-breach-report-reactions-on-freedom-and-privacy.html; Manmath Nayak, 'In Massive Aadhaar Data Leak, Personal Information of 815 Million Indians On Sale On Dark Web: Report', 31 October 2023, https://www.india.com/news/india/in-massive-aadhaar-data-leak-personal-information-of-815-million-indians-on-sale-on-dark-web-report-6460420/.

81 'Registro de Incidentes com Dados Pessoais', Ministério da Saúde, accessed 21 June 2024, https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/registro-de-incidentes-com-dados-pessoais/registro-de-incidentes-com-dados-pessoais-1; 'Dados de 2,4 milhões de brasileiros no SUS teriam vazados. Governo nega', ConvergenciaDigital, accessed 21 June 2024, https://www.convergenciadigital.com.br/Internet/Dados-de-2%2C4-milhoes-de-brasileiros-no-SUS-teriam-vazados%2E-Governo-nega-50442.html?UserActiveTemplate=mobile%2Csite.

82 Belli, L. et al. Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. FGV Direito Rio. (2023); 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, p. 1–14. (2021); Fichtner, L. What kind of cyber security? Theorising cyber security and mapping approaches. Internet Policy Review, v. 7, n. 2. (2018).

is an essential one. Thus, the requirement to categorise data into personal and non-personal, sensitive and non-sensitive, confidential and non-confidential, etc. and locally store specific categories of information within the national jurisdiction, is instrumental to give the state agency to regulate and enforce data security. Indeed, in addition to classifying data, cybersecurity frameworks may require the implementation of specific security measures, based on the result of such categorisation.

[83]As an instance, the Chinese Data Security Law (DSL)[84] defines stringent requirements for processing "important data", "core state data", and "sensitive data", and extends to all automated data-processing the requirement to comply with the notorious Multi-Level Protection Scheme (MLPS),[85] which was established already in 1994 and generalised by the 2017 Cybersecurity Law (CSL).[86] The DSL extends data localisation obligations, which mandate the storage of data in servers located in the national territory, to the aforementioned "important data".

Article 21 of the DSL prescribes that "[e]ach region and department, shall stipulate a regional, departmental, as well as relevant industrial and sectoral important data specified catalogue, according to the data categorization." Important data listed in such catalogues may encompass an enormous spectrum of data linked to economic development, national security, the public interest, individuals' rights, and corporates' interests. Such important data are subject to special security requirements as well as international transfer restrictions.[87] While the latest Chinese policies have strengthened data localisation obligations, it is important to note that such requirements were already present in the country, via the 2017 Cybersecurity Law (CSL), and were probably inspired by Russia's data localisation provisions introduced in 2015.[88]

---

[84] See the unofficial English version of China's Data Security Law: https://www.cov.com/-/media/files/corporate/publications/file_repository/data-security-law-bilingual.pdf

[85] The MLPS is a cybersecurity compliance scheme that applies to virtually all organisations in China. It was first introduced in 1994 and subsequently updated in 2019, in accordance with Article 21 of the Cybersecurity Law. The MLPS classifies systems based on the damage that a hypothetical vulnerability of the system may pose to China's cybersecurity. The scheme requires all network operators to ensure that their networks are protected against interference, damage, or unauthorised access. Under MLPS, all network operators are required to classify their infrastructure and application systems on a 1 to 5 scale and fulfil protection obligations accordingly. Systems ranked at 3 or higher are considered higher-stake, and are subject to notably stricter obligations, including on data security. See Belli, L. Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. *cit. supra.*

[86] See http://lawinfochina.com/display.aspx?id=22826&lib=law

[87] Appendix A of the Draft Guidelines for Cross-Border Data Transfer Security Assessments provides a detailed list of "important data" in different sectors. For instance, in the military sector, "important data" encompass information on the name, quantity, source and agent of purchased components, software, materials, industrial control equipment test instruments, geographical location, construction plans, security planning, secrecy level, plant drawings, storage volume, reserves of military research, and production institutions. See http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm

[88] Shcherbovich, A. (2021). Data protection and cybersecurity legislation of the Russian Federation in the context of the "sovereignization" of the internet in Russia. In L. Belli (Ed.), CyberBRICS: Cybersecurity regulations in the BRICS countries. Springer.

