PREPRINT version of 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

DATA PROTECTION IN THE BRICS COUNTRIES: LEGAL INTEROPERABILITY THROUGH INNOVATIVE PRACTICES AND CONVERGENCE

Luca Belli[*] *and Danilo Doneda*[†]

Summary:

- This paper stems from the research elaborated by the CyberBRICS project, which is the first attempt to analyse the digital policies in the BRICS countries (Brazil, Russia, India, China, and South Africa).

- The paper focuses on the ongoing developments and increasing rapprochements of BRICS data protection frameworks and on the emergence of innovative elements in such frameworks.

- 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.

- This article contextualises the BRICS and their efforts to cooperate on digital affairs, stresses a tendency towards convergence and "legal interoperability" of several aspects of their national data protection policies, and explores some examples of how BRICS countries are innovating data protection, emphasising that such innovations could inspire other countries.

- Lastly, it argues that BRICS should seize the opportunity to further enhance their cooperation on data protection, as the increased convergence and compatibility of their data protection frameworks may be beneficial for both individuals and businesses, while implementing the recent BRICS commitment to enhance intra-BRICS cooperation on digital policies.

Keywords: Brazil; BRICS; China; India; Russia; South Africa.

[*] Professor at Fundação Getulio Vargas (FGV) Law School, Coordinator of the Center for Technology and Society at FGV, Director of CyberBRICS.
[†] Professor and Director, Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP).

1. Introduction[3]

The BRICS countries – namely, Brazil, Russia, India, China, and South Africa – are an unusual grouping[4] 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, the human rights track record of some of the group members is far from stellar. Several rankings categorise some of them as "partly free", "not free" or even "authoritarian regimes,"[5] and Russia has recently announced it would no longer participate in the Council of Europe and cease to be a party to the European Convention on Human Rights, after the members of the human rights body voted to suspend the Russian Federation's rights of representation.[6]

While the authors of this paper are well-aware of the abundant critiques regarding the human rights track records of some BRICS countries, the goal of this article is not to analyse how personal data are or may be misused by BRICS governments, but rather to explore what are the normative and institutional innovations that are emerging in these countries. Indeed, such innovations are already exercising international impact, not only exercising mutual influence amongst BRICS countries, but also shaping how third countries – either traditionally or more recently influenced by BRICS – are adapting to normative and institutional innovations introduced by the grouping members.

---

[3] The authors would like to sincerely thank a group of extremely talented researchers from the CyberBRICS project for their valuable support and feedback during the elaboration of this paper. Special thanks go to Walter Britto Gaspar, Eduardo Brasil de Mattos, Smriti Parsheera, Wei Wang, Sofia Chang, and Larissa Chen.

[4] 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.

[5] 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

[6] See Resolution CM/Res(2022)3 on legal and financial consequences of the cessation of membership of the Russian Federation in the Council of Europe. Adopted by the Committee of Ministers on 23 March 2022 at the 1429bis meeting of the Ministers' Deputies.

BRICS countries act as very influential leaders both in their own regional environments and, to a lesser but increasingly relevant extent, globally, thus stressing the need for carefully studying their policy choices. To understand the relevance of this coalition of emerging powers and why the policy choices of the BRICS are likely to have a considerable impact, particularly on the Global South, we must briefly analyse how and why these very heterogeneous countries decided to establish their own process of club governance.

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.[7] However, some years after the creation of the acronym by Goldman Sachs economist Jim O'Neill[8], the countries started to scent the enormous potential represented by an alternative "post-Western"[9] system of global governance. In this sense, the BRICS club has been created to foster a multipolar order where global governance and development can be led by the Global South, increasing relevance and benefits of developing countries.

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 of large emerging economies and began engaging with them through their so-called "outreach process".[10] 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 weakened and disorientated the traditional Western powers. At this point, the leading emerging economies, who had largely escaped the aforementioned crises, jointly agreed to establish their own stand-alone summitry process, driven by a newly found sense of self-confidence.

[7] See (n. 2).

[8] *Idem.*

[9] In this sense, see Stuenkel, O. Post-Western World: How Emerging Powers Are Remaking Global Order. Polity Press. (2016).

[10] 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 G group itself). However, while the outreach model recognised 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 guest with marginal role, compared to the G members

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, 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),[11] and Contingent Reserve Arrangement, which can be seen as its most prominent institutional achievements.

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.[12] However, BRICS is not an intergovernmental organisation with a constitution and a headquarter, and 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 Argentina and Iran, two large producers of commodities, requested formally to join the grouping, thus opening a new chapter for the club.

Importantly, 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, such countries have been complaining about the injustice of such 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."[13]

In this context, the Non-Aligned Movement and its Group of 15, the Group of 77, the IBSA Trilateral[14] and, finally, the BRICS grouping can all be seen as subsequent attempts of the Global

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

[12] 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.

[13] 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

[14] 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

South, driven by the "locomotives of the South"[15] to reclaim relevance and establish an alternative to what they perceived as an arbitrary and frequently discriminatory system led by former colonizers.[16]

Recent developments in the BRICS grouping, however, 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.[17] In this context it is interesting 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. Furthermore, while keeping a low profile, and raising frequent yet not always justified criticism from observers, the BRICS are continuously 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, the BRICS have all adopted, renewed, or tabled data protection frameworks. Such trend should be welcomed, especially in countries frequently accused of democratic deficit, as some BRICS members frequently are. However, such trend should also be considered with a grain of salt, as the BRICS interest in data protection is clearly not only motivated by an intention to improve human rights standards, but rather by economic, developmental, strategic, or even protectionist considerations.

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 countries – and be harder to grasp for Western observers – but represent the rational and motivations that lead most

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-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/

[15] 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.

[16] 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).

[17] 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).

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 but also global leaders in data-intensive sectors such as instant online payments.[18] 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 2 years since the introduction of PIX, the Brazilian national digital payment system.[19]

Considering the above, this paper reflects on the complexity and evolutions of the BRICS, two decades since the first mention to this acronym[20], focusing on the increasingly relevant role played by the grouping members in the personal data governance field and on the intensification of digital governance alignments between BRICS members.

1.1. Methodology and research structure

This paper stems from the research performed by the CyberBRICS project[21], which is the first attempt to produce a comparative analysis of digital policies of the BRICS countries. We focus on the ongoing development and increasing rapprochement of BRICS Data Protection frameworks, stressing the existence of a tendency towards convergence,[22] highlighting that the grouping can be considered as an example of "enhanced cooperation"[23] for Internet governance,

[18] 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

[19] According to the ACI Worldwide and Global Data report mentioned at n.11, "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.

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

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

[22] 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.

[23] 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

and stressing the innovative character of some of the policy and governance elements that BRICS are introducing in their frameworks.

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 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 focus on the BRICS countries' Data Protection frameworks. Based on the empirical research developed by the CyberBRICS team,[24] we stress the existence of a tendency towards convergence of several aspects of the BRICS national data protection framework. We argue that the existence of a shared data protection skeleton and increased interest in cooperating on digital matters fosters "legal interoperability."[25]

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.

[24] 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

[25] 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. In this perspective, legal interoperability is the property of fostering compatibility of rules concerning the same topic within different jurisdictions or different administrative levels within a state. Like technical interoperability, legal interoperability stimulates the exchange of information within different systems. As such, interoperability of both technical and legal systems allows individuals - and, particularly, Internet users - to access and provide services in a cross-border fashion and to enjoy equal right-protection within different systems thanks to compatible (or common) rules, principles, and procedures. Shared rules and principles amongst various juridical systems have the potential to reduce transaction costs, deflating barriers to cross-border trade, and foster non-measurable benefits, such as the protection of fundamental rights. See Weber, R. 'Legal Interoperability as a Tool for Combatting Fragmentation' [2014] (4) Global Commission on Internet Governance Paper Series; Belli, L. and Zingales, N. Interoperability to foster open digital ecosystems in the BRICS. World Internet Conference Report. Chinese Academy of Cyberspace Studies. (2022).

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. Lastly, we argue that BRICS should seize the opportunity to further enhance their cooperation on data protection, as the increased convergence and compatibility of their data protection frameworks may be beneficial for both individuals and businesses in the grouping.

