Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

UNDERSTANDING THE BRICS COUNTRIES, THEIR DIGITAL COOPERATION, AND THEIR EMERGING DATA PROTECTION ARCHITECTURES

Luca Belli

Abstract

This chapter aims at introducing the emerging data architectures of the BRICS countries. It stems from the research elaborated by the CyberBRICS project, which is the first and only initiative dedicated to the analysis of the digital policies in the BRICS countries (Brazil, Russia, India, China, and South Africa). The chapter notes that, while not renowned for their commitment to data privacy, all BRICS countries undertook major regulatory developments regarding data protection in recent years, elaborating new legislation, updating existing one or establishing new regulatory agencies, while also introducing innovative institutional and normative elements in their frameworks. We contextualise the BRICS and their efforts to cooperate on digital issues, stressing a tendency towards convergence and "legal interoperability" of several aspects of their national data protection policies, and exploring some examples of how BRICS countries are innovating data protection. These points are analysed in detail along the volume. Lastly, we argue that BRICS may seize the opportunity to further enhance their cooperation on data protection, considering the increased convergence and compatibility of their data architectures, implementing the recent BRICS commitment to enhance intra-BRICS cooperation on digital policies. This latter point will be explored in the conclusion of this volume.[1]

[1] This chapter is largely based on 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). https://academic.oup.com/idpl The authors relied on the inputs and feedback of a group of extremely talented researchers from the CyberBRICS project, hosted by the Center for Technology and Society at FGV Law School, Rio de Janeiro. Special thanks go to Walter Britto Gaspar, Smriti Parsheera, Wei Wang, Sofia Chang, Larissa Chen, and Sizwe Snail.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

CONTENTS

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

1. UNDERSTANDING THE BRICS COUNTRIES, THEIR DIGITAL COOPERATION, AND THEIR EMERGING DATA PROTECTION ARCHITECTURES

1.1. Introduction

The BRICS countries – namely, Brazil, Russia, India, China, and South Africa, and their expanding group of partners – are an unusual grouping[2] and even more unusual is the thought that such countries may be trailblazers regarding a topic such as personal data protection. Indeed, while their economic and geopolitical relevance can hardly be denied and, on the contrary, is attracting an increasing number of countries[3] notably from the so-called "Global South", "Majority World" or "Global Majority"[4], the

[2] In 2001, the Goldman Sachs economist Jim O'Neill, also known as Lord O'Neill of Gatley, coined the expression BRICs, without the capital "S", to refer to Brazil, Russia, India, China. South Africa would join the grouping only at a later stage, at the 3rd BRICS Summit, in 2011, when the group adopted an upper-case "S" in the acronym, officially including the African country. The countries were originally grouped as, according to O Neil's projections, they would have experienced a similar and particularly relevant phase of new and advanced economic development. See Jim O'neill, 'Building Better Global Economic BRICs' [2001] (66) Goldman Sachs Global Economic Papers <https://www.goldmansachs.com/insights/archive/archive-pdfs/build-better-brics.pdf> accessed 7 October 2021

The long-term projections on the BRICs growth were further described by O'Neill's colleagues, Dominic Wilson and Roopa Purushothama, in 2003. See Dominic Wilson and Roopa Purushothaman, 'Dreaming With BRICs: The Path to 2050' [2003] (99) Goldman Sachs Global Economic Papers <https://www.goldmansachs.com/insights/archive/archive-pdfs/brics-dream.pdf> accessed 8 October 2021.

[3] 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." 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 ; Carien du Plessis, Anait Miridzhanian and Bhargav Acharya. BRICS welcomes new members in push to reshuffle world order. (24 August 2023). https://www.reuters.com/world/brics-poised-invite-new-members-join-bloc-sources-2023-08-24/ 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>

4 Over the past two decades, the "Global South" term has enjoyed an increasingly relevant use by academics, policymakers, and other stakeholders alike in discussions related to an ample spectrum of world politics issues. As stressed by Haug, Braveboy-Wagner and Maihold, this prominent concept is used "as a general rubric for the decolonised nations located roughly, but not exclusively, south of the old colonial centres of power" and encompasses multiple understandings, including "socio-economic marginality, multilateral alliance-building and resistance against global hegemonic power". Sebastian Haug, Jacqueline Braveboy-Wagner & Günther Maihold (2021) The 'Global South' in the study of world politics: examining a meta category, Third World Quarterly, 42:9, 1923-1944. Although it represents a powerful concept, the Global South label may be less useful as regards digital governance and data governance, as the digital and data power dynamics do not necessarily reflect old colonialist relationship i.e. domination of former colonisers on former colonies. In this perspective the use of the term Majority World or Global Majority may be more interesting. This latter term refers to all countries formally designated as "Developing Countries", "Least Developed Countries", or even "Third World Countries". While Majority World, Global Majority and Global South can interchange, the former may be preferrable as it defines the community based on the demographic and social majority it represents. Thus, it brings a less geographical and more demographic conception, while still identifying the territories and nations that have been invaded, looted, and violently subjugated by colonisers over the past centuries – in some cases until the late seventies – and often continue to be subject to new globalised forms of control. Anibal Quijano. (2000) 'Coloniality of Power, Eurocentrism, and Latin America', Nepantla: Views from South, 1(3), pp. 533– 580; Everisto

human rights track record of some of the group members is far from stellar, and some BRICS members have been routinely accused of gross violations of fundamental rights. From the perspective of Western[5] scholars, notably European ones, whose approach to data protection is solidly grounded on fundamental rights, a certain scepticism about the BRICS grouping in general and their personal data frameworks may be understandable. Indeed, several rankings categorise some of the BRICS as "partly free", "not free" or even "authoritarian regimes,"[6] and Russia has visibly left the Council of Europe, ceasing to be a party to the European Convention on Human Rights, in September 2022, after the members of the human rights body voted to suspend the Russian Federation's rights of representation, due to its invasion of Ukraine.

The authors of this volume are well-aware of the abundant critiques[7] regarding the human rights track records of some BRICS countries and of the importance of carefully considering this issue when assessing the extent to which a given system effectively protects personal data. In this respect, each following chapter dedicated to a BRICS member includes an introductory section providing the reader further human right-related context, so that the data architectures described in this volume can be

Benyera. (2021). The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data. Routledge. Similarly, the "Global Majority" term is also used, although less frequently, to describe people of African, Asian, Latin American, and Arab descent, who constitute approximately 85 percent of the global population. See Rosemary M. Campbell-Stephens. Educational Leadership and the Global Majority. Decolonising Narratives. Palgrave Macmillan. (2021).

5 Stuart Hall's work provide a fascinating analysis of the conception of "the West" highlighting that this term has been constructed to describe a type of social, political, and economic system, supposedly indicating development, compared with "the rest". The idea of the West can be traced back to the Enlightenment as an indicator of modernity, tending to impose European categories and norms to assess global phenomena. The concept is not connected to a fixed geographical, although typically includes Europe and the US. Stuart Hall. "The West and the Rest: Discourse and Power." In Stuart Hall et al. (Eds.). Modernity: An Introduction to Modern Societies. 184-227. Oxford: Blackwell Publishers, 1996. In this book, we refer to Western legal systems, when considering the systems whose core elements have been initially defined by Roman law and subsequently by French, German and US legal thinking, based on Legal Formalism, which dominated legal doctrine in the late nineteenth century, until the rise of Legal Realism at the turn of the century. These evolutions have been accompanied by consecration of three key feature of contemporary Western political culture: the limitation of government, through the rule of law; some degree of institutional separation of the economy and of science from government and religion; and the organisation of popular participation into governance through elections. These features have become essential elements of so-called "liberal democracies", forming the conceptual basis from which Western observers inevitably assess other systems. Karlson Preuß. Legal Formalism' and Western legal thought. in Jurisprudence, 14:1, 22-54. (2023); Erich Weede. Ideas, Institutions and Political Culture in Western Development. Journal of Theoretical Politics. Volume 2, Issue 4 (1990). This book starts from the assumption that all the above elements are neither universally defined nor uniformly and universally applicable. On the contrary they are typically adapted to the cultural idiosyncrasies of all nations. Hence, while Western legal and political thinking has proven to be a valuable combination of rule of law, democracy, and human rights, it would be incorrect, to assume that the combinations produced by Western systems are necessarily the best possible options or should be considered the ones based on which other systems must be assessed.

6 See for instance the Global Freedom Scores, the Internet Freedom Scores, and the Democracy Scores elaborated by annually by Freedom House and available at https://freedomhouse.org/countries/freedom-world/scores

7 See for instance, Jan Czarnocki 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).

understood in their complexity. Indeed, the reason why the term "architecture" has been chosen is precisely to stress how the combinations of regulatory, institutional and technological choices of the BRICS countries give rise to specific structures shaping their approaches to data governance.