The requirements introduced by the CSL were further specified by the 2021 Critical Information Infrastructure Security Protection Regulations that apply to Critical Information Infrastructure (CII), according to which operators are responsible for the security of networks. [89] The purpose of bringing such provisions is to protect CII including both traditional sectors and large-scale commercial internet services. The operators of CII, according to Article 37 of CSL, must store all important data and personal information gathered and produced during operations within the territory of China. CII norms require operators to form dedicated bodies for security management and include people who have been approved by the Chinese Ministry of Public Security and Ministry of State Security.[90]

The Regulations also prescribes that the Cyberspace Administration of China will conduct a security assessment on companies, especially multinational ones, which as per their business model need to send data across borders, before allowing them to transfer data. Moreover, Article 40 of CSL says that the requirement of security assessment as per CSL prevails over all other laws, meaning that any Chinese law allowing cross-border data flows needs to be reassessed in light of the CSL.

In this context, it is important to discuss whether data localisation requirements increase the state's agency over data that can provide easier access for surveillance purposes. To assert political power, states can control data, data flows, and digital technologies to "take back control" and "sovereignty" from foreign technology firms and trading partners.[91] The localisation requirements can be argued to prevent foreign adversarial governments from accessing sensitive information that could result in national security threats. Since 2020, the US has been trying to ban the Chinese app TikTok for allegedly threatening "national security, foreign policy and the economy of the United States".[92] In spite of the absence of any evidence supporting the claim, the lawmakers are concerned that sensitive information of users, may go into the hands of the Chinese government, which may use the platform to interfere into democratic processes.[93] In 2020, the US government asked the company to store the data of US users in a domestic cloud server, and for the parent company of Tiktok, ByteDance, to sell off some of its stakes in US companies while setting up an office in the

[89] Triolo, P. et al. (2021, August 18). After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come Into Focus, DigiChina, Stanford University, https://digichina.stanford.edu/work/after-5-years-chinas-cybersecurity-rules-for-critical-infrastructure-come-into-focus/

[90] Article 14 Critical information infrastructure security protection regulations

[91] Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L. J. 677 (2015). Available at: https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2

[92] Kaitlyn Tsai, Regulation of data localisation and how the legal profession play a role, 34 Georgetown Journal of Legal Ethics 1355, 2021.

[93] *Trump Agrees to TikTok Deal with Oracle and Walmart, Allowing App's U.S. Operations to Continue*, CNBC (Sep. 19, 2020), https://www.cnbc.com/2020/ 09/19/trump-says-he-has-approved-tiktok-oracle-deal-in-concept.html

US.[94] In 2024, the US Congress adopted specific legislation mandating the sale of Tiktok to a trusted US business in less than a year or face a ban in the country.[95]

More states have joined the effort to ban the Chinese app and some states, such as India, France, New Zealand, Canada, and the UK, have successfully done so, either completely or partially, for similar reasons.[96] In China, all personal data must be kept within the borders of China, unless provided and allowed so otherwise by the Cyberspace Administration of China (CAC). Further, the China Personal Information Protection Law (PIPL) differs in its treatment of certain kinds of data, such as any critical information and personal information of a certain quantity[97] that must be stored and produced within the domestic borders, unless provided and allowed so otherwise by another state authority, i.e., the State cybersecurity and informatization department.[98] PIPL allows transfer when conditions under Article 38 are satisfied and procedures are fulfilled.

Localisation requirements are increasingly seen not just as a tool for security concerns. However, scholars like Anupam Chander argue that such measures are ineffective because foreign surveillance can continue even with the localisation requirement.[99] This is possible because of technologies that allow for the infiltration of foreign networks and the collection of data on a large scale.[100] Localisation requirements alone, however, certainly do not prevent domestic cybersecurity and privacy violations and threats. Indeed, localising data in only one jurisdiction may increase the risk of breaches to data confidentiality, integrity and availability due to cyberattacks that become easier when servers storing data are localised in one place.[101] At the same time, data localisation can also facilitate national surveillance, when governmental access to data is loosely regulate, as in several BRICS countries.102

2.4 Strategic autonomy

The Chinese policy emphasis on data regulations and cybersecurity for strategic autonomy reflects Beijing's clear understanding of the key strategic advantage brought by having sound data frameworks, and its

