NON-FINAL DRAFT submitted in May 2020 to the Chinese Academy of Cyberspace Studies as a contribution to the 2020 World Internet Conference outcome publications. Please contact the author luca.belli[at]fgv.br for the final version (to be published in Chinese and English).

Data Protection in the BRICS Countries: Enhanced Cooperation and Convergence towards Legal Interoperability

Luca Belli[1]

Abstract

This paper stems from the research elaborated by CyberBRICS project, which is the first attempt to produce comparative analyses of digital policies in the BRICS countries – namely, Brazil, Russia, India, China, and South Africa. The project is hosted by Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro, and developed in partnership with key academic partners in the BRICS area, and has three main objectives: 1) to map existing policies and regulations; 2) to identify good practices; and 3) to develop policy recommendations. This paper focuses on the ongoing development and increasing rapprochement of BRICS data protection frameworks. It highlights that the grouping can be considered as an example of enhanced cooperation on Internet governance and stresses the existence of a tendency towards convergence and legal interoperability of several aspects of their data protection policies. 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, implementing the BRICS Roadmap of Practical Cooperation on Ensuring Security in the Use of ICTs, and providing a useful opportunity to test for the new BRICS Science, Technology and Innovation (STI) Architecture.

---

[1] Luca Belli PhD is Professor at Fundação Getulio Vargas (FGV) Law School, where he heads the CyberBRICS project. He is also associated researcher at Centre de Droit Public Comparé at Paris 2 University. Professor Belli is also Member of the Board of the Alliance for Affordable Internet and Director of the Latin American edition of the Computers, Privacy and Data Protection conference (CPDP LatAm). The author would like to thank Luã Fergus for the useful feedback and the entire CyberBRICS team for their excellent work, inputs, and friendship.

1. BRICS countries evolving into CyberBRICS

At eleven-years old, BRICS are no longer a mere acronym[2], but have become a reality with progressively more intense relationships, a shared institution – the New Development Bank – and a continuously expanding agenda. In a world affected by pandemics, climate change and repeated financial shocks, and at a time in which geopolitical dynamics are reconfiguring at a remarkably intense rate, the BRICS grouping represents concrete evidence of how a "Post-western World"[3] might look like.

Needless to say, the challenges that BRICS countries face are enormous, but what seems increasingly clear is that existing opportunities are at least as relevant as existing challenges. Digital policies, in general, and data protection frameworks, in particular, are telling examples.

This paper stems from the research elaborated by CyberBRICS project[4], which is the first attempt to produce a comparative analysis of digital policies in the BRICS countries. The project is hosted by Fundação Getulio Vargas (FGV) Law School and developed in partnership with key academic partners[5] in the BRICS area, and has three main objectives: 1) to map existing policies and regulations; 2) to identify good practices; and 3) to develop policy recommendations. This paper focuses on the ongoing development and increasing rapprochement of BRICS Data Protection frameworks, stressing the existence of a tendency towards convergence, highlighting that the grouping can be considered as an example of "enhanced cooperation"[6] for internet governance and, lastly, arguing that BRICS should

[2] In 2001, economist Jim O'Neill coined the expression BRICs, without the capital "S", to refer to Brazil, Russia, India, China, which were deemed to experience a similar and particularly relevant phase of new and advanced economic development. See O'Neill (2001). 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.

[3] See Stuenkel (2016).

[4] See Belli (2020) and www.cyberbrics.info

[5] Partners include the Higher School of Economics, in Moscow, Russia; the Centre for Internet and Society, New Delhi, India; the Fudan University, Shanghai, and the Hong Kong University, China; and the University of Cape Town, Cape Town, South Africa.

[6] In Internet governance parlance, this term finds its origin in the UN-sponsored World Summit on Information Society – commonly referred to as WSIS – and was consecrated in the outcome of the second phase of the World Summit on the Information Society, held in Tunis in 2005. While this concept has never been detailed, after having been consecrated by Tunis Agenda for the Information Society, world leaders have agreed on "the need for enhanced cooperation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet. " See paragraph 69 of the Tunis Agenda for the Information Society (18 November 2005),

seize the opportunity to lead the development of "legally interoperable" [7] data protection frameworks.