To do so, this paper suggests that the BRICS Roadmap of Practical Cooperation on Ensuring Security in the Use of ICTs[26] could offer a suitable framework for cooperation and implementation of the recent BRICS commitment to enhance intra-BRICS cooperation on digital policies, and to test the new BRICS Science, Technology, and Innovation (STI) Architecture, which aims at enabling and evaluating BRICS initiatives in the STI field.

2. Background: Contextualising BRICS and their Interest 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.[27] 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"[28] 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

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

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

[28] 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.

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 constructing – and experimenting with their own conceptions of – what is currently characterised as "digital sovereignty."[29]

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[30], together with the communications of a wide number of members of the Brazilian government.[31] It is also useful to 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 23 times in the XIV BRICS Summit Beijing Declaration, adopted on 23 June 2022. In the aftermath of the Snowden revelations, BRICS leaders included for the first time an explicit reference to the "paramount importance" played by the "security in the use of Information and Communication Technologies (ICTs),"[32] in the annual BRICS Summit declaration. Since the 2013 Summit, the BRICS ministers for science, technology and innovation

[29] 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. 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. *Cit. supra*. For an analysis of how digital structures enable the exercise of sovereignty, see Belli, L. Structural power as a critical element of digital platforms' private sovereignty. In Celeste, E., Heldt, A. and Iglesias Keller C. (Eds.), Constitutionalising social media (pp.81-100). Oxford, UK: Hart Publishing. (2022).

[30] 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

[31] 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

[32] See BRICS (Fifth BRICS Summit) 'eThekwini Declaration' (Durban 2013) para 34.

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[33], starting from the Memorandum of Understanding on Cooperation in Science, Technology, and Innovation,[34] the grouping structured the design of the legal frameworks within which intra-BRICS 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." [35] 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."[36]

This context has spurred renewed efforts to build and modernise data protection frameworks. 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

[33] 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.

[34] 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

[35] 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

[36] 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 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.

"transplanting"[37] foreign best practices into their domestic frameworks, but also innovating data protection practices. 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.

2.1. Enhanced Cooperation on ICT Governance

As an outcome of the 7th BRICS Summit, held in the Russian city of Ufa in 2015, BRICS heads of State 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." 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 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." [38]

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 development, which interested all BRICS countries in the subsequent years. To operationalise their stated intentions and enhance their cooperation, 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."[39]

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

[37] 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.

[38] 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

[39] See *ibid.*

principles of responsible behaviour of States including through the process of the United Nations Group of Governmental Experts (UNGGE)"[40].

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,[41] 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.[42]

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,"[43] 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".[44]

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-

[40] See *ibid.*

[41] See BRICS Working Group on ICT Cooperation, 'ICT Development Agenda and Action Plan' (Bengaluru, 11 November 2016).

[42] See *ibid.*

[43] 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

[44] 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

2022[45] and the establishment of a new BRICS Science, Technology and Innovation (STI) Architecture.[46] 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.[47]

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 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."[48] Indeed, as stressed by the Strategy, the "development and adoption of digital technologies becomes a determinant of sustainable economic growth of the grouping"[49] 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."[50]

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

[45] 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.

[46] 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

[47] ibid

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

[49] See *ibid*. 8.

[50] See *ibid*. 8-9.

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**."[51] [emphasis added]

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.

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.

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

[51] 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

BRICS.[52] 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."[53] Data governance becomes therefore essential for the functioning of economy and society but also for the assertion of (digital) sovereignty.[54]

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. 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,"[55] 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."[56] 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.[57] 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 evolutions include:

- In August 2018, the adoption of a new Brazilian General Data Protection Law (Law 13.709/2018)[58] that entered in force in September 2020, the establishment of a new

[52] 'Internet Users by Country' (*Internet Live Stats*, 2016) <https://www.internetlivestats.com/internet-users-by-country/> accessed 8 October 2021

[53] World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (2011)

[54]

[55] See BRICS (n 18) para 34

[56] See BRICS (IX BRICS Summit) 'Xiamen Declaration' (4 September 2017) <http://www.mea.gov.in/uploads/publicationdocs/28912_xiamendeclaratoin.pdf>. Accessed 8 October 2021

[57] See CyberBRICS Project (n 10)

[58] 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

National Data Protection Authority (ANPD),[59] 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,[60] and in June 2022 the Brazilian government launched a processed aimed at transforming ANPD into an independent agency.[61]

- 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".
- 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. A final and consolidated version of the Bill should be presented at the Parliament budget session in early 2023.
- In August 2021, China adopted its new Personal Information Protection Law (PILP), 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.
- In 2017, South Africa established its new Information Commissioner to oversee implementation of the 2013 Protection of Personal Information Act (POPIA), which entered into force fully in July 2021, after a one-year "grace period."

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

[59] The official website of the new Brazilian Data Protection Agency is available at <https://www.gov.br/anpd/pt-br>.

[60] 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.

[61] 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/

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, as we argue in the newt section, it is also important to stress that there are considerable differences. Particularly, it is possible to find stronger similarities between the Brazilian, Russian, and South African frameworks and the European one, as compared to the Indian and Chinese ones, which clearly aim at establishing a more original (and particular) approach, while preserving legal interoperability. The BRS part of BRICS seems to have taken stronger inspiration from Europe, likely because these countries have started their data protection efforts in the late 2000s and early 2010s when Europe was an undisputed regulatory powerhouse, with particular regard to data protection. Legal and cultural traditions may also play a substantial role, as in these three countries, whose legal systems have developed from the European continental legal system and, therefore, have a stronger predisposition to be influenced by European legal instruments and legal culture.

China and India, on the contrary have decided to pursue their own regulatory models, which are both the most recent and the most original in the realm of data protection laws. Some of the intrinsic characteristics of these two countries must also be considered as a relevant reason explaining their willingness to develop an original model, besides the particular tradition and characteristics of their legal systems. For instance, the fact their size exempts these countries from being guided out from external pressures and demands on their choices on data protection, allows them to craft their regulations more independently, based on their internal demands and legal cultures and adopting their own pace, rather than regulating to keep pace with Europe. Social and political circumstances are also to be considered, such as the greater flexibility with which state actors can move and the greater coordination they enjoy, including regarding the implementation of data protection legislation.

3.1. A shared data protection skeleton

Based on the findings of the CyberBRICS project, we can identify a non-exhaustive but telling list of policy elements around which BRICS data protection frameworks are converging.[62] Due to the relatively recent development of the BRICS data protection framework, decision makers in these countries have enjoyed the privilege of constructing their legal frameworks based on

[62] See Belli, L. Data Protection in the BRICS Countries: Enhanced Cooperation and Convergence towards Legal Interoperability. In New Media Journal. Chinese Academy of Cyberspace Studies. (2021).

existing best practices and, as we will highlight, also to find creative solutions for problems that other legislators have not been able to tackle properly.

A patent example of convergence is the definition of personal data in itself, which all BRICS consider as the information related to an identified or identifiable natural person, although, interestingly, the South African framework extends even more the protection encompassing also data related to legal persons, as we will discuss in the next section.[63] A similar approach also underpins the definitions of sensitive data, data subject and data controller, although the terminology utilised may slightly vary.[64]

The core principles upon which the data protection architecture is erected are also commonly shared. The principles included in BRICS frameworks may be found in virtually all data protection regulations and allow identifying a globally applicable principle-core that is usually common beyond BRICS, at least as regards the first four principles. The BRICS data protection principles[65] include consent, purpose limitation, fair and lawful processing, necessity, data minimisation, and accountability. Furthermore, BRICS legislators have included a similar spectrum of rights although with different flavours.[66] All BRICS frameworks embrace provisions establishing the individual rights to access to data, correction of incomplete, inaccurate, or outdated data, elimination of personal data processed with the consent of the data subject, and revocation of consent.