[94] Ibid
[95] Riley Beggin, 'Congress Passes TikTok Sell-or-Ban Bill, but Legal Battles Loom', USA TODAY, 23 April 2024, https://www.usatoday.com/story/news/politics/2024/04/23/congress-passes-tiktok-ban-biden-china/73424172007/.
[96] Why countries are trying to ban Tiktok, The New York times, April 12, 2023, https://www.nytimes.com/article/tiktok-ban.html
[97] This limit on quantity of information is provided by the State cybersecurity and informatization department
[98] Article 40 PIPL
[99] Chander A (2020) Is Data Localization a Solution for *Schrems II*?, 23 *Journal of International Economic Law* 3, p. 771–784, https://doi.org/10.1093/jiel/jgaa024
[100] Ibid.
[101] Ibid, p. 717
102 See for instance, Jan Czarnocki et al. Government access to data in third countries. *cit. supra.*

consideration of (personal) data as an increasingly essential and valuable asset.[103] As discussed above, nations are moving towards strategic autonomy, becoming increasingly weary of the dependencies that digital technologies can create and of the risk that full reliance on foreign technology may entail.104

In this perspective, strategic autonomy aims at creating digital capabilities allowing a country not to be dependent on external actors. This is clearly not only pursued by the BRICS as a key policy objective. For instance, the EU has not only embarked on a legislative restructuring of its digital policies to restrict the undue influence and abuse of dominance by U.S. tech giants and in doing so set global standards, but it has also tied digital sovereignty and technological "strategic autonomy" as top priorities.[105] Post-Snowden, the world has strengthened its data protection, following the European lead with the 2016 GDPR, which unleashed the so-called "Brussels Effect".[106]

Recently, perceiving the EU's lag in advanced digital infrastructure development and deployment (e.g. China-U.S. rivalry in AI and 5G technologies) and digital market (e.g. U.S. dominance in digital platforms and services in the EU), the EU has passed the Digital Markets Act and the Digital Services Act in 2022 in a bid to further beef up EU's control over its digital sovereignty. While the effectiveness of these norms in achieving their goals is far from granted, they are alimenting the so-called Brussels effect, by stimulating new platform-related policymaking around the world, aimed at reining in tech giant, with particular regard to their capacity to manipulate markets and regulate online content. In fact, there are two antagonistic perceptions of the impact this normative approach can concretely have. A rather optimistic vision is prvided by Hoeffler and Mérand (2023) who consider the DMA as a piece in a broader digital sovereignty jigsaw, arguing that the "market-directing face of the DMA becomes even more visible when seen in the context of several other policy proposals that build more directly on the repertoire of digital sovereignty, or what Seidl and Schmitz aptly call the EU's 'geodirigist turn'. For some business players, the DMA is only one piece of a 'tsunami of legislation' which aim to regenerate Europe's industrial capacities."[107]

[103] Triolo, P. et al. (2021, August 18). After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come Into Focus, DigiChina, Stanford University, https://digichina.stanford.edu/work/after-5-years-chinas-cybersecurity-rules-for-critical-infrastructure-come-into-focus/

104 Belli L. and Jiang. M. Digital Sovereignty in the BRICS: Structuring Self-Determination, Cybersecurity, and Control. Jiang M. & Belli L. (Eds) Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge University Press. (2024)

[105] 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

[106] Bradford, A. (2019). The Brussels effect: How the European Union rules the world. Oxford, UK: Oxford University Press.

[107] 'Digital Sovereignty, Economic Ideas, and the Struggle over the Digital Markets Act: A Political-Cultural Approach', *Journal of European Public Policy* 0, no. 0 (2023): 11, https://doi.org/10.1080/13501763.2023.2294144.

In this sense, the DSA/DMA combination points to efforts by the EU directed especially at American and Chinese Big Tech companies, aiming at controls that might, on one side, impose upon these firms the values and practices enshrined in European legislation and, on the other side, provide breathing space for new European companies trying to compete in concentrated markets. This is most evident in the portability and interoperability requirements, which hark back to a motivation to "challenge the status quo where a few digital giants control significant portions of the online space, limiting consumer choice and stifling innovation"[108].