To realise the relevance of the BRICS in general and, particularly, with regard to digital policies and data protection regulations, it is essential to consider that these countries together represent over 40% of the world population, being home to 3.2 billion individuals.[8] While the expansion of connectivity and the rise of new information and communications technologies (ICTs) are generating incredible opportunities for individuals and businesses, they also pose several challenges. The COVID-19 pandemic has clearly highlighted the essential value that connectivity has acquired, our reliance on well-functioning and secure ICTs and the key role that digital policies have acquired not for only for our future but already for the sustainability of our present.

In this perspective, the members of the BRICS grouping have realised that digital transformation is an essential element for the future of their economies and societies[9] and that data protection becomes a key priority to foster thriving digital environments, where individuals enjoy protections and businesses benefit from legal certainty. Since the BRICS ministers for science, technology and innovation met for the first time in 2014, the BRICS have remarkably intensified discussions in these areas and have started defining partnerships and enhancing their cooperation.

endorsed by the General Assembly of the United Nations in its Resolution 60/252. WSIS-05/TUNIS/DOC/6(Rev. 1)-E. <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>.
For a more detailed discussion of the topic, see Belli (2016:347-358).

[7] From a technical perspective the concept of interoperability is usually described as "the ability to transfer and render useful data and other information across systems, applications, or components" (ITU, 2015). Like technical interoperability, legal interoperability stimulates the exchange of information within different systems, by fostering compatible or shared normative frameworks. As such, interoperability of both technical and legal systems allows individuals to access and provide services in a cross-border fashion and to enjoy equal right-protection within different systems thanks to compatible (or shared) rules, principles and procedures. See Belli and Foditsch (2015).

[8] See BRICS (14 August 2019).

[9] See Belli (2020).

While adopting a number of shared documents[10], including the Memorandum of Understanding on Cooperation in Science, Technology and Innovation,[11] they started to conceive the design of the legal frameworks within which the various branches of their cooperation could be developed and thrive. As I will argue in this paper, the willingness to create partnerships and intensify research and policy synergies may be considered a telling example of what in Internet Governance vernacular is commonly referred to as "enhanced cooperation."

I argue that, when the aforementioned willingness to cooperate meets the global push towards more effective data protection regulations, it gives rise to a new generation of data protection frameworks, elaborated to meet the needs of the BRICS, while using the most modern data protection standards as a source of inspiration. Importantly, these two parallel phenomena – i.e. the enhancement of BRICS digital policy cooperation and the global movement towards personal data protection – are producing, as a collateral positive externality, a further phenomenon that is generally referred to as legal interoperability, consisting in the increasing compatibility of the BRICS normative frameworks regulating the protection of personal data.

The first section of this paper will set the scene, exploring how the increasing enhanced cooperation regarding digital policies has been unfolding in the BRICS agenda. The second section will focus on the BRICS Data Protection frameworks, providing concrete examples of what elements are already converging, based on the research developed by the CyberBRICS team.[12] The concluding section will briefly discuss the concept of legal interoperability, offering some concrete suggestions for BRICS countries to nurture and encourage this positive tendency, developing increasingly compatible and converging digital policies, particularly regarding data protection.

[10] For an analysis of such documents and their impact see Kiselev & Nechaeva (2018).
[11] The BRICS Memorandum of Understanding on Cooperation in Science, Technology and Innovation was approved at the second BRICS Science, Technology and Innovation Ministerial Meeting, held in Brasília, on 18 March 2015. See BRICS (18 March 2015).
[12] A detailed comparison of the normative elements in the BRICS data protection frameworks can be found in the BRICS Data Protection Map developed by the CyberBRICS. See https://cyberbrics.info/data-protection-across-brics-countries/

2. Enhancing cooperation on digital policies

The evolution of the BRICS digital policy agenda of the past five years can be seen as a telling example of enhanced cooperation. Indeed, the ample range of BRICS declarations and operational initiatives aimed at improving their cooperation on digital matters can be considered an example of how enhanced cooperation can be implemented in practice. Indeed, while the past decade has witnessed the construction of a stable process enabling the development of productive discussions about policy priorities in the BRICS, the past five years demonstrated the raise in prominence of digital issues and the emergence of a series of attempts to enhance cooperation on those issues, thus "enable[ing] governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet. "[13].

