ANALYTICAL REVIEWS

International Organisations Research Journal, 2022, vol. 17, no 3, pp. 212–234
Analytical Review
doi:10.17323/1996-7845-2022-03-09

Approaches of BRICS Countries to Data Regulation[1]

A. Shelepov

Andrey Shelepov—Candidate of Economic Sciences, Senior Researcher, Centre for International Institutions Research, Russian Presidential Academy of National Economy and Public Administration; 11 Prechistenskaya naberezhnaya, 119034, Moscow, Russian Federation; shelepov-av@ranepa.ru

Abstract

Data are not a new resource in the economy, but they are now growing at an unprecedented rate as a result of the proliferation of digital devices and services. An analysis of emerging national data regulation systems identifies significant differences in national approaches, especially in relation to cross-border data flows, due to economic specifics and national interests. Differences of approach among the major players create challenges for other countries, increase the fragmentation of the global regulatory environment, produce uncertainty, and increase compliance costs for businesses. These factors determine the importance of international cooperation in the field of data management.

This review presents the approaches of the BRICS countries—Brazil, Russia, India, China, and South Africa—to the regulation of data, primarily of their cross-border flows, as well as the requirements for localization of data storage and operations.

Based on the results of the review, general trends in the approaches taken by the BRICS countries to regulation can be identified, leading to the conclusion that it is possible to strengthen interaction within BRICS, primarily in relation to mutual recognition of the adequacy of existing and contemplated data protection measures to ensure mutually beneficial cross-border movement of data.

Keywords: digital economy, data governance, cross-border data flows, BRICS

Acknowledgments: the article was written on the basis of the RANEPA state assignment research programme.

For citation: Shelepov A. (2022) Approaches of BRICS Countries to Data Regulation. *International Organisations Research Journal*, vol. 17, no 3, pp. 212–234 (in English). doi:10.17323/1996-7845-2022-03-09

Introduction

Data are becoming an increasingly important resource in the global economy, and the use of data has a significant impact on economic and social processes. The role of data in the global economy is stipulated by rapid digitalization, the inexhaustibility of data as a resource, and the possibility of its use by a large number of actors without significant costs to create economic and social value.

[1] This article was submitted on 09.08.2022.

In the context of acute geopolitical contradictions and information wars, mistrust and risks of misuse and malicious use of data are growing. Accordingly, there is an increasing desire to protect data privacy through conditional cross-border data transfers or requirements for data storage and processing within specific state boundaries. Contradictions between actors in international regulatory regimes are aggravated. In order to reduce the risk of influence in multilateral institutions that contradicts Russian interests and approaches in relevant areas, it is important to strive for the formation of international principles for regulating data flows and protecting data in cooperation with key partners, primarily the other BRICS countries (Brazil, India, China, and South Africa).

To assess the prospects for data governance cooperation within BRICS, the approaches of these partner countries are examined. The analysis includes the normative documents these four countries have in force or plan to adopt. The main emphasis is on approaches to cross-border data flows, an area with the most significant differences in regulation across countries.

BRICS Approaches to Data Governance

China

Despite China's leading position in the digital economy, including its status as the largest actor in cross-border data flow chains, the relevant regulatory system in China began to take shape only relatively recently. The current economic and political system of China implies the active government participation in economic and social processes, which determines the significant role of the state in the digital economy and, in particular, the relatively strict regulation of cross-border data flows across borders and within the country.

The concept of digital sovereignty is at the core of China's policy on data flows. China's approach to digital sovereignty is based on the understanding of digital technologies and the Internet as the most important geopolitical asset. Chinese policy is aimed at promoting technology leadership on a global scale, as well as data protection (a key government concern, see S. Budnitsky and L. Jia [2018]), with a particular emphasis on security [Creemers, 2020]. This approach is also reflected in Chinese policy on data flows.

China's data flows regulatory system, which is still under development, is based on three acts that came into force in the past five years—the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law—and related regulations and by-laws.

China's Cybersecurity Law explicitly sets out localization requirements for certain categories of data. In accordance with the law, personal information and important data collected and generated by critical information infrastructure operators in China must be stored within the country [Creemers, Triolo, Webster, 2018]. While the Cybersecurity Law does not provide a detailed definition or scope of activities for critical information infrastructure operators, it notes that China will focus on protecting certain critical industries, including, but not limited to, public communications and information services, energy, transportation, finance, and public services where destruction, loss of functionality, or data leakage may lead to a threat to national security or public interest [Ibid.].

The Cybersecurity Law also provides that if the cross-border transfer of personal and sensitive data is necessary due to business needs, a security assessment must be carried out following the measures formulated by the state Cyberspace Administration and the relevant departments of the State Council ("security assessment"). The Cybersecurity Law does not directly list the measures and procedures for security assessment, however, in recent years, some draft documents in this area have been issued. One such document is the Draft Measures on Security

Assessment of Cross-Border Data Transfer. Under the Cybersecurity Law, "critical information infrastructure operators" are required to undergo security assessments, while the Draft Measures extend this obligation to "network operators." Thus, network operators in China are classified as critical infrastructure operators, which makes the interpretation of such infrastructure very broad. Formally guided by the goals of ensuring security in cyberspace, China has introduced significant legal restrictions on cross-border data flows.

In addition to these requirements that apply to data flows in general, in order to "ensure public security and facilitate access to data by regulators," China has also introduced data localization requirements for specific sectors, including health information [Hu, Gong, Yang, 2022], credit files [Order No 631, 2013], personal information collected by commercial banks [NRF, 2020], organizations that operate navigation and mapping services [Si, Cai, 2021], online taxi platforms [Interim Administrative Measures, 2016], and online bicycle sharing operators [Yang, 2020], as well as in relation to information constituting state secrets [Cadwalader, 2011].