This latter vision, however, may consider the impact of the DSA and DMA from an overoptimistic perspective, which fails to consider the need for particularly lengthy enforcement, without which the achievement of the desired impact, particularly of the DMA, seems highly unrealistic. As aptly stressed by Caffarra (2023), the DMA's aim is to regulate gatekeepers by allowing potential complainants "to get a larger share of the rents extracted by the platform (in other words, partake in the profits of monopoly) rather than a vision for how to truly deconcentrate markets."109 In other words, the DSA may facilitate "competition on the platform, not competition to the platform"110, thus frustrating the stated purpose of achieving strategic autonomy and digital sovereignty by enabling innovation and competition. On the other hand, looking at the DSA's obligations toward platforms, especially very large online platforms, one can recognize aspects of digital sovereignty as reassertion of control over of data flows and content regulation by regulating the digital architectures within which these flows occur, which can extend Europe's reach [111].

As regards this latter point, it is interesting to highlight that some BRICS countries, notably China and Russia, started considering the definition of their – very strict – content regulation frameworks as essential to assert their sovereignty in the digital space already in the early 2000s[112] and aligned their aspirations internationally through the Shanghai Cooperation Organisation (SCO).[113] Indeed, since 2011, the SCO has elaborated upon

[108] Chinmayi Sharma, 'A Marketplace for Data Portability', SSRN Scholarly Paper (Rochester, NY, 27 February 2024), 1, https://doi.org/10.2139/ssrn.4741065.

109 Caffarra C. Of Hope, Reality, and the EU Digital Markets Act. Tech Policy press. (6 May 2024). https://www.techpolicy.press/of-hope-reality-and-the-eu-digital-markets-act/

110 *Idem.*

[111] Daphne Keller, 'The EU's New Digital Services Act and the Rest of the World', Verfassungsblog, 7 November 2022, https://verfassungsblog.de/dsa-rest-of-world/.

[112] For an analysis of the BRICS content regulations see Belli, Luca and Curzi, Yasmin and Britto Gaspar, Walter, Online Content Regulation in the BRICS Countries: A Cybersecurity Approach to Responsible Social Media Platforms (2023). Luca Belli, Yasmin Curzi, Walter Gaspar. Responsible Behaviour in Cyberspace: Global Narratives and Practice. Brussels: Publication Office of the European Union. (2023). http://dx.doi.org/10.2139/ssrn.4424913

[113] 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. See http://eng.sectsco.org

an International Code of Conduct for Information Security[114] updated in 2015[115] recognising that information security includes content control within digital media and reaffirming that "policy authority for Internet-related public policy issues is the sovereign right of States."

However, as the Russian experience tellingly explains, building strategic autonomy – or constructing digital autarchy, as in the Russian case – is far from being an easy task, even when a massive state is behind such a policy objective. The Internet Sovereignty aims at reproducing China's course of action in the early 2000s with its "Great Firewall of China", which created a large national intranet that was connected through only limited channels to the rest of the internet outside the country. Such a controlled environment enables both tight content control and protectionism, allowing Chinese tech giants to emerge under the guidance of the Chinese Communist Party.

However, when China decided to implement its plan, at the dawn of the 21st century, the internet was much less pervasive than it is today. The Chinese citizens of the early 2000s were not reliant on the open internet for their everyday lives. The Russians of the 2020s, in contrast, have grown accustomed to a relatively open internet, making the necessary financial resources, personnel, technology, and disruption caused by the disconnection of the Runet significantly more complicated and intensive, compared to the situation in the early 2000s in China. [116]

2.5. Economic Dimension

Until 2020, areas like e-commerce and digital trade were discussed within the broad heading of trade and investment. In the 2020 Summit, BRICS converged to introduce digital economy as a separate agenda under the BRICS Economic Partnership 2025 in tapping the potential of BRICS through digital transformation and the promotion and transfer of cutting-edge technologies, enhancing accessibility and quality of digital goods and services with the use of ICTs, addressing the digital divide, promoting skills, and developing digital literacy.[117] In consonance with this, the 2022-2026 General Strategy of the BRICS-led New Development Bank (NDB) included financing digital infrastructure projects, such as overland and subsea cables, landing stations, telecom towers, base stations, and associated facilities.[118]