While all BRICS countries have adopted data protection legislation, the unrestricted access that some of the BRICS members' governments enjoy as regards their citizens' personal data may undermine the very essence of data protection principles, especially in terms of the full enjoyment of informational self-determination. As we stress in the introductory sections of each chapter, unchecked governmental capacity to access personal data poses a significant threat to the rule of law, due process, and individual rights. This book, however, strives to adopt a balanced stance, acknowledging that government's capacity to steer the processing of (personal) data can also have significant benefits in terms of development, thus paying a fundamental role in building what can be defined as "data sovereignty"[8].

These considerations are particularly relevant for Global South countries, where the capacity to data in the national interest can prove essential to enable policymakers to design and implement more effective, targeted, and evidence-based policies and projects. Yet, we emphasise that lack of proper safeguards regulating government's ability to access and process vast amounts of citizen data inevitably raises concerns about mass surveillance, censorship, and the suppression of dissenting voices. Indeed, while we acknowledge that the development of data protection is a process and may take years, or even decades, to achieve effectiveness and that each country has its own cultural and institutional specificities, we need to stress that unchecked government access is likely to erode trust in data protection regimes.

However, we would like also to emphasise that it is not the goal of this initial chapter, nor of this volume, to analyse how personal data are or may be misused by BRICS governments, but rather to

[8] Data sovereignty can be defined 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." See Belli, Gaspar and Singh (2024), Belli L.; Gaspar, W. B., Singh, S. Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. Computer Law & Security Review, v. 54. (2024).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" and AI sovereignty as the "capacity of a given country to understand, develop, and regulate AI systems". These definitions are provided by Jiang, Min and Belli, Luca (Eds). Digital Sovereignty from the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge University Press. (2024); Belli, L. "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).

introduce the BRICS systems, so that the reader can understand their complexity. This effort is aimed at exploring what are the characteristics of the normative and institutional frameworks that are emerging in these increasingly influential countries and to what extent they can allow "legal interoperability"[9] as regards data governance.

Studying and striving to understand these leading emerging economies is therefore essential to comprehend why other Majority World countries are increasingly attracted by their models and leadership, despite the shortcomings of some group members in terms of the rule of law, democracy, and human rights. In this perspective, the recent BRICS expansion and its increasing willingness to enhance cooperation on digital matters deserves particular attention.[10] Since the publication of the first seminal paper on "Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence", which openly called for legal interoperability amongst BRICS data governance frameworks[11], the grouping has not only enlarged, including new members and partners, but also started to explicitly advocate "for the design of a fair and equitable **global framework for data governance**, including cross-border data flows, to address the principles of collection, storage, use and transfer of data; ensure the **interoperability of data policy frameworks** at

[9]The CyberBRICS research has illustrated the interest of legal interoperability in the field of data governance for BRICS countries since 2020, being positively received by most interlocutors in the grouping. Belli L. Data Protection in the BRICS Countries: Enhanced Cooperation and Convergence towards Legal Interoperability. Chinese Academy of Cyberspace Studies. (2020).

The term "legal interoperability" is the property 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. Technical 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. GSR discussion paper: Interoperability in the digital ecosystem. (ITU 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. 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' [2014] (4) Global Commission on Internet Governance Paper Series; Belli, L. and Zingales, N. (2023). "Interoperability to foster open digital ecosystems in the BRICS countries". in Chinese Academy of Cyberspace Studies, Xinhua Institute, China Institute of International 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.

[10] This point will be explored in the upcoming sections.

[11] See supra n (2).

all levels; and distribute the monetary and non-monetary benefits of data with developing countries"[12] [emphasis added].

It is therefore essential to analyse what types of data governance conceptions and context are the BRICS departing from, to understand what their vision of a "global framework for data governance" could be. One must not forget that BRICS are emerging economies with very different levels of maturity from typically "Western" countries as well as very strong cultural and legal specificities, which need to be considered, especially when trying to promote shared approaches to specific norms. These considerations are even more relevant when applied to the new BRICS members, i.e. Egypt, Ethiopia, Indonesia, Iran, Saudi Arabia and the United Arab Emirates, which bring additional layers of complexity to the group. While all except Iran have very recently approved general data protection laws[13], the human rights track records of the new BRICS countries can hardly be said to improve the average of the grouping, having been repeatedly criticised by numerous observers.[14]

Rule of law, democracy, and human rights are considered as key pillars of effective data protection, and in many countries, they represent essential criteria for the evaluation of adequacy decisions authorising international data transfers. The adoption of data protection framework by the BRICS countries is particularly interesting as it allow us to consider what is the impact of such regulatory innovation on democracy, human rights and rule of law, and vice versa, the extent to which these core elements can be seen as an essential precondition for the effectiveness of personal data regulations. The table below provides a brief overview of the BRICS countries' governance structures, and of the level of independence of each country's data protection authority. Furthermore, each country-specific chapter of this volume is opened by a section exploring the constitutional and human rights framework in each of the five original BRICS countries, to provide additional context to the reader.

[12] BRICS. Kazan Declaration "Strengthening Multilateralism For Just Global Development And Security". XVI BRICS Summit. Kazan, Russia. (23 October 2024). Paragraph 71. https://dirco.gov.za/xvi-brics-summit-kazan-declaration-strengthening-multilateralism-for-just-global-development-and-security-kazan-russian-federation-23-october-2024/

[13] On 13 July 2020, Egypt adopted its Law on the Protection of Personal Data, under Resolution No. 151 of 2020; Ethiopia enacted the Personal Data Protection Proclamation, Proclamation No. 1321/2024, on 24 July 2024; in the United Arab Emirates, the Federal Decree-Law No. 45 of 2021regarding the Protection of Personal Data became effective on 2 January 2022; Indonesia's Personal Data Protection Law (PDP Law) No. 27 was adopted in 2022; in Iran, the Ministry of Communications and Information Technology has announced the Draft Protection of Personal Data Law in 2018, but the text is still awaiting review from the Islamic Parliament of Iran; the Kingdom of Saudi Arabia's Personal Data Protection Law (PDPL) was issued 16 September 2021 and then amended 27 March 2023. The frameworks of the "new" BRICS will be briefly explored in the concluding chapter of this volume.

[14] See for instance Economist Intelligence Unit. Democracy Index 2023. Age of conflict. (2023). https://www.eiu.com/n/campaigns/democracy-index-2023/

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

Table 1.1 – Characteristics of personal data protection architectures in BRICS countries

Country	Political System	Data Protection Authority
Brazil	Federal Presidential Republic	**Formally independent.** The National Data Protection Authority (ANPD) is formally independent, but its budget is controlled by the Ministry of Justice.
Russia	Federal Semi-Presidential Republic	**Not independent**. Roskomnadzor depends from the Ministry of Communications and Mass Media of the Russian Federation.
India	Federal Parliamentary Democracy	**Formally independent.** The Data Protection Board of India has not been established yet. Interim oversight is provided by the Ministry of Electronics and Information Technology (MEITy) .
China	Unitary Marxist-Leninist One-Party State	**Not independent**. The Cyberspace Administration of China (CAC) enforces data law, amongst other digital regulations, and is not an independent body.
South Africa	Constitutional Parliamentary Republic	**Fully independent.** The Information Regulator was established as an independent body.
Egypt	Semi-Presidential Republic	**Not independent**. The Data Protection Authority depends from the Ministry of Communications.
Ethiopia	Federal Parliamentary Republic	**Not independent.** The Data Protection Authority depends from the Ministry of Innovation and Technology.
Iran	Theocratic Presidential Republic	**Not independent.** The Supreme Council of Cyberspace oversees all data-related laws, aligned with state interests.
UAE	Federal Absolute Monarchy	**Not independent.** The Data Protection Office depends from the Dubai International Financial Centre, and a UAE-wide authority is still lacking.
Indonesia	Unitary Presidential Republic	**Not independent.** The Personal Data Protection Authority has not been established yet. Interim oversight is provided by the Ministry of Communication and Information Technology.
Saudi Arabia	Absolute Monarchy	**Not independent.** The Saudi Data and Artificial Intelligence Authority (SDAIA) oversees AI/data, but is not an independent body.

Source: The authors.

While not exempted form criticism, established democracies such as Brazil, India, and South Africa demonstrate robust constitutional governance, characterised by judicial independence and adherence to separation of powers. However, only South Africa can be said to have a completely independent data protection authority amongst the BRICS member. In contrast, the introduction of data protection law in regimes commonly criticised for their rule of law and human rights track records, such as China, Russia, Egypt, and Ethiopia, alongside absolute monarchies such as Saudi Arabia and the UAE, and theocracies such as Iran, raises important questions in terms of implementation, particularly as regards capacity to exercise oversight independently form governmental interference. These considerations are particularly relevant as strong enforcement disparities persist, especially as regards implementation of the law on governmental entities, across BRICS members. These patterns underscore the tension between formal legal and institutional frameworks and political realities, particularly in contexts where personal data governance remains nascent or politically constrained.