Since 2014, the discussion of digital matters amongst the five countries has acquired notable prominence. Together with the signature of the above-mentioned Memorandum of Understanding on Cooperation in Science, Technology and Innovation, in 2015, numerous initiatives have enhanced BRICS cooperation on digital matters. BRICS leaders have been stressing since their 7th Summit, held in the Russian city of Ufa in 2015, that ICTs "provide citizens with new tools for the effective functioning of economy, society and state […] and the use and development of ICTs through international cooperation and universally accepted norms and principles of international law is of paramount importance in order to ensure a peaceful, secure and open digital and Internet space."[14]

The Ufa Declaration can be seen as the document that started crystallising BRICS countries' consensus on the need to prioritise digital policies in general and cybersecurity in particular in their own national agendas, while also pursuing increasing compatible cybersecurity objectives. This can be considered as the start of a light cooperation on public policy issues pertaining to the national and international development of ICTs and particularly.

[13] See paragraph 69 of the Tunis Agenda for the Information Society (18 November 2005), endorsed by the General Assembly of the United Nations in its Resolution 60/252. WSIS-05/TUNIS/DOC/6(Rev. 1)-E. <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>.
[14] See BRICS. (9 July 2015).

The subsequent Goa Declaration, resulting from the 8th Summit, highlights the potential for cooperation amongst the BRICS countries that could "work together for the adoption of the rules, norms and principles of responsible behavior of States including through the process of the United Nations Group of Governmental Experts (UNGGE)"[15].

By explicitly mentioning the joint elaboration of rules, norms and principles, BRICS leaders crossed the Rubicon, willingly entering the Internet governance area and showing a clear intention to enhance cooperation on how to exercise their rights and responsibilities in international digital policymaking.

To manifest their intention in an even more explicit fashion, 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"[16].

Furthermore, the statements and the creation of a dedicated working group have been followed by several concrete initiatives, such as the BRICS Digital Partnership,[17] 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.[18]

These policy and operational initiatives emphasise "the importance of continuing BRICS scientific, technical, innovation and entrepreneurship cooperation,"[19] and culminated in the elaboration of an Enabling Framework for the Innovation BRICS Network[20] and the recent adoption of a new BRICS Science, Technology and Innovation Work Plan 2019-2022[21] and

[15] Ibid.
[16] Ibid.
[17] See BRICS Working Group on ICT Cooperation. (11 November 2016).
[18] *Idem.*
[19] See Itamaraty (27 June 2019).
[20] See BRICS STIEP WG (May 2019).
[21] See BRICS (October 2019).

established a new BRICS Science, Technology and Innovation (STI) Architecture.[22] The BRICS STI Architecture is a new mechanism that is explicitly aimed at:

- Improving the coordination and management of BRICS STI activities through the definition of an agile cooperation governance structure.
- Organising the different actions of STI cooperation according to their level of priority.
- Measuring, monitoring, and evaluating STI activities and initiatives, in order to minimise their development risks, make them result-oriented and optimise their real impact to society.
- Ensuring wide and effective dissemination of information about BRICS STI activities amongst different stakeholders including policy makers, scientists, research organisations and a wider audience.[23]

As acknowledged by the United Nations Economic and Social Council, "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."[24]

This lack of specification may be seen as problematic but, from another perspective, can also be considered as an advantage, as it provides all the necessary leeway to concretely implement cooperation amongst different partners, to achieve a wide spectrum of potential objectives, without having to be constrained by excessive procedure. De facto, the lack of a UN specification of what is enhanced cooperation allows any stakeholder to experiment different types of partnerships aiming at concrete outputs, thus privileging substance to formality.

The aforementioned initiatives and, particularly, the recent BRICS STI highlight how BRICS have fostered both intergovernmental and multi-stakeholder cooperation, with the aim to

[22] See BRICS (September 2019).
[23] See BRICS (September 2019).
[24] See UNGA (2011:6).

achieve concreate results. This is clearly not an easy task, due to the very loose configuration of BRICS and the lack of a coordinating body. However, BRICS countries have long recognized the value of enhancing their cooperation, involving a variety of actors into multi-stakeholder partnerships to deal effectively with digital challenges. Of course each BRICS country may have a different perspective on how such partnerships must be implemented and what stakeholders should be involved, but their diversity has always been considered as a point of richness rather than weakness.