[114] See https://digitallibrary.un.org/record/710973
[115] For a comparison of the differences between the 2011 and 2015 versions of the Code, see https://openeffect.ca/code-conduct/
[116] Daucé, F., & Musiani, F. (2021). Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: An introduction. First Monday, 26(5). https://doi.org/10.5210/fm.v26i5.11685
[117] Strategy for BRICS Economic Partnership 2025. November 2020. https://www.tralac.org/documents/resources/external-relations/brics/4200-strategy-for-brics-economic-partnership-through-to-2025-november-2020/file.html
[118] New Development Bank (2022). Scaling Up Development Finance for a Sustainable Future, NDB's General Strategy: 2022-2026. https://www.ndb.int/wp-content/uploads/2022/07/NDB_StrategyDocument_Eversion-1.pdf

Since, 2021, BRICS countries resolved to enhance cooperation through the BRICS E-commerce Working Group to examine the experience of BRICS and other countries and international associations in the field of e-commerce, with particular regard to consumer protection.119 However, there seems to be divergence among BRICS regarding policies on e-commerce, notably as regards, their relationship with the WTO and its members. This is because the divide between developed and developing countries in trade negotiations is heightened by differing preferences among developing nations. India, for instance, opposes forming e-commerce rules before concluding the Doha Development Agenda (DDA) negotiations.[120] India, alongside many other developing and least developed countries, prioritizes establishing its e-commerce policies and digital regulations over international e-commerce rules, emphasizing the need for policy space in data management for sectors like cloud computing and data storage.[121] Consequently, India and South Africa abstain from WTO e-commerce negotiations.

In contrast, China took a leading role reflecting its dominant position in global e-commerce and its desire to protect its commercial interests and competitiveness against the US and other developed countries.[122] Brazil and Russia take a more proactive stance in the joint statement initiative (JSI) negotiations, driven by their significant e-commerce markets and established regulatory frameworks.[123] In this context, they are actively submitting proposals and forming small working groups to promote regulatory cooperation and data flow. This divergence within the BRICS countries underlines the varied negotiation positions among WTO members, complicating consensus-building efforts, within both WTO and BRICS. [124]

Moreover, it is important to emphasise that, for the last decade, there has been constant anxiety associated with geopolitical risks due to the dependency on the dollar among BRICS members and willingness to increase independent from the dollar , 'de-dollarising' the BRICS financial market. To these longstanding concerns, we

119 BRICS. 2021 BRICS Framework for Ensuring Consumer Protection in e-Commerce. (2021).https://brics2023.gov.za/wp-content/uploads/2023/07/Framework-for-ensuring-consumer-protection-in-e-commerce-2021.pdf

120 United Nations Conference on Trade and Investment (UNCTAD) (2020). What Is at Stake for Developing Countries in Trade Negotiations on E-Commerce? The Case of the Joint Statement Initiative. United Nations: UNCTAD/ DITC/TNCD/2020/5. https://unctad.org/publication/what-stake-developing-countries-trade-negotiations-e-commerce

121 Liang, Wei & Zeng, Ka (2023). China and the BRICS in WTO E-Commerce and Fisheries Negotiations. In China and the WTO. Edited by Gan, Henry, Raess, Damian & Zeng, Ka. Cambridge University Press.

122 Liang, Wei & Zeng, Ka (2023). China and the BRICS in WTO E-Commerce and Fisheries Negotiations. In China and the WTO. Edited by Gan, Henry, Raess, Damian & Zeng, Ka. Cambridge University Press. https://www.cambridge.org/core/books/china-and-the-wto/china-and-the-brics-in-wto-ecommerce-and-fisheries-negotiations/B2CE3A3232BDDED813E50189F3F0C7B5

123 Thorstensen, Vera, Mascarenhas, Fernanda, and de Paola, Giulia (2019). E-Commerce in Brazil: Where We Are in Terms of Regulatory Practices. CCGI – No 15, Working Paper Series. https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/28007/TD%20510%20-%20CCGI_15.pdf?sequence=1&isAllowed=y

124 Liang, Wei & Zeng, Ka (2023). China and the BRICS in WTO E-Commerce and Fisheries Negotiations. In China and the WTO. Edited by Gan, Henry, Raess, Damian & Zeng, Ka. Cambridge University Press. https://www.cambridge.org/core/books/china-and-the-wto/china-and-the-brics-in-wto-ecommerce-and-fisheries-negotiations/B2CE3A3232BDDED813E50189F3F0C7B5

should some BRICS policymakers anxieties regarding future potential economic sanctions from the U.S. and Europe abruptly, weaponizing the international financial system, and cutting off key dollar- and euro-based financial channels used for transactions with crucial trading partners.[125] Additionally, there is fear that these sanctions could be employed to freeze the dollar and euro assets of an emerging market's central bank, major trading partners, or political leaders. These fears were solidified after the US and European economic sanctions froze half of the Russian central bank's gold and foreign exchange reserves, as a repercussion for the Russian invasion of Ukraine. Half of the Russian banks were cut off from the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system by the US and European governments. [126]