However, when approaching this book, the reader is invited to try to understand – and respect – that the aim of this volume is not to assess how each BRICS country is faring in terms of rule of law, democracy, and human rights, but to provide the first concrete account of the existing BRICS data architectures, from BRICS perspectives, stressing how such architectures are shaping our conceptions of data governance. This account is particularly important to assess if and how the emergence and increasing rapprochement of BRICS digital policies can lead to a "post-western model of data governance"[15] that is able to shape the regulatory, institutional and technological frameworks governing international flows.

Such effort seems needed to explain why BRICS systems are exercising considerable appeal[16] amongst Majority World countries, particularly evident in the recent BRICS+ expansion[17]. BRICS systems continue to deploy international impacts, despite relevant Western efforts to contain, "de-risk"[18] from, and ostracise some BRICS members through heavy, yet rather ineffective, sanctions. This impact is manifest not only in the growing mutual influence amongst BRICS countries, but also in their capacity of shaping how third countries – which are either traditionally influenced by BRICS or have entered

15 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 18, no. 2 (2022): 1–58.
16 See Council of Councils. The BRICS Summit 2023: Seeking an Alternate World Order? Global Memo by ORF, SWP, SAIIA, SVOP, SIIS, RSIS, FGV, and CFR. (31 August 2023). https://www.cfr.org/councilofcouncils/global-memos/brics-summit-2023-seeking-alternate-world-order
17 See *supra* (6).
18 Schaus M. and Lannoo K. The EU's aim to de-risk itself from China is risky… yet necessary. CEPS. (7 September 2023). https://www.ceps.eu/the-eus-aim-to-de-risk-itself-from-china-is-risky-yet-necessary/ ; Blenkinsop P. EU agrees to de-risk from China and debates what this means. Reutersz (30 June 2023). https://www.reuters.com/world/eu-leaders-pledge-de-risk-china-debate-what-this-means-2023-06-30/

more recently the countries' sphere of influence – are adapting to normative and institutional innovations they introduced. Being large and complex developing countries with very recent data privacy cultures, the BRICS offer very relevant teachings for other low- and middle-income countries as they face challenges shared by the Global South.[19]

Conspicuously, one of the most widespread challenges is the very limited or simply inexistent "data protection culture"[20] which makes it extremely difficult to comply with newly "transplanted"[21] data protection frameworks. Indeed, in the Global Majority data subjects are frequently unaware of their data rights, public and private entities typically do not know how to correctly comply with data protection obligations, and regulators themselves may face enormous shortage of intellectual and financial resources necessary to implement the law and build a data protection culture through education. While taking inspiration from leading European models is completely understandable, developing countries face many challenges that the Western countries are not used to dealing with. In this sense, the analysis of leading emerging economies' experiences offers much more realistic illustrations of how data protection plays out in the Global South both in terms of the problems that need to be faced and the innovations that could help solve such problems[22].

Hence, this volume endeavours to analyse and compare some extremely relevant yet enormously understudied frameworks, acknowledging that BRICS countries act as very influential leaders both in their own regional environments and, to a lesser but increasingly relevant extent, globally, as tellingly illustrated by their recent expansion.[23] Such evolutions only stress the need for carefully studying their policy choices, including by understanding why their data – and constitutional – architectures are

19 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). <https://www.ijlt.in/journal/new-data-architectures-in-brazil%2C-china%2C-and-india%3A-from-copycats-to-innovators%2C-towards-a-post-western-model-of-data-governance>

20 Professor Stefano Rodotà, one of the most influential scholars and intellectuals in the data protection field, used to consider the "data protection culture" as the assimilation by society of the crucial importance of data protection. This process consists in the gradual understanding of the instrumental value that data protection plays for the realisation of citizenship and the sustainable development of society, economy, and democracy. See Belli L. and Doneda D. O que falta ao Brasil e à América Latina para uma proteção de dados efetiva? Jota (2 September 2021).

21 The import, or even copy, of influential foreign frameworks into another country's legislation is phenomenon typically defined "legal transplant". Alan Watson, Legal Transplants: An Approach to Comparative Law (1974). Data protection offers a telling example of such practice.

22 See *supra* n (11).

23 At the time of this writing, the BRICS grouping is "composed of eleven countries: its five original members – Brasil, China, India, Russia, and South Africa -, and six new members admitted in 2024-25 - Egypt, Ethiopia, Indonesia, Iran, Saudi Arabia, and the United Arab Emirates. The group was originally composed of Brasil, Russia, India, and China in 2006; South Africa adhered in 2011; the new expansion, effective as of 2024, derived from the Johannesburg Declaration, from August 2023. Partner Countries According to the mandate agreed upon through the Johannesburg Declaration, the leaders approved the creation of the BRICS partner country category during the Kazan Summit in 2024. The BRICS partner countries are: Belarus, Bolivia, Cuba, Kazakhstan, Malaysia, Nigeria, Thailand, Uganda, and Uzbekistan." BRICS. BRICS Brasil: About the BRICS. (20 January 2025). https://brics.br/en/about-the-brics

different from Western ones. In this perspective, we acknowledge that researchers and policymakers should analyse the BRICS systems with a grain of salt. Indeed, the BRICS frameworks are not exempted from criticisms, especially as regards the very light safeguards they might offer against abusive data processing practices perpetrated by public organs.

To start exploring this unusual coalition of emerging powers, the next section will briefly analyse how and why these very heterogeneous countries decided to establish their own process of club governance.

1.1.1. The BRICS: From Acronym to Alliance

Originally, the BRICS acronym was coined to merely describe some of the largest and fastest-growing economies, to identify leading emerging powers with some shared economic characteristics, with no intention to suggest any possibility of political or normative cooperation.[24] However, some years after the creation of the acronym by Goldman Sachs economist Jim O'Neill[25], the countries started to sense the enormous potential of the acronym, which represents an alternative "post-Western"[26] system of global governance, led by emerging economies. In this sense, the BRICS club has been created to foster a multipolar order where Global Majority leaders could play a relevant role in global governance and development, considering the increasing relevance of developing countries.

Initially, the BRICS countries started to increase their synergies on the margins of the G7/8 summits. In fact, the members of the G7/8 understood the mounting global relevance and influence of large emerging economies and began engaging with them through their so-called "outreach process".[27] Besides facilitating interactions among BRICS countries, their inclusion in the G7/8 outreach process proved to be a useful learning experience, letting these emerging powers understand the functioning of global club governance and the benefits brought by high-level summit processes.

In this spirit, the BRICs countries – with a small "s" as South Africa would join later – organised their first *ad hoc* informal meeting, in 2006, on the margins of that year's UN General Assembly. Two years later, the global financial crisis and the euro crisis considerably weakened the traditional Western

[24] See (n. 2).
[25] *Idem*.
[26] In this sense, see Stuenkel, O. Post-Western World: How Emerging Powers Are Remaking Global Order. Polity Press. (2016).
[27] The most relevant of such processes is the "G8 Outreach Five", which included Brazil, China, India, Mexico, and South Africa to the 2005 G8 summit (Russia was still part of the G8 before being expelled for annexing Crimea). However, while the outreach model recognized the relevance of emerging economies – notably the future BRICS members– it also perpetrated a shared sense of exclusion, as the countries kept on being merely invited as external guests, with marginal role, compared to the G members.

powers, creating a vacuum of global leadership and stressing the need for better coordination of Global Majority leaders. Indeed, as leading emerging economies, the BRICs had largely escaped the crises, and jointly agreed to establish their own stand-alone summitry process, driven by a newly found sense of self-confidence.

Russia organised the first BRICs heads of state meeting, in 2009, as an informal club-like summit with a notable international profile. Since then, no head of state has ever missed any of the summits[28], which have been held with a rotating presidency among the members with a similar format to other informal high-level processes, such as the G7/8 and G20. In 2011, the original BRICs club become a larger BRICS, with the full integration of South Africa, and, in 2014, the bloc established the BRICS-led New Development Bank (NBD),[29] and Contingent Reserve Arrangement, which can be seen as its most prominent institutional achievements.