Over the past few years, BRICS have consistently affirmed that "the Internet is a global resource and that States should participate on an equal footing in its evolution and functioning, taking into account the need to involve relevant stakeholders in their respective roles and responsibilities."[25] This posture denotes BRICS awareness that ongoing interaction with non-governmental stakeholders is a defining feature of enhanced cooperation processes, as internationally agreed since the adoption of the Tunis Agenda. The multiplications of BRICS partnerships, architectures and institutes dedicated to several types of cooperation on technology-related matters also denotes the understanding that, frequently, the collaboration between the academic and business communities can be even more fruitful than intergovernmental one.

In this perspective, it seems important to notice that the creation of both the first BRICS Technology Transfer Center and the first BRICS Institute of Future Networks in China, respectively in Kunming[26] and Shenzhen.[27] The Chinese proactiveness is not denotes the strong interest and commitment – even in financial terms – to promote and strengthen BRICS cooperation.

Remarkably, convergence and alignment are not limited to research and development but can also interest policymaking. The recent BRICS evolutions with regard to data protection demonstrate that, when the willingness to cooperate meets with global phenomena, such as the increasing tendency to regulate personal data, BRICS countries can also align their policy frameworks. As I will argue in the next section, many Data Protection policy elements

[25] Ibid.
[26] See Kunming (11 September 2019).
[27] The first Institute has been established in Shenzhen, China, in August 2019. See XinhuaNet. (2019).

are already very similar and, as I will suggest in the final section, the further enhancement of data protection frameworks towards their legal interoperability should be considered as a strategic priority for the BRICS.

3. Data Protection in the BRICS

The interest of analysing the digital policies elaborated by the BRICS and, particularly, their data protection frameworks is notable considering that, as mentioned above, such countries are home to approximately 42% of the global population and almost 40% of existing Internet users.[28] Concretely, this means that BRICS digital policies directly affect more than 2 out of 5 individuals on this planet. Furthermore, the consideration of BRICS demographics becomes particularly relevant also for another exquisitely economic perspective.

If people generate personal data, the logic consequence of roughly 3.2 billion individuals living in the BRICS is that these countries are the BRICS grouping is the largest producer of what is currently deemed as the world's most valuable resource.

The fact that a massive and growing number of BRICS citizens are already connected and are being introduced to digital technologies does not only create incredibly large data pools. It also provides a wide spectrum of potential developers and consumers of the technologies that will shape – and are already shaping – the evolution of the digital world. Of course, given the remarkable economic and strategic value that personal data have acquired, the regulation of this "new asset class"[29] also becomes an essential factor for the assertion of digital sovereignty.[30]

Over the past 5 years, the pressing need to regulate personal data and the growing alignment in BRICS digital priorities have spurred the proposal, adoption and implementation of increasingly compatible data protection frameworks. The grouping's willingness to cooperate on data protection norms and standards emerged since the Xiamen Declaration, issued after the 9th BRICS Summit in 2017, according to which the countries

[28] See https://www.internetlivestats.com/internet-users-by-country/
[29] See WEF (2011).
[30] See Belli (2020).

committed to jointly "advocate the establishment of internationally applicable rules for security of ICT infrastructure, data protection and the Internet."[31]

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.[32]

Indeed, all BRICS countries undertook major regulatory developments regarding data protection, in recent years, elaborating new legislation, updating existing one or establishing new regulatory agencies. These evolutions include:

- In August 2018, the adoption of a new Brazilian General Data Protection Law[33] and, in August 2019, the approval a new National Data Protection Authority (although this has not been established yet).
- In December 2017, the update of the Russian Data Protection legislation including data localisation provisions.
- In August 2017, the recognition of privacy as a fundamental right by the Indian Supreme Court and the elaboration of a new Data Protection Bill, on which the Indian Parliament is expected to deliberate soon.
- In June 2017, the introduction of a new right to the protection of personal data in the new General Provisions of the Civil Code as well as data protection and data localisation norms in the Chinese Cybersecurity Law, further specified by the 2018 Personal Information Security Specification.
- In 2017, the establishment of a Data Protection Regulator in South Africa, created by the 2013 Protection of Personal Information Act, which will be fully implemented in the upcoming months.