The Cybersecurity Law has addressed the governance and security of digital data, but other types of data have remained outside the regulation perimeter. The Data Security Law has filled this gap, as it covers all types of data (including both electronic and non-electronic data) and covers the full cycle of operations with them [Data Security Law, 2021]. Unlike the Cybersecurity Law, which only governs digital data, the scope of the Data Security Law also extends to non-electronic data. In addition, while both laws provide for the possibility of being applied to illegal activities abroad, sanctions under the Cybersecurity Law are limited to cases of exporting personal data collected in China, importing "illegal" data from abroad, and actions that seriously compromise the security of China's critical information infrastructure. Under the Data Security Law, any overseas data processing activities that endanger China's national security, the public interest, or the legitimate rights of any person or entity are illegal. Thus, the Data Security Law is based on a more comprehensive approach, providing very broad grounds for its enforcement.

The term "national security" is very often mentioned in the Data Security Law in comparison with "privacy protection." Thus, it seems that strengthening national security is a key factor behind the adoption of the law. Under the Data Security Law, for the first time, the Chinese government has established a centralized classification system based on the level of data importance. Data relating to national security, the national economy, social welfare, and critical public interests are considered as core data and operations with them are subject to more stringent verification. The Chinese government is currently preparing the publication of national, regional, and departmental catalogues with a classification guide to ensure greater control over core data processing activities.

As for data exports, it seems that the main purpose of China's regime is to counter the Clarifying Lawful Overseas Use of Data (CLOUD) Act adopted in the United States in 2018. The CLOUD Act allows U.S. law enforcement agencies to request access to electronic data, regardless of the country in which they are stored. However, under the Cybersecurity Law of 2016, exports of personal data and sensitive data stored using critical information infrastructure in China is subject to security assessments. This measure is reinforced by the Data Security Law, which also provides that companies that fail to comply can be fined up to 10 million yuan (about $1.5 million), and face suspension of their activities or closure.

To complete the formation of the Chinese data regulatory framework, it was necessary to adopt legislation directly related to personal data. On 20 August 2021, the Personal Information Protection Law (PIPL) of the People's Republic of China (PRC) was adopted, with key aspects very similar to the European model embodied in the General Data Protection Regulation (GDPR) [PIPL, 2021]. The law provides for a definition of personal information, explains the

legal basis for personal data processing, establishes obligations and responsibilities of processors, and provides for strict data localization requirements to protect Chinese interests in cross-border personal information transfers. Although the PIPL is similar to the European Union's (EU) GDPR, there are some differences and additional requirements in Chinese law.

The PIPL provides for extraterritorial jurisdiction under certain circumstances. Three cases have been identified when extraterritorial jurisdiction may apply, including when the purpose of the data processing is providing goods or services to individuals in China, "analysis" or "assessment" of Chinese citizens' behaviour, or other purposes provided for by other regulatory legal acts [PIPL, art. 3]. A processor that plans to transfer personal information to organizations outside China must provide individuals with specific information about the transfer and obtain separate consent for this, take necessary measures to ensure that foreign recipients provide the same level of information protection as established in accordance with the PIPL, and conduct an impact assessment regarding personal information protection.

Chinese law provides for localization requirements. Operators or organizations that process a large amount of personal information (when the amount of personal data processed reaches certain thresholds set by the relevant government agency) are obliged to store personal information in China. If such personal information needs to be transferred overseas, the organization must undergo a security assessment by the Cyberspace Administration of China (CAC) and other relevant authorities. A similar requirement also applies if the processor falls under the definition of "critical information infrastructure operator."

In other cases of cross-border transfer, the law allows choosing one of the following options: passing the security assessment organized by the relevant government authority (CAC) (similar to critical information infrastructure operators and cases of processing large amounts of personal information), obtaining a personal information protection certificate from professional institutions recognized by CAC, concluding an agreement with a foreign personal information recipient in accordance with the standardized contract form provided by CAC that specifies the rights and obligations of both parties, or fulfilling other conditions established by laws, administrative regulations, or the relevant government authority [PIPL, art. 38].

Analysis of China's legal acts regulating data flows shows they are aimed at protecting the country's digital sovereignty and ensuring cybersecurity. Since the Chinese model for regulating cross-border data flows is based on the central role of cybersecurity in national security, it is quite restrictive [Lee, 2018; Liu, 2019]. Localization requirements and restrictions on transferring data to other countries indicate that the Chinese government seeks to maximize digital sovereignty and minimize the possibility of foreign interference, which is a distinctive feature of the PRC's approach compared to other countries analyzed. At the same time, China provides an example of a restrictive approach, which, combined with strategic state intervention in the economy, has helped stimulate domestic digital market growth and ensure the global reach of large national technology companies. Given the need to further expand these companies' activities, including international ones, economic aspects have become more and more important in data regulation policy over time (even though initially the main goal of regulating cross-border data flows in China was to ensure national security).

China is currently finalizing a national data governance and protection system that requires certain conditions to be met for cross-border data transfer, including a security assessment by government agencies, and establishes localization requirements—all critical information infrastructure operators, understood very broadly, and personal information processors must store personal information they collect locally.