Importantly the BRICS grouping has been discussing expansion for almost a decade and, since 2021, the New Development Bank has admitted Bangladesh, Egypt, the United Arab Emirates and Uruguay as new members.[30] Furthermore, at the 2023 BRICS Summit, the grouping leaders jointly agreed to enact the largest expansion of the alliance, inviting six new members — Argentina, Egypt, Ethiopia, Iran, Saudi Arabia, and the United Arab Emirates[31] — that were chosen amongst the twenty-three countries that have formally applied and the more than forty that expressed interest in joining the BRICS grouping.[32]

Since the club's inception, the number of governmental and multistakeholder gatherings, partnerships, and initiatives has been growing steadily, reaching more than 100 official initiatives per year.[33] However, it is important to emphasise that BRICS is neither an intergovernmental organisation with a constitution and a headquarter, nor a decision-making body with binding regulations, but rather a club

[28] The only exception has been Mr Putin's online participation to the XV BRICS Summit due to the pending International Criminal Court (ICC) arrest warrant, issued in connection to the Ukrainian war. See Nomsa Maseko and Kathryn Armstrong. Putin will not attend Brics summit - South African presidency. BBC News. (19 July 2023). https://www.bbc.com/news/world-africa-66247067 ; International Criminal Court. Situation in Ukraine: ICC judges issue arrest warrants against Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova. (17 March 2023). https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and

[29] See https://www.ndb.int

30 New Development Bank (NDB) (s.d.). NDB'S member countries. New Development Bank. https://www.ndb.int/about-us/organisation/members/

31 See *supra* n (16).https://brics2023.gov.za/wp-content/uploads/2023/08/Jhb-II-Declaration-24-August-2023-1.pdf

32 Tim Cocks. More than 40 nations interested in joining BRICS, South Africa says. Reuters.(July 20, 2023). https://www.reuters.com/world/more-than-40-nations-interested-joining-brics-south-africa-2023-07-20/

[33] For detailed overviews of the evolution of BRICS, see Stuenkel O. The BRICS and the Future of Global Order. Lexington Books. (2016); and o the same author, quoted supra at n. 4.

governance34 mechanism aimed at coordinating shared positions. The NBD is the only existing BRICS-led institution. In June 2022, under the Chinese rotating presidency the grouping decided the strengthen its own outreach process, the BRICS+ (read "BRICS plus") initiative, and numerous emerging economies, especially large producers of commodities, requested formally to join the grouping, being attracted by the BRICS potential for Majority World coordination, thus opening a new chapter for the club, while also contributing to strengthen its participatory legitimacy.

Crucially, despite their remarkable differences, the BRICS countries find some commonalities not only in some of their economic characteristics, but also in their shared grievances regarding imperialist attitudes and very recent colonialist past of Western countries, as well as the unfairness of Western-led global governance and institutions, such as the World Bank and the International Monetary Fund. Hence, to understand the BRICS, it is important to remember that while the existing global governance system is accepted by Global South countries, it has been established when most of the Global South countries were still colonies, which some European countries tried to retain with extremely violent repressions well into the 1960s and 1970s.35 Ignoring these essential aspects means having a very selective conception of history. Most Global Majority countries have been complaining about the injustice of the existing global intuitional system for decades, although with very meagre success, and endeavoured to counterbalance existing institutions and acquire further prominence via what came to be known as "South-South cooperation."[36]

In this context, the Non-Aligned Movement, and its Group of 15, the Group of 77, the IBSA Trilateral[37] and, finally, the BRICS and BRICS+ can all be seen as subsequent attempts of the Global South, driven

34 See Stuenkel, O. (2016) cit supra n (28); Brandi, C. (2019). Club governance and legitimacy: The perspective of old and rising powers on the G7 and the G20. South African Journal of International Affairs, 26(4), 685–702. https://doi.org/10.1080/10220461.2019.1697354

35 I. Surun, M. Pešta, and G. Metzler. Empire and Colonialism in Contemporary History (ca. 1900–2000) in Hansn J. et al. The European Experience. A Multi-Perspective History of Modern Europe, 1500–2000. OpenBook Publishers. (2023). https://doi.org/10.11647/OBP.0323 For a visual representation, see: The Map as History. Decolonization after 1945. (s.d.) https://www.the-map-as-history.com/Decolonization-after-1945

36 In 1990, the Report of the South Commission, chaired by former Indian prime minister Manmohan Singh, who was a key figure in the establishment of the BRICS, called for the establishment of a South-South cooperation, stressing that "the emerging development patterns of the North clearly suggest that the Northern locomotive economies will not pull the train of Southern economies at a pace that will satisfy its passengers-the people of the South. The locomotive power has to be generated to the maximum extent possible within the economies of the South themselves." See The South Commission. The Challenge to the South: The Report of the South Commission. Oxford University Press. (1990) p.286. https://www.southcentre.int/wp-content/uploads/2013/02/The-Challenge-to-the-South_HRes_EN.pdf

37 IBSA is a trilateral Forum which brings together India, Brazil, and South Africa to foster consultation and coordination on global and regional political issues; collaboration on concrete projects; and assisting other developing countries through the IBSA Fund. See http://www.ibsa-trilateral.org/ This organisation become well-known to Internet Governance scholars in 2011, when it put forward a proposal for a UN Committee for Internet-

by the "locomotives of the South"[38] to reclaim relevance.39 Such yearning for relevance aims at establishing an alternative to what they perceived as an arbitrary and frequently discriminatory system, led by former colonizers and frequently biased in favour of these latter countries.[40]

Recent BRICS developments provide substantial evidence both of the importance that digital technologies have acquired for the grouping and of the relevance these countries have gained regarding global digital policies.[41] In this perspective, the purpose of this introductory chapter is to note that, after having looked at European and Western models for reference, during several years, the BRICS are starting to become real innovators in terms of data policy, governance, and regulation[42] and are setting the basis for the development of a Global Majority-driven approach to global data governance.43 Furthermore, while keeping a low profile, and raising frequent yet not always justified criticism from observers, the BRICS are continuously coordinating, expanding their agenda, sharing information and best practices, mutually influencing each other's, and explicitly committing to enhance their cooperation on digital matters.

As we will discuss, all the BRICS have all adopted, renewed, or tabled data protection frameworks and consider data governance as one of their key priorities. Such trend should be welcomed, especially in countries frequently accused of democratic deficit, as some BRICS members frequently are, as even relatively partial advancements can have a considerable impact for the countries' enormous

Related Policies, which was strongly contested at that year's UN Internet Governance Forum and, despite the contestations, endorsed by the Indian Government at the 66th Session of the UN General Assembly in October 2011. See Belli L. Internet governance v. Internet government. MediaLAWS. (7 November 2011). https://www.medialaws.eu/internet-governance-v-internet-government/

[38] The report of the South Commission vocally stressed that Global South countries could not expect former colonisers and imperialist forces to be the driver of their development. Such locomotive force had to be found within the South itself. See *supra* n. 11. See also Belli, L. BRICS: The New Digital Locomotives. Beijing Review. (11 July 2022). <https://www.bjreview.com/Opinion/Voice/202207/t20220711_800300500.html>

39 Interestingly, the website of the South African chairmanship of the BRICS 2023 Summit provides an eloquent infographic that explicitly situates the grouping as the latest evolutionary step of a struggle for Global South relevance started with the First Asian-African Conference held in Bandung in 1955 and the subsequent creation of the Non-Aligned Movement in 1956 and the Group of 77 in 1964. See BRICS 2023. Evolution of BRICS. (2023). See https://brics2023.gov.za/evolution-of-brics/

[40] The Group of 15, which emerged within the Non-Aligned Movement, in 1989, the IBSA Trilateral, created in 2003, and eventually the BRICS, since 2009, have all been. A compelling review of how such events unfolded and why a South-South cooperation was born and evolved is provided by Prashad, V. Poorer Nations: A Possible History of the Global South. Verso: London-New York. (2012).

[41] See section 2.2. For an analysis of BRICS digital policies and most recent developments particularly in the field of cybersecurity, see Belli L. (Ed.), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Springer (2021); Belli, L. Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. The African Journal of Information and Communication, v. 28. (2021).

[42] On this point, see, notably 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). <https://www.ijlt.in/journal/new-data-architectures-in-brazil%2C-china%2C-and-india%3A-from-copycats-to-innovators%2C-towards-a-post-western-model-of-data-governance>

43 This point will be discussed in the next sections and in the concluding chapter of this volume.

populations. However, such trend should also be considered with a grain of salt. Indeed, it would be naïve to argue that the BRICS interest in data protection is motivated by a sudden intention to champion human rights standards, as economic, developmental, strategic, or even protectionist considerations play a key role in the countries' approach to data governance.

This latter point is key to understand why and how BRICS countries data-related policies innovate, as their rationales and motivations may differ from those of Western, and especially European, countries – and be harder to grasp for Western observers – but represent the rationale and motivations that lead most Global South countries. In such context, their adoption of data protection frameworks and the establishment of new institutional and normative arrangements offer a very interesting perspective on how and why emerging economies regulate personal data protection, and why BRICS are becoming innovators and even new world leaders in data-related policymaking.