BRICS data protection frameworks also present a very comparable set of obligations for data controllers and processors.[67] Interestingly, the data controller concept has different contours in the five frameworks. The South African framework uses the term "responsible party" rather than "controller". The new Chinese Personal Information Law refers to a "personal information handler", meaning "organizations and individuals that, in personal information handling activities, autonomously decide handling purposes and handling methods" (art. 73.1). This would be roughly synonymous with the Brazilian and Russian (or EU) data controller, while the PIPL's "entrusted party" (art. 21) would reflect the data processor acting according to the controller's instructions.[68]

[63] See CyberBRICS Project 'BRICS Data Protection Map' (*CyberBRICS Project* 2021) Policy Question 7 <https://cyberbrics.info/data-protection-across-brics-countries/> accessed 8 October 2021
[64] See *ibid*, "Definitions"
[65] ibid, Policy Question 9
[66] ibid, Policy Question 13
[67] ibid, Policy Question 14
[68] See (n 51)

Meanwhile, the Indian Bill uses the concept of "data fiduciary", which the Justice Srikrishna Committee claims to be a conscious decision to depart from the narrative of a "controller" and "subject."[69] The core obligations for data controllers in the BRICS include abiding to data protection principles, obtaining free and informed consent in order to process data, duly communicating information on the data processing, and ensuring the security of all personal data under their responsibility.

The normative elements enshrined in the Indian Bill demonstrate concrete potential to adopt innovative approaches that can inspire both BRICS countries and other countries globally. Perhaps, the most relevant example is the trend to move the Bill itself from an approach focused purely on personal data to one aimed at data governance in general, including non-personal data. This is very clear in the deliberations made by a joint parliamentary committee on the Bill which even changed the name by which the Bill is known from "Personal Data Protection" to "Data Protection Bill"[70]. Indeed, regulation of non-personal data has been subject of a growing and global debates, reflected in BRICS countries in several s ways, from their implementation of open data frameworks to what begins to be considered concretely in India, which is the proposition of data frameworks, consolidating personal and non-personal data at once.

Importantly, all BRICS countries have considered the essential role of international data transfers for the (digital) economy. All BRICS allow for international data transfers, whenever foreign third parties are deemed as providing an acceptable level of protection, but some of them have explicit data localization provisions (Russia and China) or are likely to implement them (India). Hence, we can note both convergence and divergence regarding key international issues such as data localisation and transfer restrictions. The Brazilian and South African frameworks include no requirement to store any types of personal data within national jurisdictions. Russia was the first Country to enshrine data localisation obligation in its national framework, since 2015.

The same applies to China where, the PIPL prescribes that all personal data must be stored within the country, unless the Cyberspace Administration of China (CAC) determines differently. In

[69] See Rishab Bailey and Trishee Goyal, 'Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2019' (*The Leap Blog*, 13th January 2020) <https://blog.theleapjournal.org/2020/01/fiduciary-relationships-as-means-to.html> accessed 8 October 2021

[70] See Pallavi Bedi, Shweta Mohandas. "The Centre for Internet and Society"s Comments and Recommendations on the Data Protection Bill", 2022. Available at: https://cis-india.org/internet-governance/general-comments-data-protection-bill.pdf

India, the draft Personal Data Protection Bill 2021 required every data fiduciary to ensure that at least one serving copy of personal data to which the Act applies is stored on a service or in a data centre located in the country. The Central Government may notify certain categories of personal data as exempt from this requirement on the grounds of necessity or strategic interests of the State, but sensitive personal data cannot be exempted.

In case of international data transfers, the evaluation of a sufficient level of protection is performed through quite heterogeneous mechanisms, spanning from the adoption of adequacy decisions on foreign legal frameworks, as foreseen in the GDPR, or specific administrative authorisations to transfer data for national service providers, or yet the use of corporate rules or binding agreements admitted by national authorities.[71] Given the large number of criteria and the variety of mechanisms that BRICS countries adopt to regulate international data transfers, below we provide a visual representation allowing the reader to easily understand similarities and differences between the legal regimes.

Table 1 citation: The following table provides a comparative analysis of the international data transfer requirements established by the BRICS domestic frameworks. The purpose of Table 1 is to provide a comprehensive panorama of all the various conditions that BRICS countries include in their frameworks to facilitate or restrict data transfers, as well as to allow the reader understanding what conditions are shared by all or some BRICS countries and which ones are unique to some of them.

Legend: Table 1 - International Data Transfer Requirements in the BRICS Countries

International data Sharing requirements	Brazil	Russia	India	China	South Africa
Adequacy decision / adequate protection in destination country's law	Adequate protection at destination country, recognized by the data protection authority	Adequate protection at destination country, recognized by the data protection authority	Non-critical data: Adequate protection at destination country, recognized by the Central Government following consultation with the data protection authority (with consent, explicit in the case of sensitive data, by the data subject)	There is a general obligation to adopt "necessary measures" to ensure an adequate standard of protection in comparison to PIPL.	Adequate protection at destination country provided by law

[71] See (n 49) Policy Question 22

With consent from the data subject	When the data subject provides previous, informed, and specific consent	With written consent of the data subject	When explicit consent is given by the data principal for such transfer.	When the data subject specific consents to the transfer	When the data subject consents to the transfer
When related to international agreements	When transfer results in an international cooperation agreement	When stipulated by international treaties of the Russian Federation		To carry out provisions of treaties or international agreements that the People's Republic of China has concluded or acceded to	
Contract clauses (standard clauses or negotiated clauses).	Specific contract clauses. Standard contractual clauses.		Non-critical data: Standard contractual clauses or intra-group schemes that have been approved by the Data Protection Authority (with consent, explicit in the case of sensitive data, by the data subject)	Concluding a contract with the foreign receiving side in accordance with a standard contract formulated by the State cyberspace and informatization department	Adequate protection at destination country provided by binding agreement
For the execution of a contract or its preliminary acts.	When necessary to execute a contract or preliminary acts to a contract to which the data subject is party, at their request	For the execution of a contract to which the data subject is party			When necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request
Global corporate norms	Global corporate norms				Adequate protection at destination country provided by binding corporate rules

Certificates and codes of conduct	Certificates, codes of conduct and similar tools			Undergoing personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department	
Protection of life and health	To protect the life or physical integrity of the data subject or a third party	For the protection of life, health, other vital interests of the subject of personal data or other persons when it is impossible to obtain written consent			
Authorization by the data protection authority	Authorization by data protection authority		Non-critical data: The Authority approves a particular transfer or set of transfers as permissible due to a situation of necessity		
	When necessary to comply with international law instruments related to international cooperation among intelligence, investigation and prosecution agencies	No restriction when destination country is Party to the Council of Europe Convention on the Protection of Individuals in the automated processing of personal data	Sensitive data classified as critical: to a particular person or entity engaged in the provision of health services or emergency services where such transfer is strictly necessary for prompt action	Passing a security assessment organized by the State cybersecurity and informatization department	When the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party

	When necessary to implement a public policy	When provided for by federal laws	Sensitive data classified as critical: to a particular country, a prescribed sector within a country or to a particular international organisation that has been prescribed, where the Central Government is satisfied that such transfer or class of transfers is necessary for any class of data fiduciaries or data subjects and does not hamper the effective enforcement of the Act		When the transfer is for the benefit of the data subject, and: (i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and (ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.
	To comply with a legal or regulatory obligation	When necessary to protect the foundations of the constitutional system of the Russian Federation, to ensure the defence of the country and the security of the state, as well as to ensure the safety of a sustainable and safe operation of the transport complex, to protect the interests of the individual, society and the state in the sphere of the transport complex from acts of unlawful interventions			
	To exercise rights in a judicial, administrative or arbitration procedure				

Importantly, all data protection frameworks in BRICS countries have an extraterritorial reach, with the exception of South African law, which only applies when either the responsible party is domiciled in the country or is using means in South Africa, but does not extend to foreign entities providing services, goods, or collecting data about South African nationals from abroad. Perhaps surprisingly, all BRICS data protection laws apply also to the government. However, the Indian Data Protection Bill 2021, as the 2019 version, includes a highly criticised Clause 35 attributing sweeping powers to the federal government to exempt any governmental agency from the scope of the law.

As for situations where social and cultural traits have a broader importance, major differences between BRICS data protection frameworks may be observed. Such is the case, for example, of the measures protecting children's data. Brazil has chosen a system akin to the European one, considering as children any person under twelve years old. The most recent version of India's Bill differs, considering all persons under 18 years old as unable to express consent legally. In this particular matter, the Cyberspace Administration of China (CAC) released in 2019, prior to China's data protection law a data privacy regulation related to children, the "Provisions on Cyber Protection of Personal Information of Children", which is sometimes compared to COPPA (the US Children Online Privacy Protection Act), requiring paternal consent for children under 14.