De-dollarisation has opened potential for BRICS local currencies to be used in new financial channels. For instance, Renminbi, the Chinese currency also known as Yuan, was previously used to facilitate transactions involving Chinese firms when trading with firms from BRICS but now it is used even when the local currency is different from the Renminbi.[127] After the economic sanctions against Russia, as per sources, Russian exports invoiced in renminbi grew from 0 to 16 percent.[128] Furthermore, in 2014, the People's Bank of China (PBoC) started developing a digital currency, the Digital Yuan and, in 2016, established the Digital Currency Research Institute that promoted the development of a Chinese Central Bank Digital Currency. The PBoC has successfully established a new Digital Public Infrastructure (DPI) regulated by the Chinese *Data Security Law* and *Personal Information Protection Law*. Conspicuously, in addition to fostering domestic electronic money transfers, the Digital Yuan has wider geopolitical dimensions, such as facilitating international payments in Yuan and ultimately, the de-dollarisation of the global economy.

Similar efforts are also being made by India to increase the use of the Rupee where it is not a local currency, including by promoting the international adoption of its Unified Payment Interface (UPI), a DPI dedicated to online payment. In addition to their national efforts, there are joint BRICS efforts to move away from

[125] Greene R. (2023). The Difficult Realities of the BRICS' dedollarisation Efforts- and the Renmibi's Role. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/12/the-difficult-realities-of-the-brics-dedollarization-effortsand-the-renminbis-role?lang=en

[126] Greene R. (2022). How Sanctions on Russia Will Alter Global Payments Flows. Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/03/04/how-sanctions-on-russia-will-alter-global-payments-flows-pub-86575.

[127] Greene R. (2023). The Difficult Realities of the BRICS' dedollarisation Efforts- and the Renmibi's Role. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/12/the-difficult-realities-of-the-brics-dedollarization-effortsand-the-renminbis-role?lang=en

[128] den Besten T., Di Casola P., & Habib M.M (2023). Geopolitical Fragmentation Risks and International Currencies. in 'The International Role of the Euro'. European Central Bank https://www.ecb.europa.eu/pub/ire/article/html/ecb.ireart202306_01~11d437be4d.en.html.

traditional payments and to digitalise payment systems between different countries 'allowing businesses and consumers to securely and seamlessly make and receive payments in their local currencies'.[129]

Another important limb of the digital economy for the BRICS is taxing data intensive digital services. In 2023, the global trade value of digitally delivered services reached 3.82 trillion USD, or 54 percent of the total global services trade. [130] This presented an opportunity for the BRICS to tax foreign digital services that might not only increase the national tax revenue but also create a favourable market for the domestic industries. As discussed above, any regulation on digital trade will involve different interests: the individuals, who consume the service and generate data; the firms, that provide services and process data from consumers; and the state, which regulates the movement of data. For states, besides economic interests, cyber and national security play an important role in justifying regulations. China with its 2017 Cybersecurity Law imposed restrictions to 'safeguard cybersecurity, protect cyberspace sovereignty, and national security'. India allows processing of data for a legitimate purpose such as sovereignty and security. [131]

Another major reasons why countries continue to tax big tech companies is the profit shifting. These companies are well structured to shift their profits to pay significantly lower effective tax than traditional companies. [132] Digital services tax (DST) has emerged because of it and has even gained momentum among BRICS. Digital taxes can be traced from the efforts of the OECD to reform the international tax system addressing the tax challenges arising from digitalisation of the economy.[133] Countries, instead of taxing data processing directly, are taxing digital services provided by a company. This may act as a strong fiscal reason not to collect all the data of an individual for corporate benefit.