It is important to understand that such blend of developmental and normative strategies produce incredible evolutions for large emerging economies. As an instance, in less than a decade, BRICS countries have become not only some of the most connected countries in the world[44] but also global leaders in data-intensive sectors such as instant online payments.[45] This latter example is particularly telling as, in the past five or six years, India and China have climbed the world ranking becoming the first and second country with highest number of real-time online payments in the world and, even more staggeringly, Brazil has reached the top ten, starting from the bottom, in only 4 years since the introduction of PIX, the Brazilian national digital payment system.[46] Conspicuously, these trends should be considered in parallel with the evolving discussions on data and digital sovereignty, which find in the BRICS grouping some of the most fascinating examples of heterogenous initiatives and expressions of the concept.[47]

---

44 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. (2024). https://cyberbrics.info/connectivity-across-brics-countries/

45 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

46 In 2024, the PIX systems processed more than 5.6 billion transactions per month. All PIX statistics are updated on a monthly basis on the website of the Brazilian Central Bank https://www.bcb.gov.br/en/financialstability/pixstatistics According to the ACI Worldwide and Global Data report mentioned at n.11, already in 2022 "Brazil's PIX system has gotten off to a flying start, passing a billion transactions within months of launching and continuing to go from strength to strength. There are now more than 100 million PIX users." See *ibid*, p. 8.

47 Digital sovereignty is an increasingly debated issue, which does not have a universal definition yet. For an analysis of the concept of Digital Sovereignty see J. Pohle and T. Thiel 'Digital sovereignty' (2020) 9(4). Internet Policy Review <https://doi.org/10.14763/2020.4.1532> accessed 23 July 2021.

It is also important to emphasise that, as demonstrated by the latest Russian developments, normative and institutional frameworks regarding data protection – as virtually any other type of framework – may be repurposed to fit the national security needs of governments at war. In this respect, the Russian experience is useful not only to study the country's data protection system, but also to predict which kind of developments one might expect from countries with poor human right records entering war.

Considering the complex scenario depicted above, this chapter aims at offering to the readers the elements necessary to grasp the evolutions of the BRICS, two decades since the first mention to this acronym.[48] This introductory chapter must be seen as instrumental to understand the increasingly relevant role played by the grouping members in the data governance field and the intensification of digital governance alignments between BRICS members.

1.1.2. Methodology and research structure

This book stems from the research performed by the CyberBRICS project[49], which is the first attempt to produce a comparative analysis of digital policies of the BRICS countries. In this chapter, we focus on the ongoing development and increasing rapprochement of BRICS Data Protection frameworks, stressing the existence of a tendency towards convergence,[50] highlighting that the grouping can be considered as an example of "enhanced cooperation"[51] for Internet governance, and stressing the innovative character of some of the policy and governance elements that BRICS are introducing in their frameworks.

In this chapter, first, we provide context to understand the BRICS and their efforts to cooperate on digital affairs, analysing official documents issued by the grouping, reviewing existing literature and

The various dimensions of the concept in the BRICS context are explored in a dedicated forthcoming publication. See Belli, L. and Jiang, M. (Eds.). (2024). Digital Sovereignty from the BRICS Countries. Cambridge University Press. For a digression on why emerging economies might be keen on building digital sovereignty narratives, see L. Belli 'BRICS Countries to Build Digital Sovereignty' in L. Belli (Ed) CyberBRICS: Cybersecurity Regulations in the BRICS Countries. (1st edn, Springer 2021); Belli L. (June 2023). Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil. G20's Think20 (T20). https://t20ind.org/research/building-good-digital-sovereignty-through-digital-public-infrastructures/

[48] See the 2001 paper by Jim O'Neil quoted *supra*.

[49] See <www.cyberbrics.info>.

[50] For an introduction to the policy convergence phenomenon, see Colin J. Bennett, 'What Is Policy Convergence and What Causes It?' (1991) 21 (2) British Journal of Political Science 215.

[51] In Internet governance parlance, this term finds its origin in the UN-sponsored World Summit on Information Society – commonly referred to as WSIS – and was consecrated in the outcome of the second phase of the World Summit on the Information Society, held in Tunis in 2005. While this concept has never been detailed, after having been consecrated by Tunis Agenda for the Information Society, world leaders have agreed on "the need for enhanced cooperation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet." See Tunis Agenda for the Information Society (adopted 18 November 2005) WSIS-05/TUNIS/DOC/6(Rev. 1)-E (Tunis Agenda) par 69 <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html> accessed 8 October 2021.

presenting relevant data on the countries' interactions. While setting the scene, we explore how an enhanced cooperation on the governance of Information and Communication Technologies (ICTs) has been unfolding in the BRICS agenda. Subsequently, we present the BRICS countries' Data Protection frameworks. Based on the empirical research developed by the CyberBRICS team,[52] we stress the existence of a tendency towards convergence of several aspects of the BRICS national data protection framework. In this perspective, we argue that the existence of a shared data protection skeleton and increased interest in cooperating on digital matters fosters legal interoperability. Then, we explore some concrete examples of how BRICS countries are innovating data protection, developing new institutions, strategies and as well as new generation of data protection tools that can inspire other countries.

These examples provide a teaser of the country-specific chapters of this volume, which will analyse in detail the data architectures of each BRICS member. Although each chapter is structured in a slightly different fashion, reflecting the specificities of each country's system, a "core structure" has been followed by all authors to facilitate comparison. Indeed, all authors have: i) introduced the legal system of each country with a particular focus on their human rights and rule of law track record, so that the reader can understand how the normative frameworks analysed are *de facto* applied; ii) described the normative networks in the context of which each country's data protection law must be considered; iii) analysed the national data protection framework; iv) and scrutinised the institutional mechanism dealing with the oversight and implementation of the normative framework. Furthermore, each country-specific chapter includes the English translation of the national data protection law as an annex.

Lastly, the concluding chapter of the book adopts a prospective stance, focusing on the possibilities of BRICS countries' cooperation regarding the personal data flows, trying to understand which types of mechanisms would be more suitable to foster sustainable transborder data exchanges, to foster digital trade and cooperation while guaranteeing that data subjects rights are respected, and cybersecurity is fully enforced.

[52] For a detailed comparison of the normative elements in the BRICS data protection frameworks, see 'BRICS Data Protection Map' (*CyberBRICS Project* 2021) <https://cyberbrics.info/data-protection-across-brics-countries/> accessed 8 October 2021

1.2. Background: Contextualising the Increasing Interest of the BRICS for Digital Cooperation

Some figures are key to realise the relevance of the BRICS in general and, particularly, the impact that their digital policies and data protection regulations inevitably deploy on a global scale. These countries together represent over 40% of the world population, being home to 3.2 billion individuals (*i.e.* 3.2 billion data subjects or data producers, depending on the perspective), and crystallise 26% of the world gross domestic product and a share of over 16% of world trade.[53] Hence, the digitalisation of the BRICS economies and societies represent a major opportunity for individuals and businesses in these countries, while also prompting considerable challenges.

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 protection becomes a key priority to foster thriving digital environments, where individual's rights are protected, businesses benefit from legal certainty, and "data colonialism"[54] from foreign tech giants is avoided or at least mitigated. At the same time, BRICS are well-aware of the risks that massive adoption and reliance of ICTs may generate and that sound policies are vital not only to regulate how individuals and businesses interact but, chiefly, to protect vital interests of the State.

In this sense, it is possible to argue that the disclosures by former National Security Agency (NSA) contractor Edward Snowden played a major role as a triggering event for the intensification of digital policymaking in the BRICS countries. Indeed, since 2013, the BRICS have elaborated and implemented an ample range of data-related strategies, laws, and regulations, aimed at strengthening cybersecurity55 and constructing – and experimenting with their own conceptions of – what is currently characterised as "digital sovereignty."[56]

It is worth to remember that the Snowden disclosures have been a particularly severe and acute wakeup call for BRICS, with the Brazilian President's personal phone being wiretapped[57], together with the communications of a wide number of members of the Brazilian government.[58] It is also useful to

[53] See the official website of the Indian 2021 Presidency of BRICS <https://brics2021.gov.in/about-brics>.
[54] The concept of "data colonialism" is eloquently discussed in Couldry, N. and Mejias, U.A. (2019). The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism. Stanford University Press.
55 See Belli L. (2021), supra n. (41).
[56] See supra n (25).
[57] -See Sonia Bridi and Glenn Greenwald 'Documentos revelam esquema de agência dos EUA para espionar Dilma' (*Fantástico*, 1 September 2013) <http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html> accessed 14 October 2021
[58] See 'EUA grampearam Dilma, ex-ministros e avião presidencial, revela WikiLeak' (*O Globo*, 4 July 2015) <http://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html> accessed 14 October 2021

emphasise that, since the revelations, Mr Snowden has been exiled in Russia. It is therefore not a coincidence that, since 2013, the protection of personal data and cybersecurity measures emerged as increasingly essential issues for BRICS countries to assert their (digital) sovereignty.