Finally, all BRICS countries seem to envisage a benefit in having a specific authority overseeing the implementation of the law, although the way they design their national authorities differs considerably and may be seen as a reflex of their legal and institutional frameworks. In 2020, Brazil has established a new Data Protection Authority (DPA), the National Data Protection Authority (ANPD), complemented by a very innovative multistakeholder body acting as a Privacy and Data Protection Council (CNPD). Only very recently, has the ANPD become an independent body, after the promulgation of a decree[72] by the Federal Government that, at the time of this writing, needs to be confirmed by Brazilian Parliament. When ANPD was originally created, it was established as an agency directly dependent from the Brazilian government and located inside the so-called "direct public administration", within the Brazilian Presidency.

In Russia, data protection is overseen by the Federal Service for Supervision of Communications, Information Technologies and Mass Communications (Roskomnadzor), while in China the responsible body is the Cyberspace Administration of China (CAC), which are not independent bodies, but are incorporated as parts of the respective federal governments. Both organs have extremely large remit, encompassing several attributions that, in other countries, are typically attributed to different regulators, such as data protection, content regulation, or

[72] See (n) 58.

telecommunications regulators. Importantly, their lack of independence has been criticised and identified by scholars and observers alike, as the one of the core reasons why the Russian and Chinese frameworks cannot be deemed as providing protections that are substantially equivalent to data protection systems where the regulators' independence is guaranteed.

The Indian Personal Data Protection Bill 2021 provided for the establishment of an independent Data Protection Authority, although neither the Bill not the Authority have been approved so far. Lastly, South Africa was the only BRICS country to have a genuinely independent Information Regulator, subject only to the Constitution and to the law and accountable to the National Assembly. As mentioned above, this may change when the Brazilian Congress will confirm the Presidential Decree transforming the ANPD into and independent body and when India will establish its new Data Protection Authority.

3.2. Innovative BRICS Data Protection Practices

While BRICS countries are taking relevant inspiration from existing frameworks to develop their own national data protection regimes, it is essential to acknowledge that they are also introducing considerable innovations. In this section we offer a selection of the most innovative features of the BRICS data protection frameworks. While these elements have only been introduced recently, they should be considered carefully as they offer some interesting and innovative approaches that are likely to be replicated by other countries in the future.

3.2.1. Brazil and the LGPD implementation: the National Council of Data Protection and Privacy and the influence of the consumer protection framework

The Brazilian data protection framework, even if only very recently enacted and still lacking several steps to be fully implemented, clearly presents some very particular characteristics. Importantly, such features mainly stem from typical experiences and practices present in other fields of the country's legal system.

The framing and drafting of the LGPD took at least 8 years since its first official draft was released[73] till its enactment. In fact, this first official draft is the development from unofficial drafts produced during the series of debates in a Mercosur (the economic area bounding together Argentina, Brazil, Paraguay and Uruguay) working group on electronic commerce which, since

[73] A record of the original draft submitted to public consultation as well as the contributions received are available at <http://www.doneda.net/2020/03/08/consultas-publicas-protecao-de-dados/>.

2004, evaluated a proposal made by Argentina of a data protection model law for the economic area.[74] As Brazil did not have such a law nor a bill, some drafts began to circulate within federal government's boundaries at that time[75], which developed into a draft bill submitted to public consultation in 2010 by the Brazilian Ministry of Justice[76].

This first draft resembled, in its structure and fundamental concepts, the data protection framework in Convention 108 of the Council of Europe and Directive 95/46/CE of the European Union. At the same time, it presented some typical traits of the Brazilian law system, such as the explicit reference to Brazilian consumer law pillars and to the Public Civil Action law. The final text of the LGPD, even if based on this initial draft, changed enormously, due to the relevant number of contributions received in the public consultations organised by the Brazilian Ministry of Justice, and the intense legislative process, from 2016 to 2018, which included a series of public hearings, consultations and calls for suggestions and meetings with stakeholders.

The result of such participatory process was the engagement of several actors in this discussion but also the introduction of Brazilian legal system views and instruments into the texts as a way of absorbing the views of the various stakeholders. Moreover, as we will highlight, the participatory multistakeholder process, which led to the elaboration of the Law, has been baked into the governance system designed by the law. The final text of what later became LGPD is the result of an intense debate among diverse sectors of Brazilian society which not merely legitimised data protection tools and concepts transplanted from foreign legislations, but rather shaped them in a way they could best fit Brazilian legal tradition, introducing regulatory and participatory structures which became key characteristics of the Brazilian data protection framework in comparison with international standards.

These remarks on the LGPD's formative process are brought into consideration to give context on some specific characteristics of LGPD which we identified as innovative practices. This context is also different than the one found in other non-European countries, which typically debated their own data protection bills for a shorter time and, typically, considered the need to

[74] Mercosur, 'XII Reunión ordinaria del subgrupo de trabajo nº13 – Comércio Electrónico' (15 June 2004) <https://documentos.mercosur.int/simfiles/docreuniones/23116_SGT13_2004_ACTA02_ES.pdf> accessed 8 October 2021

[75] For a description of the development of Brazilian General Data Protection Law since its first drafts, see Danilo Doneda, 'Panorama histórico da proteção de dados pessoais' in Laura Schertel Mendes, Danilo Doneda, Ingo Sarlet and Otávio Rodrigues Jr., *Tratado de Proteção de Dados Pessoais* (Forense 2020) 3-20. The original draft law is available at <http://culturadigital.br/dadospessoais/>.

[76] This consultation is still available at <http://pensando.mj.gov.br/dadospessoais2011/> (April 2021)

include into their legal system those rules that could facilitate international data transfers, thus fostering digital trade with Europe.

In Brazil, the pressure to shape domestic legislation to better accommodate international data flows has never been one of the major guiding forces for the elaboration of a data protection framework. In fact, one of the few elements of external pressure was the commitment of the federal government to join the OECD as a member country[77], which would require the integration of several OECD Recommendations in the Brazilian legal system, including the establishment of a data protection framework. Nevertheless, this urge was important to motivate some of the federal government bodies, which were traditionally silent if not sceptical about LGPD, to endorse the proposal.

Such multistakeholder endorsement from the Brazilian private sector, academia and civil society, together with the consensus reached in the National Congress, played a relevant role to facilitate the LGPD's approval and enactment. Considering this particular background, it is not surprising that the resulting law would reflect (i) the presence of a multistakeholder consultative council as an auxiliary body to the Brazilian Data Protection Authority, and (ii) strong connection to the Brazilian consumer protection framework, noticeable in both procedural and substantial material aspects of the LGPD.

LGPD created as its Data Protection Authority the National Data Protection Authority (ANPD or "*Autoridade Nacional de Proteção de Dados*"), together with a consultative multistakeholder body, the National Data Protection and Privacy Council ("*Conselho Nacional de Proteção de Dados e Privacidade*"). The Council has strictly consultative functions and does not take decisions, nor has any supervision or administrative tasks. Its competences are listed in article 58-B of LGPD and include providing ANPD with suggestions, proposals and support for its actions and, particularly, for the development of the National Data Protection Policy; drafting annual reports on the actions performed by ANPD; drafting studies and promoting debates and public hearings and, generally, promoting data protection knowledge and culture among Brazilian people.

[77] OECD's Guidelines on the protection of privacy and transborder dataflows of personal data was a pivotal document on the development of international data protection standards when it came out in 1980 and maintains its importance. Compliance with these guidelines is one of the requirements if Brazil is eventually to join OECD as a member country. See 'Personal Data Protection at the OECD' (*OECD*, 2021) <https://www.oecd.org/general/data-protection.htm> accessed 8 October 2021

The Council presents a multistakeholder composition: out of its 23 members, 5 are appointed by the Federal Government, 1 by the Federal Senate, 1 by the House of Representatives, 1 by the National Justice Council, 1 by the Public Ministry National Council, 1 by the Brazilian Internet Steering Committee, 3 chosen amongst representatives of non-governmental organizations, 3 from science and technology institutions, 3 from national confederations from the productive sector, 2 from the private sector and 2 from unions and worker organizations. The process utilized to nominate each counsellor depends on the stakeholder group they represent: the institutions explicitly mentioned in LGPD define themselves who is their respective counsellor. The stakeholder groups mentioned generically will have the possibility to suggest candidates and the board of directors of ANPD will choose the most adequate representatives of each group, and subsequently submit those names to the Presidency of Republic, which will have a final say on the list and nominate the counsellors.