At the same time, economic interests tend to soften China's official position regarding free data flows and convergence in approaches with other countries, including BRICS partners, despite the previously introduced restrictions. Thus, the PIPL expressly states that the

PRC government will strive to conclude international agreements on personal data transfers and mutual recognition of standards for personal information protection [PIPL, art. 12]. In 2020, the Chinese government announced its readiness to allow cross-border data flows in the Hainan Free Trade Zone [Lu, 2020]. The Chinese authorities also noted the importance of international coordination in the field of data security and recognized that local data storage requirements cannot be considered universal for all countries. Experts agree that a key reason for a shift in China's data flow policy is the desire to strengthen the digital dimension of economic projects, in particular within the One Belt One Road Initiative (OBOR)—the Digital Silk Road launched in 2015 [Liu, 2020].

India

Despite its large population and the rapid increase in access to telecommunications networks, as well as numerous national companies in the telecommunications industry, India has not yet adopted special legislation to govern data flows, including their cross-border movement. However, a comprehensive data regulation is currently under discussion and is expected to be adopted in the near future.

Based on the interpretation adopted by the Supreme Court of India in 2017, the right to life of Indian citizens includes the right to privacy, including data and privacy protection [Committee of Experts on Data Protection, 2018]. Shortly after this announcement, a special committee was established, chaired by former Supreme Court Justice B.N. Srikrishna, which presented a report on the need for new data protection legislation along with a draft Personal Data Protection Bill. The bill was aimed at regulating the flow and use of personal data and the activities of various entities processing personal data; protecting the fundamental rights of persons whose data is being processed; establishing a regulatory framework for accountability, data processing, and cross-border transfers; and providing legal protection in case of violations. It also proposed to establish the Data Protection Authority to reach these objectives. The 2018 bill was slightly revised before being submitted for consideration and is currently awaiting approval in the Indian Parliament as the 2019 Personal Data Protection (PDP) Bill [PDR Bill, 2019].

The PDP Bill, introduced in the Indian Parliament by the Ministry of Electronics and Information Technology on 11 December 2019, is largely modelled after the EU's GDPR. It applies to personal data processed in India by the Government of India, any company or legal entity registered in India, and foreign companies dealing with personal data of Indian individuals (for example, dealing with data of Indian citizens outside the country), subject to certain requirements. These requirements provide for extraterritorial application of the act if the processing of data by foreign companies, regardless of their physical presence in India, is connected with "any business carried on in India or any systematic offering of goods or services to data principals within India; or profiling data principals within India" [Ibid.].

The bill provides for the creation of the Data Protection Authority (DPA), which is entrusted with broad rule-making, administrative, and quasi-judicial functions. Its functions are similar to that of the European Data Protection Board.

The bill imposes obligations on data fiduciaries ("those who, alone or in conjunction with others, determine the purpose and means of processing of personal data"), including providing data principals with detailed notice prior to data collection and obtaining their consent; processing data only for a clear, specific, and legitimate purposes and in a fair and reasonable manner; retaining data only until the purpose of the collection is achieved; and taking steps to ensure transparency and accountability.

The bill establishes different localization rules for different categories of personal data. Data localization requirements are identified within a three-level structure. Restrictions on

transfers (localization requirements) do not apply to personal data in general but are imposed on "sensitive personal data" and "critical personal data." Sensitive personal data may be transferred abroad for processing if the individual has expressly consented to this and subject to certain additional conditions, but it still must be stored in India [PDR Bill, 2019]. Sensitive personal data includes "such personal data which may reveal, be related to, or constitute: financial data; health data; official identifier; sexual orientation; biometric data; genetic data; transgender status; caste or tribe; religious and political belief or affiliation; and any other data" specified by the Government of India in consultation with the DPA and the regulator in the specific sector [Ibid.]. Critical personal data, in general, cannot be transferred outside of India and is processed only within the country. However, to a limited extent, regulators plan to allow the transfer of such data to other countries or organizations, although the specific mechanism is not specified in the bill. Critical personal data is defined as "such personal data as may be notified by the Central Government to be the critical personal data" [Ibid.].

A key motivation for including localization requirements in the proposed regulation appears to be the protection of Indian economic interests by ensuring that local digital data is primarily used to develop domestic digital companies (so-called "data champions"), thereby limiting "data colonialism" by large technology companies [Hicks, 2019; Mint, 2019]. In addition to protecting economic interests, India's restrictive approach to regulating cross-border data flows is based on various advantages of data localization to ensure effective regulatory oversight and enforce domestic laws. For example, Indian regulations require all payment system providers to store data relating to such systems locally (even if such data are processed abroad) so that the Reserve Bank of India can "have unfettered supervisory access to data stored with these system providers as also with their service providers / intermediaries/ third party vendors and other entities in the payment ecosystem" [Reserve Bank of India, 2018]. Similarly, in the context of personal data protection, the Srikrishna Committee report noted that the "effective application" of the Indian PDP Bill "will invariably require data to be stored locally within India, and this would mean that such a requirement, where applicable, would limit the possibility of cross-border data transfers." At the same time, data localization requirements, in addition to their legal and regulatory advantages, are in line with the logic of domestic economic development policy: if more data can be stored in India, this will lead to improvements in domestic digital infrastructure for new digital technologies such as artificial intelligence and the Internet of things [PRS Legislative Research, n.d.].

In general, the PDP Bill is to a large extent based on the EU's GDPR. However, the specifics of the Indian approach to digital economy development based on supporting "national champions" predetermined a number of differences that characterize India's policy as more protectionist. The key difference is India's planned introduction of localization requirements.