When the BRICs leaders met for the first time in 2009, before even becoming BRICS with a capital S, the terms "digital" or "cyber" were not even mentioned once in their first Joint Statement. These terms are featured 27 times in the XVI BRICS Summit Kazan Declaration, adopted on 23 October 2024. In the aftermath of the Snowden revelations, BRICS leaders included for the first time an explicit reference to the "paramount importance" of the adoption of "universally accepted norms, standards and practices [on] the security in the use of Information and Communication Technologies" [59] in their annual BRICS Summit declaration. Since the 2013 Summit, the BRICS ministers for science, technology and innovation have established continuous cooperation, meeting for the first time in 2014, intensifying their relations and defining partnerships.

Through an increasing number of shared documents on ICT cooperation[60], starting from the Memorandum of Understanding on Cooperation in Science, Technology, and Innovation,[61] the grouping structured the design of the legal frameworks within which intra-BRICS coordination, partnerships and synergies could be developed. As we will stress in the next section, this evolution culminated with the recent call for the establishment of "legal frameworks of cooperation among BRICS States [and] a BRICS intergovernmental agreement on cooperation" [62] on cybersecurity and the recent adoption of the United Nations Convention against Cybercrime, whose proposal was intensely lobbied for by Russia, China and India and brokered thanks to the essential role of Brazil and, to a minor extent, South Africa.

The process aimed at creating partnerships, promoting joint research projects and fostering policy synergies may be considered an example of what in Internet Governance vernacular is commonly referred to as "enhanced cooperation."[63] This context has spurred renewed efforts to build and

[59] See BRICS (Fifth BRICS Summit) 'eThekwini Declaration' (Durban 2013) para 34.
[60] For an analysis of such documents and their impact see Vladimir Kiselev and Elena Nechaeva, 'Priorities and Possible Risks of the BRICS Countries' Cooperation in Science, Technology and Innovation' [2018] 5(4) BRICS Law Journal <https://doi.org/10.21684/2412-2343-2018-5-4-33-60> accessed 8 October 2021.
[61] See BRICS (Second BRICS Science, Technology and Innovation Ministerial Meeting) 'BRICS Memorandum of Understanding on Cooperation in Science, Technology and Innovation' (Brasília, 18 March 2015) <https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/ii-reuniao-de-ministros-de-ciencia-tecnologia-e-inovacao-do-brics-documentos-aprovados-brasilia-18-de-marco-de-2015> accessed 8 October 2021
[62] 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
[63] The concept of "enhanced cooperation" is introduced by paragraph 69 and 71 of the Tunis Agenda for the Information Society. See (n. 5). Importantly, the United Nations Economic and Social Council has acknowledged that "the Tunis Agenda underlines the need for enhanced cooperation to enable Governments to carry out their

modernise digital policies in general and data governance frameworks in particular. Conspicuously, while elaborating their frameworks, the BRICS have enjoyed the advantage of having the most modern data protection standards – chiefly, the European General Data Protection Regulation (GDPR) – as a source of inspiration, while adapting the norms to their domestic legal traditions and political systems.

Importantly, the enhancement of BRICS digital policy cooperation and the movement towards personal data protection are producing particularly interesting outcomes. Being "late-movers" BRICS countries have learned from first movers' successes and failures, thus not only "transplanting"[64] foreign best practices into their domestic frameworks, but also innovating data protection practices.65 Furthermore, by taking inspiration from the same sources, BRICS frameworks are triggering policy convergence and enabling "legal interoperability", due to the increasing compatibility of the BRICS normative frameworks regulating the protection of personal data. As we will point out in the next section as well as in the conclusion of this volume, this latter point has now officially entered the BRICS agenda, having been explicitly included as part of the BRICS commitments since the 2024 Summit.

1.2.1. Enhanced Cooperation on ICT Governance

As an outcome of the 6th BRICS Sumit, held in the Brazilian city of Fortaleza in 2014, the BRICS leaders for the first time agreed on enhancing "cooperation on combating cybercrimes and we also recommit to the negotiation of a universal legally binding instrument in that field [considering] that the UN has a central role in this matter."66 Such commitment was expanded at the 7th BRICS Summit, held in the Russian city of Ufa in 2015, when the BRICS Declaration asserted the "inadmissibility of using ICTs and the Internet to violate human rights and fundamental freedoms, including the right to privacy, and reaffirm that the same rights that people have offline must also be protected online."[67] At the same time the Ufa Declaration stressed that "a system ensuring confidentiality and protection of users' personal data should be considered" and BRICS leaders reiterated their "condemnation of mass

roles and responsibilities in international public policy issues pertaining to the Internet [but does] not specify how the process of enhanced cooperation should be designed, the means by which enhanced cooperation could be achieved or how the desired results should manifest themselves in practice." See United Nations (General Assembly, Economic and Social Council) 'Enhanced cooperation on public policy issues pertaining to the Internet, Report of the Secretary-General' (4 May 2011) A/66/77–E/2011/103.

64 The concept of "legal transplantation" is well-known in comparative law studies and refers to "the moving of a rule or system of law from one country to another". See Watson A. Legal Transplants: An Approach to Comparative Law. (1974) p. 21.

65 See Belli L. supra n. (17).

66 BRICS. Sixth BRICS Summit – Fortaleza Declaration. Paragraph 34. (16 July 2014). https://brics2023.gov.za/wp-content/uploads/2023/07/140715-leaders-Fortaleza-Declaration.pdf

67 See BRICS (VII BRICS Summit) 'Ufa Declaration' (9 July 2015) <https://www.brics2021.gov.in/BRICSDocuments/2015/Ufa-Declaration-2015.pdf> accessed 8 October 2021

electronic surveillance and data collection of individuals all over the world, as well as violation of the sovereignty of States and of human rights, in particular, the right to privacy."

While the reader might be forgiven for thinking that such commitment might sound peculiar, coming from some countries that have a less than stellar track-record in terms of privacy protection, the consideration of the abovementioned elements is key to understand the rationale behind the successive policy developments at both international and domestic BRICS level in the subsequent years. To operationalise their stated intentions and enhance their cooperation and coordination, BRICS leaders established a BRICS Working Group on ICT Cooperation so that "members could actively lead and cooperate to strategize synergies, [...] sharing of information and case studies on ICT policies and programs in creating an enabling environment."[68]

It is important to realise that the goal of the working group is to foster both exchange of policy strategies adopted at domestic level and facilitate the development of shared positions at the international level, primarily at the UN level, which is considered by all BRICS at the only legitimate forum having a central role to play as regards the establishment of global regulatory frameworks. The subsequent Goa Declaration, resulting from the 8th Summit, started to adopt a more assertive posture regarding BRICS-led policymaking efforts, stressing the potential for cooperation amongst the BRICS countries that could "work together for the adoption of the rules, norms and principles of responsible behaviour of States including through the process of the United Nations Group of Governmental Experts (UNGGE)"[69].

By explicitly mentioning the joint elaboration of rules, norms and principles, BRICS leaders crossed the Rubicon, willingly showing a clear intention to enhance cooperation in international digital policymaking. The subsequent years witnessed the establishment of several initiatives aimed at making cooperation on technological and digital matters more tangible, such as the BRICS Digital Partnership,[70] and the BRICS Science & Technology Enterprise Partnership (BRICS-STEP), subsequently renamed STIEP, the BRICS Partnership on New Industrial Revolution (PartNIR), the Innovation BRICS Network (iBRICS Network), and the BRICS Institute of Future Networks.[71]

[68] See *ibid*.
[69] See *ibid*.
[70] See BRICS Working Group on ICT Cooperation, 'ICT Development Agenda and Action Plan' (Bengaluru, 11 November 2016).
[71] See *ibid*.

1.2.2. A New Phase for BRICS Digital Cooperation

The abovementioned policy and operational initiatives emphasise "the importance of continuing BRICS scientific, technical, innovation and entrepreneurship cooperation,"[72] as well as the understanding that the development of technology and innovation is a key vector to convey the values that are traditionally backed into policies and regulations. Such posture culminated in the elaboration of an Enabling Framework for the Innovation BRICS Network (iBRICS Network), "a mechanism for direct dialogue among actors of innovation of the BRICS countries, which will promote mutual support, joint projects and the exchange of best practices with a view to advancing BRICS systems of innovation".[73]

Besides the Enabling Framework, the 2019 BRICS Summit, organised under the Brazilian Presidency, led to the adoption of two relevant innovations, corroborating the thesis of an ongoing enhanced cooperation: the new BRICS Science, Technology and Innovation Work Plan 2019-2022[74] and the establishment of a new BRICS Science, Technology and Innovation (STI) Architecture.[75] Notably, the BRICS STI Architecture aims at defining an "agile cooperation governance structure" to improve the coordination and management of BRICS STI activities and prioritise them; measure and evaluating STI initiatives, to minimise their development risks and optimise their impact; and ensure dissemination of BRICS STI activities amongst different stakeholders.[76]

The BRICS-led initiatives and, particularly, the recent BRICS STI Architecture highlight the potential but also the remaining challenges to be faced to achieve concrete results through cooperation. This is clearly not an easy task, due to the very elastic configuration of BRICS and the lack of a coordinating body: there is no stable "BRICS Secretariat" as the Presidency is rotating, thus increasing the difficulty of monitoring the effective execution of all existing initiatives. However, history demonstrates that, despite their different perspectives, their diversity of approaches has always been acknowledged as a

[72] See 'BRICS Informal leaders' meeting on the margins of the G20 Summit – Joint Media Statement – Osaka, 28 June 2019' *Ministério das Relações Exteriores* (28 June 2019) <https://www.gov.br/mre/en/contact-us/press-area/press-releases/brics-informal-leaders-meeting-on-the-margins-of-the-g20-summit-joint-media-statement-osaka-28-june-2019>. Accessed 8 October 2021

[73] See BRICS, 'Enabling framework for the innovation BRICS network 'iBRICS Network'' (2019) <http://brics2019.itamaraty.gov.br/images/documentos/Enabling_Framework_iBRICS_Network__Final.pdf>. Accessed 8 October 2021

[74] See BRICS, 'BRICS Science, Technology and Innovation Work Plan 2019-2022' (October 2019) <http://brics2019.itamaraty.gov.br/images/documentos/BRICS_STI_Work_Plan_2019-2022__Final.pdf> accessed 8 October 2021.