In a very condensed timeframe, BRICS have revolutionised data protection in their legal systems. Interestingly, despite the absence of any formal agreement on the substance of

[31] See BRICS (2017).
[32] The BRICS Data Protection Map developed by the CyberBRICS team may be a useful resource for readers interested in learning more. See https://cyberbrics.info/data-protection-across-brics-countries/
[33] An English version of the Law can be downloaded at https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/

their domestic frameworks, several regulatory elements are extraordinarily similar. The main reason for such convergence is likely the common inspiration from existing frameworks, particularly the European GDPR as well as the OECD Guidelines.

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. Due to the relatively recent development of the BRICS data protection framework, BRICS decision makers have enjoyed the privilege of constructing their norms based on existing best practices.

A patent example is the definition of personal data, which all BRICS – with a slightly different formulation in China[34] – consider as the information related to an identified or identifiable natural person. A very similar approach also underpins the definitions of sensitive data, data subject and data controller.[35]

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 global principle core that is usually common beyond BRICS, at least as regards the first four principles. The BRICS data protection principles[36] include consent, purpose limitation, fair and lawful treatment, necessity, data minimisation, and accountability. Furthermore, BRICS legislators have included a very similar spectrum of rights although with different flavours.[37] 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.

[34] See: policy question 7 of the BRICS Data Protection Map https://cyberbrics.info/data-protection-across-brics-countries/
[35] See: "Definitions", *ibid.*
[36] See: policy question 9, *ibid.*
[37] See: policy question 13, *ibid.*

BRICS data protection frameworks also present a very comparable set of obligations for data controllers and processors.[38] Interestingly, while the definition of data controller is virtually the same in the five frameworks, the Chinese Specification does not include the role of data processor.[39] The core obligations for data controllers in the BRICS include abiding to data protection principles, obtaining a free and informed consent in order to process data, duly communicating information on the data processing, and ensure the security of all personal data under their responsibility.

Finally, yet importantly, all BRICS countries have considered the essential role of international data transfers for the (digital) economy. All BRICS favour data transfers but only if foreign third parties are deemed as providing an acceptable level of protection. 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.[40]

4. Towards legal interoperability on data protection in the BRICS

The abovementioned elements highlight that a shared Data Protection skeleton is emerging in the BRICS, spontaneously increasing the compatibility of national frameworks. The reasons why these regulatory (r)evolutions are happening in the BRICS may be quite heterogeneous and the overall results are very positive. First, the protection of personal data has finally entered national debates. This, by itself, is a tremendously important advancement in countries where there is near-to-zero data protection culture, but personal data are harvested at industrial scale.

The raising relevance of data protection is due partly to the global policy tendencies, notably the adoption of the GDPR, as well as the numerous data-related scandals and the realisation

[38] See: policy question 14, *ibid*.
[39] See: policy question 9, *ibid*.
[40] See: policy question 22, *ibid*.

that data protection is an essential tussle of cybersecurity and digital sovereignty.[41] In this context, the BRICS willingness to enhance their cooperation and alignment regarding digital policy making is patent and the benefits of compatible regulations may be enormous for both users and businesses.

In fact, although in most BRICS countries data protection frameworks still have to be finalised or properly enforced, the introduction of norms, based on which compliance can be planned, is providing greater juridical certainty to any entity processing data while also expanding individual rights. The governments of the BRICS nations clearly understand that each of their citizens is a producer of personal data that, combined, are immensely valuable, and know that strong data protection frameworks are key to protect their economies and societies.

Indeed, it is undeniable that the establishment of sound regulations foster the protection of individual rights and the establishment of more sustainable digital environments. This consideration is becoming increasingly popular amongst the billions of people in the BRICS and many individuals are beginning to understand the potential value of their data, the need to regulate how they are used and prevent misuse, demanding high standards for data protection[42].

Modern and compatible frameworks are needed to protect individual rights and provide legal certainty for businesses. 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,[43] grounded on a process of adoption and reproduction of rules, procedures and good practices that are deemed as reliable and efficient.

[41] See Belli (2019).
[42] See Saks (2019).
[43] For a more detailed discussion on how juridical systems be interoperable, see Belli & Foditsch (2015).

Given the BRICS appetite for Internet of Things (IoT), Smart Cities, 5G, 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.

On the one hand, the development of initiatives fostering personal data protection and individual control in BRICS countries could be extremely interesting form a research and development standpoint, giving rise to new technology and business opportunities. On the other hand, policy-oriented research and initiatives may produce valuable output that can provide guidelines on how to foster further cooperation and legal interoperability through new and creative approaches. Both types of initiatives would 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.