The approach prescribed in the draft PDP Bill (localization requirements depending on the category of personal data) is also proposed to be used in relation to non-personal data. The draft National E-Commerce Policy [Government of India, 2019] provides for data localization measures. The report of the Committee of Experts on Non-Personal Data, established by the Ministry of Electronics and Information Technology, recommended the introduction of data localization requirements for certain categories of non-personal data, similar to those envisaged in the PDP Bill. Thus, sensitive non-personal data can be transferred outside the country, but will have to be stored in India, and critical non-personal data can only be stored and processed locally [Committee of Experts on Non-Personal Data, 2020].

Some commentators believe that in recent years the Indian government has moved from minimal oversight of cybersecurity and data security to over-control. In particular, due to the vagueness of some concepts, concerns have been raised about the potentially "excessive" powers granted to the Government of India under the PDP Bill. Most of the criticism is related to

localization requirements. The PDP Bill, similar to the National E-Commerce Policy titled "Indian Data for India's Growth," explicitly highlights the country's commitment to the development of its digital sector using data to drive national companies' growth. Unlike developed countries, the Indian government seems to believe that implementation of such an approach is impossible without data localization measures. Accordingly, the Personal Data Protection Bill assumes that copies of sensitive personal data will be stored in India, and the cross-border transfer of critical personal data will be almost completely prohibited.

Given the broad scope of the definition of sensitive personal data, the proposed bill imposes a greater compliance burden on companies compared to the current legal regime (currently data can be transferred to any country provided that the transfer is necessary to fulfil an existing contract and the principal has consented to such transfer) [Ministry of Communications and Information Technology, 2011, rule 7]. In addition, there is an opinion that the Government of India will treat any data as critical personal data, since this term is not clearly defined in the PDP Bill [2019]. At the same time, cross-border transfer of non-critical personal data will also be possible only in limited circumstances to countries for which the government expressly allows such transfers (adequacy approach), pursuant to intra-group data transfer schemes approved by the government, when explicit consent is given by the data principal, or based on a need for any specific purpose determined by the regulatory body [Ibid.].

Thus, several important issues regarding enforcement aspects and their impact on data flows regulation in India remain unclear. In the near future, the Government of India is most likely to pass the PDP Bill approved by the joint parliamentary committee. After its entry into force, the scope of data localization requirements and other norms that are not clearly defined and will be applied based on the regulator's decisions will become clear. Accordingly, potential for India's cooperation on data regulation issues with other BRICS countries will become clearer.

Brazil

Currently, Brazil's main regulation on data flows is the Personal Data Protection Law (Lei Geral de Proteção de Dados Pessoais, LGPD). It was adopted in 2018, entered into force in 2020, and in 2021 liability for violation of its provisions became effective. The law systematizes and unifies the Brazilian legal framework, which consists of more than 40 different legislative acts in the field of data governance, replacing some provisions of existing laws and supplementing others. The law provides for the regulation of personal data processing, including by digital means, by a natural person or legal entity under public or private law, with the aim of protecting fundamental rights to freedom and privacy and free personal development [LGPD, 2018].

Based on the text of the law, several types of data with different regulation regimes can be identified. Personal data means data that allows identifying a natural person directly or indirectly. This type of data is understood quite broadly, without further explanation. Personal data is subject to regulation under the LGPD. Confidential data are data with processing possible only after obtaining the express consent of the data principal and for a specific purpose. The LGPD determines that, without express consent, the processing of such data is only possible when the information is necessary in situations related to a legal obligation, public policy, preservation of human life and physical integrity, for preserving health privacy, and fraud prevention. Sensitive data reveals a person's racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic information, biometrics, or information about a person's health or sex life. The processing of sensitive personal data is carried out only in the following situations: with the specific and explicit consent of data principal or his/her legal representative, for specific purposes, or without the consent of data principal, when it is

necessary for: the fulfillment of a legal or regulatory obligation by data controller; joint processing of data when this is necessary for the public administration to comply with public policy requirements provided for in laws or regulations; research conducted by a research organization, while ensuring the anonymization of sensitive personal data; regular exercise of rights, including under a contract and within the framework of judicial, administrative, and arbitration procedures; protecting the life or physical security of data principal or a third party; protection of health, exclusively within the framework of a procedure carried out by medical professionals, health services, or sanitary authorities; ensuring fraud prevention and security of the data principal; and identification or authentication of registration in electronic systems. Public data processing must take into account the purpose, good faith, and public interest that justify data accessibility [Ministry of Citizenship, n.d.].

The law applies to any data processing operation carried out by a natural or legal person under public or private law, regardless of the means, the country in which its headquarters is located, or the country in which the data is located, provided that the processing is carried out in Brazil, processing activities are aimed at offering or providing goods or services or at processing data of natural persons located in Brazil, or the personal data being processed was collected in Brazil. Thus, similar to other norms considered, the Brazilian law provides for extraterritorial application.

Concrete definitions of the terms "data controller" and "data processor" are not provided in the text of the law. The National Agency for the Protection of Personal Data (ANPD), established by this law, is responsible for clarifying the statuses and issuing relevant instructions. The lack of definitions and explanations creates legal uncertainty in the early stages of the law's enforcement, since the recently established ANPD (its creation was delayed, including due to the initial veto of the president and then the pandemic) has not yet issued the required instructions.

The Brazilian law permits cross-border personal data transfers only in the following cases: to countries or international organizations that provide a level of personal data protection that is adequate to the LGPD provisions; when a controller offers guarantees of and proves compliance with the principles and respect for the rights of data principal and the data protection regime provided for by this law, in the form of special contractual clauses for a specific transfer, standard contractual clauses, binding corporate rules, and regularly issued certificates and codes of conduct; when the transfer is necessary for international legal cooperation between state intelligence, investigative, and prosecutorial bodies, in accordance with international law principles; when the transfer is necessary to protect the life or physical security of the data principal or a third party; when national authorities authorize the transfer; when the transfer is part of an obligation in the framework of international cooperation; when the transfer is necessary to carry out public policies; and when the data principal has given his/her specific and expressed consent to the transfer, being previously informed about the international nature of the transfer.