The presence of a sound multistakeholder element in the Council pays tribute to, at least, two driving factors. First, the noticeable multistakeholder experience of the Brazilian Internet governance ecosystem, where CGI.br – the Brazilian Internet Steering Committee ("*Comitê Gestor da Internet*") – has played a pivotal role in the development of the Internet in the country since its early days, frequently characterised as a "multistakeholder model" that became a global benchmark.

The second factor was the concrete dialogue between several sectors by the time LGPD was yet a Bill and was being debated in National Congress. The resonance among diverse stakeholders gave birth even to a coalition of institutions, enterprises, and organizations from several areas to support the approval and enactment of LGPD, and one of the side products of these discussions was indeed the need to create a governance structure in the Brazilian data protection framework to accommodate and give a voice to these stakeholders in the process of implementation of data protection.

3.2.2. Freely Shareable Personal Data, Opt-out, and Data Localisation in Russia

In Russia, personal data protection is regulated by Federal Law No. 152-FZ, which was adopted in 2006 and subsequently amended in December 2017 and in December 2020.[78] As emphasised

[78] See Russian Federal Law No. 519-FZ of 30 December 2020 'On Amendments to the Federal Law 'On Personal Data'' <http://publication.pravo.gov.ru/Document/View/0001202012300044> accessed 8 October 2021

above, the Russian data protection framework is implemented by Roskomnadzor, a super regulator with particularly large competence and powers, which has been frequently criticised for its lack of independence. The latest amendments to the Russian framework entered in force partly in March 2021 and partly in July 2021. As discussed by Zanfir-Fortuna and Iminova[79], these amendments aim at tackling four areas.

First, the amended provisions introduce a new category of personal data that can be freely shared and are defined as "personal data allowed by the data subject to be disseminated." Second, the Russian legislation now includes rules allowing personal data to become freely sharable with an unlimited number of persons. To do so, the law establishes the obligation to collect specific, affirmative, and separately collected consent from the data subject. The rationale behind the creation of this new category of personal data reminds the one behind GDPR Article 9(2)(e), a largely underappreciated norm[80], which allows to process sensitive data when "processing relates to personal data which are manifestly made public by the data subject."

According to the amended Russian data protection framework, personal data allowed by the data subject to be disseminated can only be processed when an organisation or individual processing them can prove that the data subject expressed consent according to the modalities specified by the law. Third, the law introduces the possibility for Roskomnadzor – the Russian of Communications, Information Technologies, and Mass Communications Regulator – to create a centralised database of all the expressions of consent regarding the unlimited dissemination of personal data. Lastly, the law establishes a new absolute right to opt out of the dissemination of personal data, which can be exercised "at any time."

Conspicuously, consent is the only legal basis for the processing and dissemination of "freely" shareable personal data. Such data is defined by a new paragraph 1.1, in Article 3 of the Law, as "personal data to which an unlimited number of persons have access to, and which is provided by the data subject by giving specific consent for the dissemination of such data, in accordance with

[79] Gabriela Zanfir-Fortuna and Regina Iminova, 'Russia: New Law Requires Express Consent For Making Personal Data Available To The Public And For Any Subsequent Dissemination' (*CyberBRICS Project*, 2 March 2021) <https://cyberbrics.info/russia-new-law-requires-express-consent-for-making-personal-data-available-to-the-public-and-for-any-subsequent-dissemination/> accessed 8 October 2021

[80] For a rare analysis of this norm, see Edward S. Dove and Jiahong Chen, 'What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e)' [2021] 11(2) International Data Privacy Law <https://academic.oup.com/idpl/article/11/2/107/6146670> accessed 8 October 2021

the conditions in the Personal Data Law." According to the new Art 10.1, personal data can be freely shared only after the obtention of specific, express, unambiguous, and separate consent. Under Law 152-FZ, the natural or legal person that determines the purposes of personal data processing, the composition of personal data to be processed, and the operations performed with personal data is defined as the "data operator."[81] Article 10.1(1) creates a new obligation for the operator to obtain the data subjects' separate, specific and express consent to be able to disseminate personal data, on top of the regular consent to process data.

Silence or inaction cannot configure the consent needed for free dissemination of data and the data subject must also enjoy the possibility to choose specific categories of personal data that can be freely disseminated. Furthermore, any operator, be it the first one collecting the freely shareable data or anyone else processing freely shareable personal data bears the onus to "provide evidence of the legality of subsequent dissemination or other processing", under Article 10.1(2).

The establishment of the aforementioned obligation has also led the Russian legislator to introduce the possibility for Roskomnadzor to create a centralised consent management system to collect all the expressions of consent. Indeed, according to Article 10.1(6), consent to turn personal data into freely shareable data can be collected by the operator or via a dedicated "information system" to be created by Roskomnadzor.[82] This proposed system may resemble the Data Empowerment and Protection Architecture proposed by the Indian government and discussed in the next section.

Another innovative practice introduced by the recent amendments of the Russian law is the new absolute right to opt-out of dissemination of freely shareable personal data. Indeed, Article 12.1(12) prescribes that the free dissemination of personal data can be halted at any time, on request from an individual. Such right to opt out from dissemination can be exercised to withdraw the previously expressed consent, by specifically identifying the personal data to which the request refers, and the diffusion of which should be terminated. Interestingly, the opt-out request can also be used as a tool to stop the dissemination of data about which consent has not been

[81] This term refers to both roles of controller and processor, which are split in other BRICS frameworks such as the Brazilian LGPD or the South African POPIA. See CyberBRICS Project (n 10)

[82] The provisions dedicated to the establishment of this system are scheduled to enter in force in July 2021. At the time of this writing, Roskomnadzor has not yet published the technical specifications outlining the functioning of this consent management system.

lawfully collected. In this latter case, the data subject can address the request either to the operator that is illegally disseminating the personal data or to a Court of law.

The timeframe for stopping the dissemination will depend on the modalities of the request. In case of lawful collection of consent, Article 10.1(13) establishes that sharing must terminate as soon as the request is received. In case of illegal sharing, Article 10.1(14) prescribes that sharing will need to stop within three business days from the reception of the request or within a different timeframe established by a Court order.

Lastly, it is important to mention that, although Russian "data localisation" policies are not particularly recent, Russia can be considered a "trailblazer" in this peculiar field, as the normative provisions it adopted as early as September 2015, have inspired many other countries[83], including BRICS neighbours, such as China and India. Particularly, Article 18 of the Federal Law No. 152-FZ enshrines the obligation of the operator to ensure the localisation within Russian servers of the processing activities related to all personal data collected from Russian citizens.

Data localisation came into force on 1st September 2015 and includes the possibility of blocking the operator's online resource, whenever personal data of Russian citizens are processed in violation of localisation requirements. Clearly, the recent Russian invasion of Ukraine and the consequent Western sanctions have exacerbated the already ongoing tendency towards data localisation and "Internet sovereignty" which is deemed by Russia as top priority of national security justifying the implementation of a wide array of restrictive measures.[84]

To illustrate this tendency, several scholars have highlighted the relevant number of initiatives that Russia has introduced, over the past years, with the aim to expand control over data flows and regulate Internet users' behaviour, for instance blocking access to a large number of content

[83] For up-to-date details on how widespread the adoption of data localisation norms is, see Cory N., and Dascoli L. How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. Information Technology & Innovation Foundation. (2021).

[84] See Shcherbovich, A. Data protection and cybersecurity legislation of the Russian Federation in the context of the "sovereignization" of the internet in Russia. In Belli, L. (Ed.), CyberBRICS: Cybersecurity regulations in the BRICS countries. Springer. (2021) p. 67-131. https://link.springer.com/chapter/10.1007/978-3-030-56405-6_3 Daucé, F. and Musiani F. (Eds.) Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet. Vol. 26. N. 5 (May 2021). https://firstmonday.org/ojs/index.php/fm/issue/view/693

labelled as "extremist information," while also building considerable cyber-defense capabilities.[85] As such, data localization has become one of the fundamental tussles – although not the only one – of the Russian strategy for the assertion of digital sovereignty, based on a blend of data-related policies and "infrastructure-embedded control."[86] It is important to recognise that this Russian blend of digital sovereignty is increasingly inspiring governments and legislators globally.[87]

3.2.3. The Indian Data Empowerment and Protection Architecture

In July 2015, the Government of India launched the Digital India[88] program, an ambitious plan aimed at fostering the digital transformation of the country. While Digital India has very strong connectivity and eGovernment components, another key component, which is based on the establishment of a Digital Public Infrastructure, is a set of APIs[89] commonly referred to as the "Indian Stack"[90] that is particularly relevant to explain the evolutions that the Indian data protection framework undertook since the inception of Digital India.