[75] See BRICS, 'A New BRICS STI Architecture' (September 2019) <http://brics2019.itamaraty.gov.br/images/documentos/The_New_BRICS_STI_Architecture__Steering_Committee__Final_19_9_19.pdf> accessed 8 October 2021

[76] ibid

point of richness rather than weakness, and considerable results, such as the establishment of the NDB, can be achieved.

In this spirit, the 12th BRICS Summit culminated with the adoption of a new Strategy for BRICS Economic Partnership 2025, featuring Digital Economy as one of the three key pillars of the strategy around which BRICS "define[d] a development path of BRICS and set the framework for cooperation of its members."[77] Indeed, as stressed by the Strategy, the "development and adoption of digital technologies becomes a determinant of sustainable economic growth of the grouping"[78] and, for this reason, BRICS countries "acknowledge the importance of digital governance in the era of global digitalization and cooperate with each other in the area of digital governance" and have committed to take steps to "exchange experiences and explore approaches to regulatory issues of digital transformation of economy."[79]

The BRICS' Leaders 2021 Declaration represented a further milestone, as the countries have started recognising explicitly the interest of enhanced cooperation in these issues. Indeed, the 2021 Declaration contains explicit commitment of BRICS Heads of State to the "respect of the right to privacy of individuals" and the promotion of cybersecurity, "**advance[ing] practical intra-BRICS cooperation in this domain**, including through the implementation of the BRICS Roadmap of Practical Cooperation on ensuring Security in the Use of ICTs and the activities of the BRICS Working Group on Security in the use of ICTs, and underscore[ing] also the importance of **establishing legal frameworks of cooperation among BRICS States on this matter** and acknowledge[ing] the work towards consideration and elaboration of proposals, including on **a BRICS intergovernmental agreement on cooperation** on ensuring security in the use of ICTs and on **bilateral agreements among BRICS countries**" [80] [emphasis added].

Hence BRICS' enhanced cooperation has been developing on three different fronts: i) through the research and scientific initiatives highlighted above; ii) through the establishment of a joint institution aimed at providing funding for development projects, the NDB; iii) and through the policy coordination that, as we anticipated above, may find its most structured example in the process that led to the

[77] See BRICS 'Strategy for BRICS Economic Partnership 2025' (November 2020) <https://eng.brics-russia2020.ru/images/114/81/1148155.pdf> accessed 8 October 2021
[78] See *ibid*. 8.
[79] See *ibid*. 8-9.
[80] 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

adoption of the new UN Convention against Cybercrime.[81] Indeed, for almost a decade, BRICS members have coordinated their cybersecurity approaches, identifying as common denominator the need to craft a universal regulatory framework on cybercrime under the aegis of the United Nations, and building their international policy approaches upon such shared understanding.

It is important to note that, in August 2024 this vision came to fruition, with the adoption of the new UN Convention against Cybercrime, an effort that RIC countries, chiefly Russia, have been trying to promote at least since the early 2010s.[82] Until recently, the mere idea that the proposal of cybercrime treaty led by Russia and China and backed by BRICS countries and their Global South partners could be adopted by the UN was an option considered as less than serious by most observers. However, despite the criticisms that can legitimately be raised about the Convention[83] – whose scope is so broad that it could facilitate surveillance and repression – its adoption represents a concrete instance of the impact that BRICS coordination and joint action may have regarding international digital policymaking.

In this respect, the BRICS should be seen as a laboratory for policy coordination of Global South leaders. The push towards cooperation and convergence is increasingly involving governance, policymaking, and regulatory areas, besides research, development, and trade partnerships. The following session posits that the recent BRICS data protection developments provide useful material to observe how the elaboration of domestic frameworks, together with their shared international aspirations, are offering an opportunity to align BRICS data policies, despite the non-existence of any binding commitment to do so. This objective has been clearly emphasised by the most recent Kazan Declaration, where BRICS+ heads of state openly advocate for a "global framework for data governance, including cross-border data flows, to address the principles of collection, storage, use and transfer of data [to] ensure the interoperability of data policy frameworks"[84].

Such objective builds upon an already established willingness to strengthen cooperation on e-commerce issues, as clearly expressed by the India-chaired 2021 Summit, that adopted the BRICS Framework for Ensuring Consumer Protection in e-Commerce. This document recognised that "[a]dequate safeguards and measures are needed to ensure privacy and security of the consumers [and resolved] to enhance cooperation through the BRICS E-commerce Working Group" while also

[81] United Nations General Assembly. Draft United Nations convention against cybercrime. A/AC.291/L.15. (7 August 2024). https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf
[82] Ballard, M. (2010, April 20). UN rejects international cybercrime treaty. *Computer Weekly*. https://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty
[83] Hassan T. Upcoming Cybercrime Treaty Will Be Nothing But Trouble. Human Rights Watch. (7 August 2024). https://www.hrw.org/news/2024/08/07/upcoming-cybercrime-treaty-will-be-nothing-trouble
[84] See supra n (12).

emphasising "the role of the digital economy as an important tool for modernization and transformation of the industry, promotion of inclusive economic growth, support of seamless global trade and business conduct, thus helping BRICS economies meet their Sustainable Development Goals."[85]

As this volume illustrates, many data protection policy elements are already remarkably similar in the BRICS countries and, given this already existing compatibility, the enhancement of their legal interoperability, perhaps through the adoption of a "BRICS Data Protection Framework" or a "BRICS Data Security Framework" may respond to the call for "a legal frameworks of cooperation" highlighted above, and should be considered as a strategic priority for the BRICS. Moreover, as we will suggest in the following sections, in their effort to regulate data protection, BRICS are putting forward some innovative elements that should be utilised as "experiences" to be exchanged, as suggested by the Strategy for BRICS Economic Partnership 2025. Other non-BRICS countries would also benefit from studying such innovative "experiences" as they provide useful approaches to tackle challenges that are faced by virtually all countries.

1.3. Data Protection in the BRICS

To understand why BRICS digital policies and, particularly, their data protection frameworks are particularly relevant, we need to consider not only that these countries encompass roughly 40% of the world population, but that more than 40% of global Internet users are also from the BRICS.[86] Personal data refer to and are generated by individuals. Hence, a population of 3.2 billion individuals, out of which more than half is connected to digital technologies, makes the BRICS grouping the largest producer of what is currently deemed the world's most valuable resource and a "new asset class."[87] Data governance becomes therefore essential for the functioning of economy and society but also for the assertion of (digital) sovereignty.[88]

Importantly, the large number of connected individuals contributes not only to the creation of enormous consumer bases and consequent data pools. It also expands remarkably the number of potential developers that can shape the evolution of technology well beyond the BRICS countries.

[85] BRICS. Framework for Ensuring Consumer Protection in e-Commerce. (2021). https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-44.pdf
[86] 'Internet Users by Country' (*Internet Live Stats*, 2016) <https://www.internetlivestats.com/internet-users-by-country/> accessed 8 October 2021
[87] World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (2011)
[88] See supra n (25).

The abovementioned considerations and the mounting economic and geopolitical relevance of personal data have triggered intense data-related policy-making efforts in all BRICS countries. The Snowden revelations elevated "security in the use of Information and Communication Technologies (ICTs)" to the level of "paramount importance,"[89] while the 9th BRICS Summit Xiamen Declaration enshrined the countries commitment to jointly "advocate the establishment of internationally applicable rules for security of ICT infrastructure, data protection and the Internet."[90] In this context, alignment in data related policies has been growing.