The establishment of a cooperation governance structure, a monitoring process and the involvement of a wide range of stakeholders "including policy makers, scientists, research organisations and a wider audience"[44] seem to be very promising elements on which digital policy cooperation could be enhanced, with particular regard to data driven technology and personal data related policies 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, where their perspectives and interests align. Although the current geopolitical scenario is characterised by increasing nationalism and mounting scepticism towards multilateral bodies, the BRICS have still a very relevant role to play, demonstrating that and international cooperation can be both achievable and beneficial, even when partners are very diverse.

[44] See BRICS (September 2019).

Despite their obvious heterogeneity, they have a relevant advantage of being a small club that continues to share an ample range of interests. Enhancing their cooperation is not only possible, it would likely be the smartest geopolitical choice.

The development of convergent and legally interoperable data protection frameworks should be uppermost in the list of their priorities as it is one of the few regulatory field 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 and, to some extent, already happening. As founder and director of the CyberBRICS project, the author of this chapter hopes that more research and cooperation on such policies will emerge, allowing Cyber-BRICS to grow strong on the foundations built by solid BRICS.

5. References

Belli, Luca (Ed.). (2020). CyberBRICS: CyberBRICS: Cybersecurity Regulations in the BRICS Countries. Springer. https://cyberbrics.info/cyberbrics-cybersecurity-regulations-in-the-brics-countries-full-ebook/

Belli, Luca. (2016). De la gouvernance à la regulation de l'Internet. Paris: Berger-Levrault.

Belli Luca. (13 November 2019) From BRICS to CyberBRICS: New Cybersecurity Cooperation. China Today. http://www.chinatoday.com.cn/ctenglish/2018/tpxw/201911/t20191113_800184922.html

BRICS. (September 2019). A New BRICS STI Architecture. http://brics2019.itamaraty.gov.br/images/documentos/The_New_BRICS_STI_Architecture__Steering_Committee__Final_19_9_19.pdf

BRICS. (October 2019). BRICS Science, Technology and Innovation Work Plan 2019-2022. http://brics2019.itamaraty.gov.br/images/documentos/BRICS_STI_Work_Plan_2019-2022__Final.pdf

BRICS. (July 2018). 10th BRICS Summit Johannesburg Declaration — BRICS in Africa: Collaboration for Inclusive Growth and Shared Prosperity in the 4th Industrial Revolution. July 25-27 2018, Johannesburg, South Africa. http://www.brics.utoronto.ca/docs/180726-johannesburg.html

Kunming. (11 September 2019). Kunming enhances technology cooperation with BRICS countries. http://en.kunming.cn/c/2019-09-11/10793655.htm

Internet World Stats. Available at: <https://www.internetworldstats.com/stats.htm>.

Itamaraty. (27 June 2019). BRICS Informal leaders' meeting on the margins of the G20 Summit – Joint Media Statement – Osaka, 28 June 2019. http://www.itamaraty.gov.br/en/press-releases/20557-brics-informal-leaders-meeting-on-the-margins-of-the-g20-summit-joint-media-statement-osaka-28-june-2019

ITU. (2015). "Interoperability in the digital ecosystem". GSR discussion paper. Retrieved from http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/Discussionpaper_interoperability.pdf

O'Neill, Jim. (November 2001). Building better global economic BRICs. New York: Goldman Sachs. Global Economics Paper, n. 66. http://www.goldmansachs.com/our-thinking/archive/archive-pdfs/build-better-brics.pdf

Sacks, Samm (07 Feb 2019). **China's privacy conundrum.** Slate Available at: <https://slate.com/technology/2019/02/china-consumer-data-protection-privacy-surveillance.html>.

Stuenkel, Oliver. (2016). Post-Western World: How Emerging Powers Are Remaking Global Order. Polity Press.

UNGA (United Nations General Assembly) (2011). Enhanced cooperation on public policy issues pertaining to the Internet Report of the Secretary-General. Economic and Social Council A/66/77–E/2011/103.

WEF (World Economic Forum). (January 2011). Personal Data: The Emergence of a New Asset Class. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

XinhuaNet. (7 August 2019). BRICS set up new institutional branch to strengthen cooperation on ICT. http://www.xinhuanet.com/english/2019-08/07/c_138289903.htm