Indeed, the use of the India Stack is deemed by the Indian Government as instrumental to achieve the Digital India vision, consisting in a substantial digital transformation fostering inclusive growth in highly strategic areas, such as digital products and services, automated manufacturing, thus unleashing job opportunities.[91] While the expansion of connectivity is instrumental to support the abovementioned vision, two elements of the India Stack are key for our analysis: Aadhaar and DEPA.

Aadhaar means "foundation" in Hindi and is the national digital identity system that, as of 2021, has been extended to more than 94% of the Indian population, making it "one of the most successful rollouts of any tech product anywhere."[92] As noted by Kak, Parsheera and Kotwal,

---

[85] Idem.

[86] See Daucé and Musiani (2021) *cit. supra*.

[87] See Cory and Dascoli (2021) *cit. supra*.

[88] Digital India, available at <https://www.digitalindia.gov.in/> accessed 8 October 2021

[89] An API, or application programming interface, is a piece of software that allows different software applications to interact and exchange data, according to the specifications established by the API.

[90] See <https://www.indiastack.org/>.

[91] Importantly, such vision is not exempted from critique, notably considering that India Stack has been essentially designed by iSpirt (the Indian Software Products Industry Round Table), a think tank for the Indian software products industry which has been criticised for its close ties with both government and large corporations, raising concerns related to conflict of interests, transparency and accountability. See https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf

[92] Aaryaman Vir and Rahul Sanghi, 'The Internet Country: How India created a digital blueprint for the economies of the future' (*Tigerfeathers*, 14th January 2021) <https://tigerfeathers.substack.com/p/the-internet-country> accessed 13 October 2021

Aadhaar's ability to uniquely identify individuals based on their biometric/demographic information has led the Indian government to make "mandatory, the use of Aadhaar numbers for various welfare schemes like the transfer of direct cash benefits under public distribution of food grains, employment guarantee benefits, midday meals in schools, subsidies, etc." While Aadhaar can be made mandatory for government benefits, welfare, it continues to be extensively used on a "voluntary basis" as an ID proof for all these other purposes.

Due to the Aadhaar potential for privacy abuses, the constitutionality of the program was challenged before the Indian Supreme Court. In its landmark Puttswamy case[93], the Court seized the occasion to pronounce the existence of a fundamental right to privacy in India, which can only be limited through fair, just, and reasonable procedures, clearly foreseen by the law. At the same time, the Court's decision opened the path to the elaboration of an Indian Data Protection Bill, which currently needs to be finalized by the Indian Parliament.

With the elaboration of the Data Protection Bill still ongoing, in August 2020, the Indian government's policy think tank, Niti Aayog, issued a draft paper aimed at fostering discussion on a new Data Empowerment and Protection Architecture (DEPA) framework.[94] The paper builds upon previous development of the "electronic consent framework", which was adopted in 2017,[95] as well on the existing implementations of the concept through the account aggregators framework, already adopted by the Indian financial sector.[96] DEPA is presented as a "secure consent-based data sharing framework to accelerate financial inclusion."

Through the establishment of DEPA, Niti Aayog aims at creating "an evolvable regulatory, institutional, and technology design for secure data sharing" that can "empower individuals with control over their personal data."[97] The elaboration of DEPA is particularly relevant, as it has been conceived to create a software architecture, based on shared public protocols, allowing all Indians to regulate, and somehow "customize", the flow of personal information that third parties may collect and process.

---

[93] For an analysis of the case, see Vrinda Bhandari and others, 'An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict' [2017] 11 IndraStra Global <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54766-2> accessed 13 October 2021

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

[95] See iSPIRT, 'Electronic Consent Framework' (*ProductNation*, 5 May 2019) <https://pn.ispirt.in/tag/electronic-consent-framework/> accessed 13 October 2021

[96] See George Mathew, 'Account Aggregators: New framework to access, share financial data' (*The Indian Express*, September 8 2021) <https://indianexpress.com/article/explained/account-aggregators-new-framework-to-access-share-financial-data-7490966/> accessed 13 October 2021

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

In practice, DEPA will be a system of digital consent management. The system will be based on the development of technical specifications to allow individuals to give consent to processing of personal data, defined by Ministry of Electronics and Information Technology[98], and the introduction of "consent managers" that will act as a new category of intermediaries. Such DEPA framework has already been adopted in the financial sector, through the Account Aggregator system, established by the Reserve bank of India. This latter system is grounded on the specification of technical standards and the establishment of a category of regulated intermediaries, named "account aggregators," which act as consent managers within the financial sector.[99]

In this perspective, the role of the DEPA consent managers will be to facilitate the flow of personal data from information providers to the users of the information, based on the consent of the individual. Thus, consent managers are supposed to act as data fiduciaries, which enable a data principal to gain, withdraw, review, and manage his consent through an accessible, transparent, and interoperable platform. They are not supposed to exploit personal data, but rather to be "data blind" and merely serve as a "conduit for encrypted data flows."[100]

Importantly, DEPA is also presented by Niti Aayog as the final layer of the India Stack, aimed at providing secure digital data sharing through consent. To understand DEPA, is indeed necessary to take a step back and remind that DEPA is a key "layer" of the India Stack, which aims at allowing all interested stakeholders – be them public bodies, businesses, start-ups, or non- profits – to use the Indian public digital infrastructure to deliver services.

However, despite its clear potential, DEPA needs to be considered in the light of the latest version of the Personal Data Protection Bill, to understand how DEPA must be established. One concern with this model is that it could lead to the over-simplification of consent. Indeed, while it is interesting to study how technology solutions can help manage consent effectively and empower data subjects, it must be noted that such framework is proposed while India still lacks a general data protection law. As pointed out by Reddy et al. (2020), the proposed data protection framework, in addition to consent, allows for various other lawful grounds of processing and, in

[98] See Ministry of Electronics and Information Technology, Electronic Consent Framework - Technology Specifications Version 1.1 (2016) <http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf> accessed 13 October 2021

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

[100] See Niti Aayog (n 88) 15

this perspective, additional research on the potential loss of control in event of relying on the other lawful grounds should be conducted.[101]

Indeed, the "consent manager" proposed under DEPA has the potential to become an element for both enhancement or reduction of data control from the individual, depending on how the DEPA structure is designed and its degree of synergy with the future Data Protection Law. As emphasized by Reddy et al., one must keep in mind that the primary objective of the DEPA framework shall be to grant individual control over personal data through the establishment of a secure and well-functioning protocol to share data across institutions, ultimately leading to individual empowerment and well-being.

Lastly, it is important to note the Russian and Chinese influences that may be found in the proposed Indian data architecture. First, all the last versions of the Indian Personal Data Protection Bill have introduced data localisation provisions, following the examples set by Russia and China, although tempered in some ways. In the 2021 Indian proposal, personal data considered as 'critical' must be processed in India. Sensitive personal data, however, can be transferred to another country, provided a copy of it remain stored in-country. The bill also commands the government to issue a detailed policy on data localization practices.

Lastly, while the earlier versions of the Data Protection Bill were silent on the issue of protecting deceased people's personal data, the Report of the Joint Committee on the Data Protection Bill of 2021[102] proposed the introduction of such a protection by means of section 17 of the bill. It is highly likely that this provision will be maintained in the final version of the Bill. The Chinese influence on its neighbour is evident, considering that China introduced the explicit protection of deceased people's personal data with PIPL, in 2021.

3.2.4. China's Personal Information Protection Law (PIPL) and the development of data protection in China

After essaying an approach to the subject of protection of personal information in legislation such as the Cybersecurity Law of the People's Republic of China[103], which entered into force in 2017

[101] See Shweta Reddy and others, The Centre for Internet and Society's comments and recommendations to the Data Empowerment and Protection Architecture (The Centre for Internet and Society, India 2020) available from <https://cis-india.org/depacomments> accessed 14 October 2021

[102] http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

[103] See Rogier Creemers, Paul Triolo and Graham Webster, 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)' (*New America*, 29 June 2018) <

and included in its general data governance framework the mission of ensuring and protecting "the lawful rights and interests of citizens, legal persons and other organisations", the Popular Republic of China has recently enacted its own data protection legislation, in the form of the Personal Information Protection Law (PIPL).