This section explores some of the results of the comparative research developed by the CyberBRICS project, regarding the Data Protection dimension. While the BRICS frameworks deserve in-depth analysis, this section highlights some of the most striking commonalities, highlighting the existence of a certain degree of compatibility.[91] All BRICS countries undertook major regulatory developments regarding data protection, in recent years, elaborating new legislation, updating existing one or establishing new regulatory agencies.

The most recent developments include:

- In August 2018, the adoption of a new Brazilian General Data Protection Law (Law 13.709/2018)[92] that entered in force in September 2020, the establishment of a new National Data Protection Authority (ANPD),[93] in late 2020, and a new National Council on Privacy and Data Protection. In February 2022, the new fundamental right to data protection was enacted in the Brazilian Constitution,[94] and the transformation of the ANPD into a formally independent agency between 2022 and 2023.[95]
- In late 2020, Russia amended its general data protection law (Federal Law No. 152-FZ on Personal Data), after having reinforced its data localization obligations in 2019, with the adoption of the so-called "Sovereign Internet Law". The localisation of major Internet

[89] See BRICS (n 18) para 34.
[90] See BRICS (IX BRICS Summit) 'Xiamen Declaration' (4 September 2017) <http://www.mea.gov.in/uploads/publicationdocs/28912_xiamendeclaratoin.pdf>. Accessed 8 October 2021
[91] See CyberBRICS Project (n 10)
[92] See 'Brazilian General Data Protection Law – Unofficial English version' (*CyberBRICS Project* 2020) <https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/>. Accessed 8 October 2021
[93] The official website of the new Brazilian Data Protection Agency is available at <https://www.gov.br/anpd/pt-br>.
[94] In May 2020, Brazilian Supreme Court recognized a fundamental right to data protection in the 1988 Brazilian Constitution, derived but not coincident with the right to privacy and the "habeas data" writ.
[95] See the "Non-official Translation of Executive Order n. 1124/2022, which transforms the Brazilian Data Protection Authority into an independent administrative agency." (*CyberBRICS Project* 2022) https://cyberbrics.info/non-official-translation-of-executive-order-n-1124-2022/

companies in the Russian territory was introduced in July 2021 and, since September 2022, new data security requirements entered in force, together with the State system for detection, prevention and elimination of consequences of computer attacks (GosSOPKA).

- In August 2017, the Supreme Court of India recognised privacy as a new fundamental right, thus opening the path to the elaboration of a new Data Protection Bill, which was introduced in the Parliament in December 2019 and considerably reshaped by a Joint Parliamentary Committee in December 2021. India is also experimenting electronic consent frameworks within its Data Empowerment and Protection Architecture (DEPA), in the context of the so-called "India Stack" aimed at propelling the new vision of Digital India. The final version of the Bill was adopted in August 2023 as the Digital Personal Data Protection Act 2023.
- In August 2021, China adopted its new Personal Information Protection Law (PIPL), after having adopted a new Data Security Law, in June 2021, and having also introduced new rights to privacy and to the protection of personal information in its new Civil Code, in January 2021. China also adopted stringent measures on Security Assessment on Outbound Data Transfers in September 2022, and later announced it would make it more flexible in September 2023.
- In 2017, South Africa established its new Data Protection Authority, the Information Regulator to oversee implementation of the 2013 Protection of Personal Information Act (POPIA), which entered into force fully in July 2021. In 2022, the Information Regulator established its Enforcement Committee, an essential organ to fully implementing and being able to enforce POPIA.

In a very condensed timeframe, BRICS countries have revolutionised their domestic data protection frameworks, introducing major developments in their legal systems. Interestingly, despite the absence of any formal agreement mandating the harmonisation of their national frameworks, several regulatory elements are emerging in an extraordinarily similar fashion. The main reason for such convergence is likely the common inspiration from existing frameworks, particularly the European General Data Protection Regulation (GDPR), the Council of Europe Convention 108, and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

While the BRICS domestic framework on data protection present a shared skeleton highlighting several similarities, it is also important to stress that there are considerable differences. Some of these similarities include: (i) the definition of personal data in itself, which all BRICS consider as the information related to an identified or identifiable natural person; (ii) the core principles and individual rights upon which the data protection architecture is erected; (iii) the set of obligations for data controllers and processors; (iv) recognition of the essential role of international data transfers for the

(digital) economy[96]; (v) the extraterritorial reach of data protection laws; (vi) the application of these norms to government activities, although with multiple exceptions and varying levels of intensity; and (vii) the creation of data protection authorities to support the application of these laws.

Conversely, some divergences include (i) the different stances toward data localisation; (ii) the suite of available legal tools for international data transfers; and (iii) particularities of some BRICS data protection laws, such as South Africa's "personal data" rights extending beyond natural persons to include legal persons as well. These, in sum, are indicators of BRICS States' convergence and divergence around a shared "data protection skeleton", which showcase points of potential tension and legal interoperability. These points will be analysed in more detail in the following chapters and the conclusion of this volume.

1.4. Towards legal interoperability on data protection in the BRICS?

As the following chapters will illustrate, a shared Data Protection skeleton is emerging in the BRICS, but the national frameworks include also remarkably different and unique elements that should be studied carefully. The raising relevance of data protection in the BRICS is due partly to the global policy trends, such as the "Brussels effect" triggered by the adoption of GDPR, but also the numerous data-related scandals, and the increasing awareness that personal data laws are essential to foster well-functioning and cybersecure digital economies, while strengthening digital sovereignty.[97]

In this context, the BRICS willingness to protect personal data and enhance their cooperation regarding digital policy stems from the consideration that compatible regulations may be enormously beneficial to foster digital trade and online businesses, while achieving their shared cybersecurity goals. Hence, the establishment of compatible BRICS solutions for data governance may be seen as an experiment aimed at scaling up such solutions "for the design of a fair and equitable **global framework for data governance**, including cross-border data flows", as proclaimed by the 2024 BRICS Declaration.

The governments of the BRICS nations clearly understand that each of their citizens is a producer of personal data that, combined, have not only immense economic relevance, but also unmatchable strategic value.[98] Moreover, the demand for data protection is becoming increasingly popular amongst the billions of people in the BRICS, as many individuals are beginning to understand the potential value

[96] See Belli, Gaspar, Singh. (2024) n. 8.
[97] Idem. See also Belli L. 'From BRICS to CyberBRICS: new cybersecurity cooperation' (*China Today*, 13 November 2021) <http://www.chinatoday.com.cn/ctenglish/2018/tpxw/201911/t20191113_800184922.html> accessed 14 October 2024.
[98] See supra n (82).

of their data, the risks that personal data processing may entail, and the subjective dimensions of data sovereignty.[99]

In this context, modern and compatible frameworks are instrumental to protect individual rights and provide legal certainty for businesses, while also being a key pillar of international digital trade. As this introductory chapter has argued, BRICS countries have already developed a remarkably compatible normative basis. This aspect of BRICS data protection regulations will be expanded upon in the following chapters, dedicating particular attention to potential vectors of legal interoperability in the concluding chapter of this volume. However, the following chapters of this volume will also illustrate how many differences exist and that it is indeed in the interest of the grouping to work toward the enhancement of digital cooperation in general and legal interoperability in data-related policy in particular. However, it is also important to keep in mind that the drive towards legal interoperability can be influenced by several factors, including global geopolitical and regulatory trends, the concrete economic incentives and strategic interests that can foster – or hinder – cooperation and harmonisation efforts, and the public support or averseness towards such efforts. Legal interoperability in data protection brings multiple benefits, spanning from the reduction of barriers to cross-border data flows, thus increasing economic growth and partnership opportunities in research, development and innovation, while also strengthening cybersecurity through the adoption of shared information security standards.

In this perspective, as we will argue in the concluding chapter of this volume, the promotion of legal interoperability in data governance is likely to strengthen data sovereignty through a collaborative effort. Indeed, the definition of shared regulatory arrangements for data governance and data transfers, can enhance transparency, accountability, security and control over personal data, thus extending the reach of data subjects' rights while increasing legal certainty for data controllers as well as for regulators.

As we stressed in the previous sections, over the past decade, the BRICS countries have been constructing the bases of their legal interoperability through multiple BRICS Declarations and high-level documents. The latest evolutions expressed in the BRICS 2024 Declaration suggest that the path towards legal interoperability in data governance is a firm choice, driven by global trends, economic incentives, and shared strategic interests. While their unique national idiosyncrasies present challenges, the benefits of promoting shared solution to data governance are clear. Importantly, we should not underestimate that by working together to enhance digital cooperation and achieve legal

[99] Anja Kovacs and Nayantara Ranganathan, 'Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India' [2019] Data Governance Network Working Paper 03 <https://cyberbrics.info/data-sovereignty-of-whom-limits-and-suitability-of-sovereignty-frameworks-for-data-in-india/> accessed 14 October 2021

interoperability in data-related policy, the BRICS can act as a policy laboratory for Global South-driven solutions defining the bases of a more inclusive digital economy.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)