Approaches to taxation however differ amongst BRICS. India and other OECD countries like Austria, France, Italy, and the United Kingdom are taxing digital services provided by big tech companies located in the US.[134]Countries like South Africa and Russia have imposed or increased the scope of their value added tax

[129] About BRICS PAY project. BRICS PAY. https://www.brics-pay.com
[130] Global Trade Outlook and Statistics (2024). World Trade Organisation. https://www.wto.org/english/res_e/booksp_e/trade_outlook24_e.pdf
[131] The Digital Personal Data Protection Act (DPDA). 2023. Section 7. (India)
[132] Borders, Kane, et. al. Digital Service Taxes. 2023. halshs- 04174657
[133] Tax challenges Arising from Digitalisation- Report on Pillar One Blueprint: Inclusive Framework on BEPS, OECD.
[134] Office of the United States Trade Representative. 2021. "USTR Welcomes Agreement with Austria, Rance, Italy, Spain, and the United Kingdom on Digital Services Taxes". October 21, 2021.. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/october/ustr-welcomes-agreement-austria-france-italy-spain-and-united-kingdom-digital-services-taxes Accessed 27 April, 2024. ;Govindarajan, V., Srivastava, A., Warsame, H., Enache L. 2019. " The Problem with France's Plan to Tax Digital Companies". Harvard Business Review. July 17 2019. https://hbr.org/2019/07/the-problem-with-frances-plan-to-tax-digital-companies Accessed April 26 2024.

(VAT) to include digital services from foreign suppliers.[135] China remains reticent about imposing taxes on digital services. In a general sense, electronic services are subjected to VAT but there is no specific tax in place for digital services by foreign suppliers.[136]

Conclusion

BRICS regulations concerning data flows, both personal and non-personal, develop amidst a complex bundle of State interests, encompassed by the often-elastic nomenclature of sovereignty, and a shifting scenario of digital transformation. This article has described a set of emerging regulatory initiatives and tendencies in BRICS countries and their data protection, cybersecurity, strategic autonomy, developmental, and economic dimensions. This regulatory landscape is an ongoing construct, which allows space for enhancing digital cooperation, identifying and/or building legally interoperable regulations amongst BRICS countries.

Indeed, it is of utmost important to stress that being sovereign does not mean being isolated, it means being able to retain full awareness, self-determination and control.137 This, in turn, can contribute to compatible regulatory frameworks and governance models tailored to the characteristics of the grouping and their component States, which may be more palatable to satisfy the needs of Global South countries, such as countering technological dependency and digital colonialism, but would require considerable attention to ensuring fundamental rights.

Achieving such convergence could take various, non-exclusive paths. Legal interoperability may be achieved by the more traditional process of adequacy decisions between nations regarding their data protection and cybersecurity frameworks. This process would require close contact between relevant agencies in BRICS countries, which could plant the seed of further collaboration in capacity-building, and information sharing. A similar and supporting pathway would be adding the issue to the diplomatic toolset in BRICS fora, by which

[135] Ponomareva K (2023). Digital Transformation Challenges to the Tax Security of the State in Russia and Other BRICS Countries. *BRICS Law Journal* 10(4):142-161. https://doi.org/10.21684/2412-2343-2023-10-4-142-161; South Africa: Practical considerations for foreign suppliers of electronic services to South African customers. Baker McKenzie. January 2023. https://insightplus.bakermckenzie.com/bm/tax/south-africa-practical-considerations-for-foreign-suppliers-of-electronic-services-to-south-african-customers; VAT on Electronically Supplied Services in Russia. Clifford & Chance. December 2018. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2018/12/vat-on-electronically-supplied-services-in-russia-status-and-prospects.pdf

[136] Ponomareva K (2023). Digital Transformation Challenges to the Tax Security of the State in Russia and Other BRICS Countries. *BRICS Law Journal* 10(4):142-161. https://doi.org/10.21684/2412-2343-2023-10-4-142-161

137 Belli L. & Costa Barbosa A. Brasil precisa liderar o debate global sobre soberania de IA. O Globo. (21 April 2024). https://oglobo.globo.com/opiniao/artigos/coluna/2024/04/brasil-precisa-liderar-o-debate-global-sobre-soberania-de-ia.ghtml ; Belli L. What is AI Sovereignty and Why Brazil Can Lead the Global Debate About It. Medianama. (14 June 2024). https://www.medianama.com/2024/06/223-views-ai-sovereignty-brazil-global-debate/

BRICS countries set common goals related to cooperation regarding research development and regulatory frameworks.