This wasn't at all the first time China's legislation touched the subject, as there were prior initiatives related to specific areas and topics such as "finance, credit reporting, telecommunications, internet, healthcare, e-commerce, and postal services"[104], and even specific legislation to protect children's personal information - the "Measures on Online Protection of Children's Personal Data" issued by the Cyberspace Administration of China (CAC), which was, unsurprisingly, put into comparison with the much older (1998) U.S.' Children's Online Privacy Protection Act (COPPA)[105], often with highlights to the more comprehensive approach of the Chinese legislation[106]. Other pieces of legislation also began to include typical data protection provisions, such as the *E-commerce Law* of 2018[107], which included a right of access for individuals to their personal data.

Another milestone in the development of data protection legislation in China was the enactment of China's first Civil Code[108], which entered into force in 2021 and presents a chapter entitled "Rights to Privacy and Protection of Personal Information", providing for rules determining limits to what can be done with personal information and conditions for its processing (articles 1033 and 1035), a definition of personal information broadly compatible with international standards

https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/> accessed 14 October 2021

[104] Mingli Shi, 'China's Draft Privacy Law Both Builds On and Complicates Its Data Governance' (*New America*, 14 December 2020) https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-privacy-law-both-builds-on-and-complicates-its-data-governance/ accessed 14 October 2021

[105] Children's Online Privacy Protection Act of 1998, 15 U.S.C. < https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule > accessed 14 October 2021.

[106] "Not only do the measures have a broader application compared to its counterpart in the U.S., but these measures also include prescriptive requirements on management measures to safeguard children's personal data." Gil Zhang and Kate Yin, 'China has released its version of COPPA' (*The Privacy Advisor*, 1 October 2019) <https://iapp.org/news/a/china-has-released-its-version-of-coppa/> accessed 14 October 2021

[107] United States Legislative Information, 'China: E-Commerce Law Passed' (*Library of Congress*, 21 November 2018) <https://www.loc.gov/item/global-legal-monitor/2018-11-21/china-e-commerce-law-passed/> accessed 14 October 2021; China Law Translate, 'PRC E-commerce Law (2018)' (*China Law Translate*, 31 August 2018) <https://www.chinalawtranslate.com/en/p-r-c-e-commerce-law-2018/> accessed 14 October 2021

[108] Civil Code of the People's Republic of China, available at <http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf > accessed 14 October 2021

("Personal information is the information recorded electronically or in other ways that can be used, by itself or in combination with other information, to identify a natural person, including his name, date of birth, identification number, biometric information, residential address, telephone number, email address, health information, whereabouts, and the like", in article 1034), liability rules, among other topics, including providing citizens with the right of action against the misuse of their personal data.

More recently, China began pursuing the enactment of a specific data protection legislation. The roots of the current proposal dates back to 2003, when a group of scholars within the Institute of Law at the Chinese Academy of Social Sciences led by Professor Zhou Hanhua prepared a data protection legislation draft[109], made public in 2005 and based on foreign experience adapted to China's specificities which, at the time, didn't make it to the legislative process. This draft, however, was the direct precursor to the current PIPL ("Personal Information Protection Law") - indeed it holds the same name as the 2005 proposal.

The PIPL draft was released by the China's National People's Congress (NPC) Standing Committee to public consultation in October 2020 and, after an initial series of feedback, a second version was released in May 2021. A new version of the text was then produced and on 20 August of the same year, the Standing Committee of China's National People's Congress promulgated China's Personal Information Protection Law (PIPL). The law entered in force on 1st November of 2021.

PIPL's final text presents very interesting developments, some of them even showing resemblance with paths taken by other BRICS countries when refining their own proposals. Take, for instance, what can be eventually perceived as gradual decay of consent as a principal or primary legal basis for data processing, which took place also in the Brazilian debate over its draft data protection law: its first public version, published in 2010[110], presented consent as the main legal basis for personal data processing, even mentioning the other legal bases (which were indeed present on the draft) as of a subsidiary character in comparison to consent. The Brazilian draft

[109] Available at https://pkulaw.cn/fulltext_form.aspx?Db=qikan&Gid=019044374cb8c449903aad34e3bfa5e1bdfb&EncodingName= accessed 14 October 2021

[110] For a description of the development of Brazilian General Data Protection Law since its first drafts, see Doneda (n 60) 3-20.

changed over the years to consolidate consent as one among the other legal bases for data processing[111], all in *pair conditio*, the approach that ended up in the LGPD.

Something similar indeed happened with PIPL, whose first draft[112] relied a lot on consent. Even if not appointing consent as a main or special legal basis, much of the text's structure and parameters were built on the assumption that consent was the instrument used for legitimising data processing. Its final version, even if maintaining this structural approach, seems to include a more diffuse approach on the legal basis for data processing by including two of the main standard legal bases present not only in the Brazilian legislation but also in most of such statutes, which are the processing of data for complying with a legal obligation and also for the execution of a contract (article 13).

PIPL presents a structure and conceptual framework which resembles the current international data protection standards, such as the Convention 108 of the Council of Europe or the OECD Guidelines. In its final version, PIPL introduced some provisions which can be generally found in the most recent data protection statutes, such as a data portability right (Article 45). Other particular innovations in this last text are the consideration of personal data of children (under 14) as sensitive data and also the more accurate provisions on international data transfers (Article 38).

In fact, PIPL goes even beyond these standards and points to some developments on the edge and yet to be considered in other major data protection legislations, such as the provision on its article 58 that commands big platform internet services to establish an independent supervision board with external members, to stop providing services that violate the law, a mandatory accountability measure which is an original feature among data protection frameworks. The same article 58 also mentions the obligation of internet platforms to release reports on their data processing activities and to accept what is described as "society's supervision".

PIPL, in fact, provides for a set of provisions which are relatively or even entirely new to data protection frameworks, such as the ban on automated decision-making for price discrimination (Article 24) or the specific provisions to the handling of deceased people's data (Article 49). This

[111] The second public version of the draft data protection legislation of 2015 followed this approach. See Ministério da Justiça e Cidadania, 'Conheça a nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais' (*Pensando o Direito*, 21 October 2015) <http://pensando.mj.gov.br/dadospessoais/2015/10/conheca-a-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/> accessed 14 October 2021

[112] The first draft of PIPL, made public in October 2020, is available at: < https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/ > accessed 14 October 2021

kind of provision regarding dead people's data usually depends not only on data protection standards but on other aspects of a country's legal system regarding the protection of personality and family law, among others, but, in PIPL, the subject was subjected to the data protection framework. It is important to stress this element of innovation as it is already deploying an international influence, as we have highlighted in the previous analysis of the Indian case.

PIPL recognises the Cyberspace Administration of China (CAC) as an equivalent to a Data Protection Authority (DPA), while also recognising that other authorities may have legal competence on data protection issues. Institutionally, CAC is under the Office of the Central Cyberspace Affairs Commission, which is headed by the Secretary-General of the Chinese Communist Party. CAC, created in 2011, is in charge of cyberspace security and internet content regulation among other issues[113], and would also, according to the current PIPL proposal, become the lead agency responsible for developing regulations and technical standards that will govern how the PIPL will be implemented[114].

3.2.5. The South African framework: POPIA's scope and the nature of the DPA and of the DPO

POPIA is a data protection law of the Republic of South Africa, established in November 2013 to bring transparency and accountability on entities processing personal data, aiming at providing individuals with control over their personal information. POPIA applies to any organization processing personal data within South Africa and to foreign organisation processing personal information in the country. However, the territorial scope defined by Section 3 of POPIA can be seen as narrower than GDPR of LGPD as the South African law applies only applies when the responsible party (*i.e.* the controller) is either domiciled in South Africa or is "using means" in

[113] Cyberspace Administration of China, available at <http://www.cac.gov.cn/> accessed 14 October 2021

[114] "Article 62:The State cybersecurity and informatization department coordinates overall the following personal information protection work by the relevant departments:
1. Formulate concrete personal information protection rules and standards;
2. Formulate specialized personal information protection rules and standards for new technologies and new applications regarding sensitive personal information, facial recognition, artificial intelligence, etc.;
3. Support the research and development of secure and convenient electronic identity authentication technology;
4. Advance the construction of service systems to socialize personal information protection, and support relevant organizations to launch personal information protection evaluation and certification services." Rogier Creemers and Graham Webster, 'Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021)' (*DigiChina Project*, 20 August 2021) <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> accessed 14 October 2021

South Africa, hence avoiding the more overarching reference to the offering of goods or services, or monitoring of individuals from abroad.

