CyberBRICS, Focus on Cybersecurity

Efficiency in governance for data protection and cybersecurity is vital

By Luca Belli

Concluding a very productive ministerial meeting held in Brasilia in August 2019, the BRICS Ministers of Science, Technology and Telecommunications have released an important Joint Declaration highlighting the strategic interest of BRICS partnerships on new digital infrastructures, 5G technologies, the Internet of Things (IoT) and cybersecurity.

Modern infrastructures, efficient cybersecurity governance and, particularly, sound data protection regulations, are crucial issues for the inclusive and sustainable development of BRICS countries. Especially as they are massively betting on digitalization and on the potential of interconnected and interdependent technologies, such as 5G and IoT.

Digital transformation is an essential element for the future of BRICS economies and societies, and this is precisely why BRICS member countries are elaborating on digitalization strategies and some are already implementing these strategies.

China is by far the country with the most systemic approach, having invested heavily in 5G technologies, so much so that it is now leading the global 5G race, as well as cybersecurity capabilities. China recently adopted well-coordinated cybersecurity legislation, an e-commerce law and data protection standards.

Brazil, by contrast, has only recently started to implement its one-year-old Digital Transformation Strategy, and while the new General Data Protection Law will come into effect in 2020, the organ that will have to implement it still has to be created. The Brazilian government only established a National Plan for IoT in June 2019, but Brazil still lacks a cybersecurity strategy, although the Presidency's Institutional Security Cabinet is working to develop one.

In such a complex context, digital transformation may offer great benefits while at the same time also create great risks. Billions of interconnected devices controlled via 5G networks have the potential to greatly enhance robotics, industrial automation, smart farming, and provide incredible efficiency gains due to vast data collection and processing capabilities. At the same time, the interconnection of every "thing" requires the highest level of security to avoid hackings, data leaks and the transformation of the BRICS digital dreams into potential nightmares.

As cybersecurity experts say, there are only three types of Internet users in the world: those who have already been hacked, those who will be hacked, and those who are being hacked as we speak.

Half of the BRICS population is already connected to the Internet, generating an incredible amount of data, producing new innovative products and daily purchase of devices that are connected by default. These advancements are revolutionizing our online and offline lives and, while they are generating new multifaceted threats, are also presenting unprecedented opportunities.

Over the next five years, massive projected growth in Internet access is expected in the big countries that make up the BRICS area, especially China, India and Brazil. In this context, an important clarification seems necessary to understand why BRICS countries are particularly keen on embracing the opportunities of digitalization. The 3.2 billion people living in the BRICS countries are not simply potential consumers or developers of digital services. They are the potential producers of what is currently deemed as the most valuable asset in the world: personal data.

From this perspective, it becomes more intuitive why the Indian government advocates so tenaciously for sovereign control of data, why Russia has just adopted Digital Sovereignty legislation and why all BRICS countries are adopting or implementing personal data regulations.

The BRICS countries, where 42 percent of the world's population resides, are also the holders of 42 percent of the world's most valuable resource: the personal data of their citizens. Thus, the development of digital policies, particularly with regard to cybersecurity and data protection, becomes a highly strategic priority for economic and social development and for ensuring the safety of people, the data they produce and the critical infrastructures they utilize daily.

It is particularly important to note that the multibillion population of BRICS countries is increasingly demanding higher standards of data protection to make sure that the abundance of personal data that digital technology has the ability to collect be used to improve people's lives.

The fact that in the last 5 years, all members of the group have adopted or proposed regulatory frameworks for personal data protection, is a clear signal of the strategic importance of data control and security for both the governments and the people of BRICS.

42% of the world's population lives in the BRICS countries, and this is the bloc's most valuable resource: the personal data of its citizens. Their protection is a strategic priority.

BRICS Communications Ministers gathered in their 5th meeting on August 14, 2019 in Brasilia.

The enormous opportunities offered by technological improvements can be seized only in the presence of solid personal data regulation and cybersecurity frameworks.

This point is particularly relevant, considering that BRICS countries are the main targets of cyber-attacks, as well as being the countries from which most cyber-attacks originate. For this situation to change, thorough strategies and well-informed policies need to be developed and implemented, creating a synergy among BRICS.

In an environment where access to digital technologies is becoming essential for communicating, learning, doing business and socializing, and all "things" are being connected in IoT systems, BRICS need not only efficient but also convergent digital policies.

The early findings of the research developed by the CyberBRICS project demonstrate that BRICS face common challenges and many of the policies they are adopting, or are already in place, present several points of commonality. In this sense, they should seize digital transformation to enhance their cooperation and develop common or, at least compatible, solutions.

Members of the bloc can learn a great deal from their own experiences and are in a phase which is particularly propitious to align their regulatory frameworks. According to the BRICS Science, Technology and Telecommunications ministers, studying and understanding their collective digital polices is a complex task. They reaffirmed their commitment to enhance joint research cooperation and address the challenges of cybersecurity.

A cooperative stance and a comparative perspective are essential, not only to foster mutual understanding and the respect for each other's culture, but also to enable the development of interoperable technologies and regulations capable of fostering access to innovative services and products, while ensuring protection of users' rights.

BRICS members may have different sensitivities, but their priorities and goals are frequently very similar. In this light, the establishment of a solid, multi-stakeholder cooperation initiative, where BRICS governments can dialogue with academics, the private sector and civil society representatives, receiving input and feedback as regards the various aspects of their cybersecurity policies, would be a profitable strategy for all.

To begin with, BRICS governments, which in recent years have consistently stressed the value of enhanced cooperation on research and technological development, could support the establishment of a BRICS think-tank cooperation mechanism on cybersecurity. As the pioneering experience of the CyberBRICS project demonstrates, analyzing existing digital policies is paramount to identifying good practices and proposing sustainable and fair solutions.

Brazil's rotating presidency of BRICS is a unique opportunity to formulate a positive and proactive agenda, highlighting the benefits of improved cooperation on digital policies in general and on cybersecurity in particular.

Luca Belli, *PhD is Professor of Internet Governance and Regulation at FGV Law School, in Rio de Janeiro, where he heads the CyberBRICS project.*