The level of data protection in a foreign country or international organization is assessed by Brazilian national authorities, which take into account general and sectoral legislation in force in the destination country or international organization, the nature of data, compliance with the general principles of personal data protection and respect for the rights of data principals provided for by the LGPD, adoption of security measures provided for by Brazilian regulations, availability of judicial and institutional guarantees for the observance of rights related to the protection of personal data, and other specific circumstances of the transfer.

Six of the eight mechanisms for approving cross-border data transfers require decisions by the ANPD. This supervisory body is at the formation stage. The five ANPD directors were appointed by President Bolsonaro and took office on 6 November 2020. The ANPD has also hired 19 out of 31 employees it can under the presidential Executive Order 10.474/2020. It remains unclear how long it will take to assess, establish, and approve data transfer mechanisms

as provided for in the law. At the moment, companies can use only two data transfer mechanisms—specific and clear consent or the need to perform a contract.

In the future, the approach chosen by the ANPD will determine the cross-border data transfer regime. There are several models in the world that can be examined to choose the best one for Brazil. Alternatively, Brazil could develop its own governance model. The ANPD could consider the "EU plus" approach for determining the adequacy of protection in certain jurisdictions, as Israel and Colombia have done, or choose the UK model, delegating such decisions to data controllers. The ANPD may also recognize the existing EU standard contractual clauses (SCCs) and binding corporate rules (BCRs) or simply require contractual safeguards to provide adequate protection, as Canada has done. It can also initiate the issue of certificates or codes of conduct—through participating in the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) System [APEC, n.d.] or working with local associations to recognize codes of conduct and expand their scope by appointing third party certifiers [IAPP, 2020]. Establishing rules for cross-border data transfers is one of the priorities of the ANPD for the next two years, so its first decisions are expected by the end of this year or in early 2023 [ANPD, 2021]. To the moment, the ANPD has launched international cooperation with the EU and the UK. In April 2021, the agency took part in the UK-Brazil Digital and Cyber Dialogue 2021 to share experiences and discuss international data flows governance issues. In addition, ANPD members took part in the Data Protection Academy project organized by the University of Maastricht as part of the cooperation between the ANPD and the European Commission [Neeser, 2021].

The Brazilian data protection law was largely modelled after the EU's GDPR. These two legal acts are very similar: in fact, their principles coincide, extraterritoriality is implied, and similar rights are guaranteed to data principals. The cross-border data transfer provisions in Brazilian law are also similar to the GDPR. The differences between the two laws are minor. An important factor of this is Brazil's accession to the Organization for Economic Co-operation and Development (OECD) and its desire to develop domestic legislation in line with the OECD approaches. At the same time, the EU and the OECD cooperate closely, and many principles and recommendations proposed by the OECD are reflected in the EU's legal framework.

In its current form, the LGPD does not impose localization requirements, and experts assess it as restrictive, but not prohibitive. For example, the United Nations Conference on Trade and Development (UNCTAD) in its report placed Brazil in the category of countries with a conditional data transfer regime, assessed the conditions for data transfer as quite strict, and the approach itself as prescriptive [2021]. However, various political forces, mainly from the left of the political spectrum, seek to either amend the LGPD to tighten its conditions, or introduce new, more restrictive laws.

In general, Brazil's political system is competitive, diverse, and relatively balanced. Left-wing parties and their representatives are in favour of greater restrictions in data flows governance, and support localization and "landing" of companies. They are particularly concerned about the de facto dominance of some companies and platforms, which creates conditions for undermining competition and violating citizens' rights. Right-wing and centre parties oppose localization, but still advocate for certain rules. They are interested in the effective implementation of the LGPD and progressive development of the ANPD to establish a harmonious data governance framework. The outcomes of presidential and parliamentary elections will greatly affect data regulation developments. Given the relative equality of support to the two options, there may be stagnation since neither side will be able to gain the necessary majority to ensure the adoption of their initiatives as laws. The president has more power to issue decrees, so presidential elections are more likely to affect the governance regime compared to parliamentary ones. Lula's victory would most likely lead to strengthening Brazil's identity as a developing

country, a representative of the Global South, an active participant in South-South cooperation, and an important BRICS actor. One can expect increased restrictions on cross-border data flows and the adoption of "landing" and localization requirements, as this is in line with the left parties' agenda. Regardless of the election results, regulators will focus on addressing the risks posed by digital platforms, especially those with a dominant position in the digital services market. Bolsonaro's victory would most likely preserve the current approach, which combines the absence of localization requirements with acknowledging the need to restrict data flows in certain cases.

In general, Brazil's position could contribute to successful BRICS cooperation on data governance. There are no visible contradictions between Brazil and other BRICS members, as it recognizes the right of each jurisdiction to establish its own requirements and rules and notes that data flow restrictions may inevitably arise. Requirements for jurisdictions to recognize their data protection regimes as adequate do not include political components or values. Brazilian regulation is soft compared to China or even Russia and the policy develops rather by inertia, but certain political forces advocate for stricter requirements, including localization.

South Africa

The legal framework for data governance in South Africa is currently being established. The need to adapt national legislation to the new circumstances is highlighted by the growth in the number of Internet users in the country since 2000, which has accelerated significantly during the coronavirus pandemic, and the increasing demand for electronic communication and digital commerce tools.