While its most distinguishing features are not unique in the world, they deserve to be mentioned as they make the South African framework unique within the BRICS context and may serve as useful experiences to be studied by other (BRICS). First, POPIA applies not only to personal data relating to living individuals, but also to personal data relating to existing legal persons, such as companies and non-profits. Second, POPIA establishes the Information Regulator as the independent data protection authority within the South African jurisdiction, but also empowering the body to monitor and enforce compliance with the Promotion of Access to Information Act, 2000 (PAIA Act 2 of 2000). In this sense, the data protection officer has a broader function than the one usually attributed by other frameworks. For this reason, the DPO is defined by POPIA and PAIA as an "information officer", which plays an instrumental to fulfil obligations related to both the protection of personal data and the due regulation of access to records held by public or private entities.

One of the main peculiarities of POPIA is that its Section 1 considers as a "data subject" the individual or the "juristic person" to whom personal information relate. In the same spirit, personal information is any information relating to an identifiable, living, natural person, and where it is applicable an identifiable, existing "juristic person." In the South African legal framework, there are two categories of legal subjects: natural persons and juristic persons (which are usually defined as "legal persons" in other frameworks). All human beings are considered as natural persons and legal subjects. Juristic persons are certain types of associations of natural persons, such as companies or non-profits. Hence, a major peculiarity of POPIA is that it includes juristic persons under its scope of application.

All responsible parties must appoint an Information Officer (IO). If no appointment is made, the head of the organisation (for example, the Chief Executive Officer or Managing Director) is automatically considered as the organisation's IO. Importantly, the details of each organisation's IO must be registered with the Information Regulator of South Africa or InfoReg (the national DPA), which has established a dedicated online portal to facilitate this task.[115] IO are also allowed to delegate their duties to deputy information officers.

Lastly, an important procedural element in the appointment of the Board of InfoReg, as it is both a testament to the highly democratic and open tradition that South Africa has endeavoured to bake into all governance processes since the Mandela era and a good practice that other countries could

[115] Online Portal – Registration of Information Officers, available at <https://www.justice.gov.za/inforeg/portal.html> accessed 14 October 2021

very easily copy. To identify members of the InfoReg, with appropriate qualifications and a sufficient degree of diversity – at least one member must have experience as a practising advocate or attorney, or a professor of law at a university, while the remaining members must be appointed on account of any other qualifications, expertise and experience relating to the objects of the regulator – the South African Parliament issues an open Call for Applications or Nominations.[116]

While different from the Brazilian type of multistakeholder participation within the national DPA, this form of openness to applications and nomination from any individuals, organisations, institutions and civil society at large is a very important procedural step that has the potential to strengthen the democracy, diversity and inclusivity of data protection institutions.

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

As argued above, 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 more carefully and that have the potential to inspire non-BRICS legislators and regulators. 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 an essential tussle of well-functioning digital economies, while fostering cybersecurity and strengthening digital sovereignty.[117]

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.

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. Moreover, the demand for data protection is becoming increasingly

[116] The most recent Call is available at <https://www.parliament.gov.za/press-releases/media-statement-justice-and-correctional-services-committee-calls-nominations-information-regulator> accessed 14 October 2021

[117] See Luca Belli '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 2021

popular amongst the billions of people in the BRICS and many individuals are beginning to understand the potential value of their data and the subjective dimension of data sovereignty.[118]

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.

In such context, the BRICS alignment towards shared data protection rules and principles has the potential to reduce transaction costs, deflating barriers to cross-border trade, and foster similar levels of protection of individual rights. Importantly, the convergence towards increasingly legally interoperable frameworks is already happening due to a phenomenon of transnational diffusion,[119] grounded on a process of adoption and reproduction of rules, procedures and good practices that are deemed as reliable and efficient. On top of such phenomenon, BRICS countries are demonstrating their willingness and capacity to be innovators and offer important contributions to the creation of a new generation of data protection policy and technology tools.

Given the BRICS appetite for Internet of Things (IoT), Smart Cities, fintech, and a variety of data-hungry technologies, and given the already relevant degree of compatibility of the existing BRICS data protection frameworks, this policy area should be a considered a suitable testbed to further cooperation enhancement. In this sense, it is important to stress the recent BRICS leaders' approval of the revised Terms of Reference of the BRICS Working Group on Security in the Use of Information and Communication Technologies (WGSICT), which plays a key role as regards BRICS digital policy coordination and cooperation, as well as of the BRICS Roadmap of Practical Cooperation on Ensuring Security in the Use of ICTs.[120]

In this context the BRICS leaders have explicitly reaffirmed "the importance of establishing legal frameworks of cooperation among BRICS member States on ensuring security in the use of ICTs and acknowledge the work of the WGSICT towards consideration and elaboration of proposals on this matter."[121]

Considering the high level of compatibility of existing data protection frameworks in the BRICS and the ongoing tendency towards enhanced cooperation on digital matters, it would be interesting to see the WGSICT putting forward concrete proposals on a BRICS Framework on Data

[118] 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

[119] For a more detailed discussion on how juridical systems be interoperable, see Belli and Foditsch (n 11).

[120] See BRICS 'Declaration of the 11th BRICS Summit' (Brasília 2019) para 19 <https://eng.brics-russia2020.ru/images/00/68/006895.pdf> accessed 14 October 2021

[121] See *ibid.*

Protection Cooperation. The WGSICT enjoys a unique position as well as an explicit mandate to elaborate proposals in this sense, thus becoming a key vector of legal interoperability within the BRICS. Such proposals would also allow to concretely implement BRICS STI Architecture, offering a unique opportunity to test a cooperation mechanism that is explicitly aimed at improving the coordination of BRICS initiatives on science, technology, and innovation.

BRICS countries have demonstrated that, while the countries remain a very elastic and heterogeneous grouping, they can achieve impressive results with concrete actions, including creating an entirely new global financial institution such as the New Development Bank, when their perspectives and interests align. Despite their obvious heterogeneity, it is evident that BRICS perspectives over personal data protection largely align, and their frameworks are already compatible, even in the absence of a formal agreement. Moreover, the BRICS have a relevant advantage of being a small club that continues to share an ample range of interests. Thus, enhancing their cooperation on digital matters, generally, and data regulation, particularly, is not only possible, but it may also represent a smart strategic and economic choice.

There is an increasing yearning for enhanced cooperation on digital governance amongst BRICS countries, as highlighted by the 2021 and 2022 BRICS Summit Declarations. Such cooperation may have a variable geometry, considering that some countries have a stronger ideological alignment than others, *i.e.* the IBSA countries on the one hand and the China-Russia duo on the other. However, considering that many data protection policy elements are already remarkably compatible and convergent, the enhancement of their legal interoperability looks not only feasible and achievable, but also in the interest of the grouping.

This scenario may be shaped by the definition of the policy elements of a general "BRICS Data Protection Framework" or a more specific "BRICS Data Transfers Framework" or "BRICS Data Security Framework." Indeed, as we have pointed out in the previous section, BRICS leaders have made explicit their appetite for the development of "intra-BRICS legal frameworks of cooperation" and BRICS policies are starting to be seen as models influencing other countries – including BRICS countries themselves.

The development of convergent and legally interoperable data protection frameworks should be uppermost in the list of their policy priorities as it is one of the few regulatory fields that is simultaneously key to protect individuals, provide juridical certainty to businesses, and foster international trade. Growing cooperation and legal interoperability amongst BRICS countries regarding digital policy is possible, it is already happening, and is explicitly advocated by BRICS leaders themselves. The degree of policy convergence now depends on how much BRICS will

manage to synchronise their political priorities and, critically, how much they will decide to dare in the implementation of the tools that are at their disposal.