Setting up the tools for a convergent regulation of data flows in BRICS countries, based on shared principles rights and obligations, respecting national sovereignty, while promoting transparency, research and development, and cooperation, is crucial to solidify certain understandings of these issues from the perspectives of these countries. Current movements in free trade agreements point to a growing role of digital trade and, by consequence, data protection in the lexicon of international instruments[138] often negotiated at very different conditions than those of South-South cooperation efforts.

As we have stressed along this article, the capacity to understand how and why data are processed, which entities are involved in the processing, and being able to effectively regulate such processing is the essence of data sovereignty, be it from an individual or a state perspective. Indeed, these considerations are not only the basis of personal data protection and its cornerstone, informational self-determinations, but play an instrumental role to allow state to build solid cybersecurity, developmental and economic policies, and strategic autonomy.

However, the elaboration of data-related international agreements able to effectively address the abovementioned considerations may require a remarkably complex diplomatic process, even if limited at the intra-BRICS level, where countries may have similar and compatible opinions on such issues. A possibly more agile alternative aimed at achieving at least some of the goals related to personal data governance is the establishment of shared binding corporate rules and model contractual clauses, with a strong focus on data security. This private law alternative could draw upon existing experiences, such as ASEAN's Model Contractual Clauses (MCCs) and the Ibero-American Data Protection Network's (RIPD) Model International Transfer of Personal Data Agreement, as well as China's Personal Information Export Standard Contract and Measures on the Standard Contract. Some essential components of such an arrangement should be:

1. The definition of legally interoperable mechanisms based on shared/converging data governance rules, building on recent BRICS Summit Declarations calling for intra-BRICS cooperation and legal frameworks on cybersecurity;
2. The adoption of BRICS model contractual clauses with a strong focus on data security and the mutual recognition of binding corporate rules (contractual clauses);

[138] Mira Burri, 'Data Flows versus Data Protection: Mapping Existing Reconciliation Models in Global Trade Law', in *Law and Economics of Regulation*, ed. Klaus Mathis and Avishalom Tor, Economic Analysis of Law in European Legal Scholarship (Cham: Springer International Publishing, 2021), 129–58.

3. The establishment of joint data-governance related research and capacity-building actions.

BRICS leaders have made explicit their appetite for the development of "legal frameworks of cooperation among BRICS States [and] a BRICS intergovernmental agreement on cooperation" [139] and BRICS policies are starting to be seen as models influencing other countries – including BRICS countries themselves. The development of convergent and legally interoperable data protection frameworks should be uppermost in the list of their policy priorities as it is one of the few regulatory fields that is simultaneously key to protecting individuals, providing juridical certainty to businesses, and fostering international trade.

Growing cooperation and legal interoperability amongst BRICS countries regarding digital policy is possible; it is already happening and is explicitly advocated by BRICS leaders themselves. The degree of policy convergence now depends on how much BRICS will manage to synchronise their political priorities and, critically, how much they will decide to dare in the implementation of the tools that are at their disposal. BRICS should seize the opportunity to further enhance their digital cooperation, promoting a vision of data governance, based on solid and mutually respectful data sovereignty[140] could offer a suitable framework for cooperation and implementation of the recent BRICS commitment to enhance intra-BRICS cooperation on digital policies and to test the new BRICS Science, Technology, and Innovation (STI) Architecture, which aims at enabling and evaluating BRICS initiatives in the STI field.

In this perspective, BRICS countries can foster a new approach to data governance, which can be compatible with the most modern data protection standards but can include sound data sovereignty considerations, based on the aforementioned dimensions. If such policy experiments are undertaken by the BRICS grouping, the result may be an interesting "post-western data governance model" [141] that can be particularly useful to cater to the digital transformation needs of the Majority World.

[139] BRICS (XIII BRICS Summit) 'New Delhi Declaration' (9 September 2021) <https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-51.pdf> accessed 8 October 2021.

[140] The Roadmap was proposed at the 8th BRICS Summit in Goa, India, and adopted at the 9th BRICS Summit in Xiamen, China. See https://brics2021.gov.in/BRICSDocuments/2017/Xiamen-Declaration-2017.pdf.

[141] 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. Vol. 18 Issue 2 (2022).