The Protection of Personal Information Act (POPIA) signed in 2013 is the main one in this legal framework. Given the fundamental nature of the proposed changes in the activities of public authorities and private companies, its entry into force took eight years. The provisions of the law entered into force in stages, and some of them were revised after the adoption of the 2020 Cybersecurity Act. In addition, the provisions regarding reporting by private companies provided for a one-year transitional period, and therefore POPIA only became effective in practice from July 2021.

Based on the basic principles of South African data policy, the main responsibilities of data operators include compliance with the requirements for ensuring the legality and openness of operations with data, as well as their security. POPIA requires all organizations involved in personal data processing to appoint a person responsible for compliance with personal data regulations and submit relevant information to the national regulator. By default, this task is assigned to companies' executive directors. According to POPIA, data operators should submit internal regulations to ensure security of processed data for consideration by the national regulator. In case of violation of data integrity and security, operators are obliged to submit information about the incident to competent authorities within 72 hours.

POPIA applies to data operators that are registered legal entities in South Africa. The extraterritoriality of the act is manifested if the data controller is not registered in South Africa but uses automatic and/or non-automatic data processing tools for data collected in South Africa. An exception is made for operators who only transmit data through the territory of South Africa and whose activities are not related to data collection and processing in the country. Unlike the laws of other BRICS countries discussed above, POPIA does not apply to the activities of companies that are registered in foreign jurisdictions but offer goods or services to consumers in South Africa.

According to the act, the transfer of personal information to a third party outside of South Africa is prohibited except for certain cases. One such case is if the data recipient outside of

South Africa is committed to comply with corporate rules or agreements that provide for a sufficiently high level of data protection that meet the following requirements: effectively support the principles of rational data processing, which are substantially similar to the conditions for lawful processing of personal information relating data principal, which is an individual or, where applicable, a legal entity;[2] are substantially consistent with the content of the act regarding the onward personal information transfer from the recipient to a third party located abroad.[3] Other cases include those in which the data principal has consented to the transfer of information, the transfer of information is necessary for the fulfillment of contractual obligations between data principal and the responsible party or for the implementation of pre-contractual measures taken in response to the request of data principal, the transfer is necessary for the conclusion or performance of a contract concluded for the benefit of data principal between the responsible party and a third party, the data transfer is carried out in the interests of the data principal, obtaining the consent of the data principal for data transfer does not seem appropriate, and if there are no obvious grounds for assuming that the data principal could refuse to transfer the data concerned.

Thus, South African law does not establish requirements for digital data localization, but the transfer is still conditional. The requirement for localization can likely be strengthened in the process of implementing the Draft National Data and Cloud Policy proposed in 2021 [Republic of South Africa, 2021].

Over the past few years, South Africa has made significant progress in the development of national data governance. The benefits created by the development of digital and data processing technologies have become an impetus for the development of relevant national legislation. The second equally important factor is cybersecurity. The adoption of the Cybercrimes and Cybersecurity Act and the entry into force of all the POPIA provisions made it possible to resolve several important regulatory issues—conditions for data transfer to operators located abroad were specified, the powers of the national regulator in terms of monitoring local data operators were defined, and offences related to the violation of data privacy were determined. Nevertheless, on several issues, there is a need for further decision-making at the state level.

First, the issue of formalizing data localization requirements has not been addressed, although such requirements are organically combined with POPIA requirements. Lack of resources needed to enforce this solution locally leads to the absence of such requirements, which could both reduce the attractiveness of the South African market for foreign data companies and create additional difficulties for national operators. The need to store user information locally is highlighted as a priority area of work in the Draft National Data and Cloud Policy. Thus, in the near future relevant proposals are likely to be presented as draft laws.

Second, South Africa's cautious position toward international agreements on data governance may result from a lack of available competencies or trained workforce, as well as resources for its formation, to fulfil obligations on ensuring personal data security at the international level, as required, for example, by the African Union Convention on Cyber Security and Personal Data Protection. The case of negotiations on e-commerce within the World Trade Organization (WTO) supports this idea—Indian and South African positions focus on the expected negative consequences of lifting protectionist restrictions in e-commerce for digital industries in developing countries, which will face competition with more advanced foreign information technology giants, having both a technological base and relevant competencies. Maintaining

[2] It should be noted that there are no other comments regarding the semantic content of the "principles of rational data processing" in POPIA. Some experts indicate there are eight basic principles of data processing. See for example: https://www.popiact-compliance.co.za/popia-information/17-conditions-for-lawful-processing-of-personal-information

[3] The text of the law does not specify what is meant by these provisions.

restrictions should therefore allow developing countries to catch up with developed ones without putting their emerging industries at risk.

Third, along with the lack of resources, there are some shortcomings in the institutional environment. The powers to control implementation of relevant laws are distributed among various bodies—for example, compliance with certain POPIA provisions is controlled by the national regulator, while the police are responsible for monitoring compliance with other regulations, also acting as the operator of a special coordination centre involved in monitoring cyber incidents and, in some cases, as a platform for interaction with foreign authorities on combating cybercrime. At the same time, a legal gap remains that allows foreign actors, in exceptional cases which are not specified in the law, to bypass this coordination centre and directly interact with the responsible representatives of the country's judiciary, which according to some experts, can be considered as a violation of state sovereignty.

Finally, to date insufficient data have been accumulated regarding the effectiveness of the adopted regulatory measures in practice. The Cybercrimes and Cybersecurity Act came into force in December 2021, while the abovementioned coordination centre on cyber incidents is still being prepared for launch in 2022. POPIA fully entered into force in 2021, therefore, to date the actual experience of compliance by national data operators with the requirements for enforcing personal data protection plans agreed by the state regulator is less than one year. The real impact of the measures discussed is yet to be assessed in the coming years.

Conclusion: Potential for BRICS Cooperation

The analysis shows that four BRICS countries differ in terms of regulatory approaches to data, primarily regarding restrictions on their cross-border flows. The main difference is that China and India use or plan to apply a restrictive or binding approach, which implies data localization requirements. Brazil and South Africa currently use a prescriptive approach, implying conditionality of cross-border data transfers and different requirements for those willing to export personal data.

China pursues an expansionist strategy that reflects the logic of its domestic regulation models. The state control data governance model (which may also be called the cyber sovereignty model) aims to support the entry of national digital and telecommunications companies into developing countries' markets, including in the framework of the One Belt One Road initiative [Erie, Streinz, 2021]. The approaches of other countries are more focused on development using domestic resources. India relies on a protectionist approach to data governance aimed at supporting domestic companies; in Brazil there is a political struggle between free data flows and localization proponents, and each group claims to protect the national interests; and South Africa, similar to India, declares supporting "national champions" through proper data governance as a priority in its Draft National Data and Cloud Policy [Industrial Development Think Tank, 2019].

Thus, despite some differences, there is a potential for convergence in BRICS approaches based on the common idea of supporting domestic digital sectors. Cooperation within BRICS is also important as the digital platforms from the U.S. and other western countries strive to build digital markets in their own interests, and these countries' governments seek to support their companies through appropriate regulation of cross-border data flows.

The basis for a feasible, inclusive multilateral governance is an agreement on convergence of data regulation while maintaining sovereignty, which, to varying degrees, is stated as a goal by all countries considered. The consensus on data protection in this case may primarily concern the level of protection rather than regulatory practices, without introducing conditionality or

localization requirements, and just defining basic cooperation and interaction principles for relevant government bodies [Heseleva, Ramos, Ichilevici de Oliveira, 2020].

Accordingly, within BRICS cooperation could primarily address mutual recognition of regulatory norms as corresponding to a certain universal level of protection to ensure proper cross-border data transfers, with a possible further expansion to other aspects of data governance.

References

Asia-Pacific Economic Cooperation (APEC) (n.d.) What Is the Cross-Border Privacy Rules System. Available at: https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system (accessed 7 September 2022).

Budnitsky S., Jia L. (2018) Branding Internet Sovereignty: Digital Media and the Chinese-Russian Cyberalliance. *European Journal of Cultural Studies*, vol. 21, issue 5, pp. 594–613. Available at: https://doi.org/10.1177%2F1367549417751151.

Cadwalader (2011) New Laws in China Regarding "State Secrets" and Related Issues: Uncertainties, Obstacles, and the Need to Strengthen Internal Compliance Procedures. Clients & Friends Memo. Available at: http://www.cadwalader.com/uploads/cfmemos/unpublished_9fad844172d0f2825abf771d457de53f.pdf (accessed 7 September 2022).

Committee of Experts on a Data Protection Framework for India Under the Chairmanship of Justice B.N. Srikrishna (Committee of Experts on Data Protection) (2018) A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. Report of the Committee and Draft Bill. Available at: https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf (accessed 7 September 2022).

Committee of Experts on Non-Personal Data Governance Framework (Committee of Experts on Non-Personal Data) (2020) Report. 111972/2020/CL&ES. Available at: https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf (accessed 7 September 2022).

Creemers R. (2020) China's Approach to Cyber Sovereignty. KAS Innovation No 4, Konrad-Adenauer-Stiftung. Available at: https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537 (accessed 7 September 2022).

Creemers R., Triolo P., Webster G. (2018) Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). *New America Blog Post*, 29 June. Available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (accessed 7 September 2022).

Data Security Law of the People's Republic of China (Data Security Law) (2021) Order of the President of the People's Republic of China No 84, Adopted at the 29th Meeting of the Standing Committee of the Thirteenth National People's Congress, 10 June. Available at: http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml (accessed 7 September 2022).

Erie M.S., Streinz T. (2021) The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance. *New York University Journal of International Law and Politics*, vol. 54, no 1, pp. 1–92. Available at: https://www.nyujilp.org/wp-content/uploads/2022/02/NYUJILP_Vol54.1_Erie_Streinz_1-91.pdf (accessed 7 September 2022).

General Personal Data Protection Act (LGPD) (2018) Lei No 13.709, 14 agosto [Law No 13.709, 14 August]. Presidência da República, Secretaria-Geral, Subchefia para Assuntos Juridícos. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (accessed 7 September 2022). (in Portuguese)

Government of India (2019) Draft National E-Commerce Policy: India's Data for India's Development. Ministry of Commerce & Industry. Available at: https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf (accessed 7 September 2022).

Heseleva K., Ramos V.J., Ichilevici de Oliveira A. (2020) Towards a Multilateral Consensus on Data Governance. *G20 Insights*, 29 May. Available at: https://www.g20-insights.org/policy_briefs/towards-a-multilateral-consensus-on-data-governance/ (accessed 7 September 2022).

Hicks J. (2019) "Digital Colonialism:" Why Countries Like India Want to Take Control of Data From Big Tech. *The Print*, 29 September. Available at: https://theprint.in/tech/digital-colonialism-why-countries-like-india-want-to-take-control-of-data-from-big-tech/298217/ (accessed 7 September 2022).

Hu C., Gong J., Yang J. (2022) China. *Digital Health Laws and Regulations*. International Comparative Legal Guides, Global Legal Group. Available at: https://iclg.com/practice-areas/digital-health-laws-and-regulations/china (accessed 7 September 2022).

Industrial Development Think Tank (2019) Towards a Digital Industrial Policy for South Africa: A Review of the Issues. University of Johannesburg. Available at: http://www.thedtic.gov.za/wp-content/uploads/DPIP.pdf (accessed 7 September 2022).

Interim Administrative Measures for the Business of Online Taxi Booking Services (Interim Administrative Measures) (2016) Order No 60 of the Ministry of Transport, the Ministry of Industry and Information Technology, the Ministry of Public Security, the Ministry of Commerce, the State Administration for Industry and Commerce, the General Administration of Quality Supervision, Inspection and Quarantine, and the Cyberspace Administration of China. Available at: https://uk.practicallaw.thomsonreuters.com/w-003-2260?transitionType=Default&contextData=(sc.Default)&firstPage=true (accessed 7 September 2022).

International Association of Privacy Professionals (IAPP) (2020) Top-5 Operational Impacts of Brazil's LGPD: Part 3: International Transfers. 5 November. Available at: https://iapp.org/news/a/top-5-operational-impacts-of-brazils-lgpd-part-3-international-transfers/ (accessed 7 September 2022).

Lee J.A. (2018) Hacking Into China's Cybersecurity Law. *Wake Forest Law Review*, vol. 53, no 1. The Chinese University of Hong Kong Faculty of Law Research Paper No 2018-08. Available at: https://ssrn.com/abstract=3174626 (accessed 7 September 2022).

Liu J. (2019) China's Data Localization. *Chinese Journal of Communication*, vol 13, issue 1, pp. 84–103. Available at: https://doi.org/10.1080/17544750.2019.1649289.

Lu X. (2020) Is China Changing Its Thinking on Data Localization? *The Diplomat*, 4 June. Available at: https://thediplomat.com/2020/06/is-china-changing-its-thinking-on-data-localization/ (accessed 7 September 2022).

Ministry of Citizenship (n.d.) Classificação dos Dados [Data Classification]. Available at: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados (accessed 7 September 2022). (in Portuguese)

Ministry of Communications and Information Technology (2011) Notification. New Delhi, 11 April. *The Gazette of India: Extraordinary*, part II-sec 3(i). Available at: https://meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf (accessed 7 September 2022).

Mint (2019) India's Data Must Be Controlled by Indians: Mukesh Abani. 20 January. Available at: https://www.livemint.com/Companies/QMZDxbCufK3O2dJE4xccyI/Indias-data-must-be-controlled-by-Indians-not-by-global-co.html#:~:text=Gandhinagar%3A%20Richest%20Indian%20Mukesh%20Ambani,and%20control%20their%20own%20data (accessed 7 September 2022).

National Data Protection Authority (ANPD) (2021) Planejamento Estratégico ANPD 2021–2023 [ANPD Strategic Planning 2021–2023]. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/planejamento-estrategico/planejamento-estrategico-2021-2023.pdf(accessed 7 September 2022).

Neeser R. (2021) Is the Brazilian Data Protection Law (LGPD) Really Taking Off? *JD Supra*, 8 June. Available at: https://www.jdsupra.com/legalnews/is-the-brazilian-data-protection-law-1094165/ (accessed 7 September 2022).

Norton Rose Fulbright (NRF) (2020) PBOC Issues New Specification on Personal Financial Information. Available at: https://www.nortonrosefulbright.com/en/knowledge/publications/fcdc5f10/pboc-issues-new-specification-on-personal-financial-information (accessed 7 September 2022).

Order of the State Council No 631 (Order No 631) (2013) The Regulation on the Credit Reporting Industry, as Adopted at the 228th Session of the Executive Meeting of the State Council on December 26, 2012, Is Hereby

Issued and Shall Come nto Force on March 15, 2013 (translated from Chinese). Available at: http://www.pbccrc.org.cn/crc/jgyhfw/201309/1ca0f775b50744cabaf83538288d77a9/files/e8a8bf080ed64f48914a652da1d8fdc3.pdf (accessed 7 September 2022).

Personal Information Protection Law of the People's Republic of China (Personal Information Protection Law) (2021) Adopted at the 30th Meeting of the Standing Committee of the Thirteenth National People's Congress, 20 August Available at: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (accessed 7 September 2022). (in Chinese)

POPI Act Compliance (n.d.) POPIA Conditions for lawful processing and how to comply. Available at: https://www.popiact-compliance.co.za/popia-information/17-conditions-for-lawful-processing-of-personal-information (accessed 7 September 2022).

PRS Legislative Research (n.d.) Report Summary on A Free and Fair Digital Economy. Available at: https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy#:~:text=Srikrishna)%20submitted%20its%20report%20and,draft%20a%20data%20protection%20Bill (accessed 7 September 2022).

Republic of South Africa (2021) Draft National Policy on Data and Cloud. Department of Communications and Digital Technologies. Staatskoerant, 1 April. Available at: https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf (accessed 7 September 2022).

Reserve Bank of India (2018) RBI Guidelines on Storage of Payment System Data. Available at: https://www.nbti.in/rbi-guidelines-on-storage-of-payment-system-data/ (accessed 7 September 2022).

Si J., Cai R. (2021) Regulation on Digital Maps in China. *Zhong Lun*, 29 September. Available at: http://www.zhonglun.com/Content/2021/09-29/0938259959.html#:~:text=According%20to%20the%20Map%20Administration,number%EF%BC%88%E5%AE%A1%E5%9B%BE%E5%8F%B7%EF%BC%89 (accessed 7 September 2022).

The Personal Data Protection Bill (PDR Bill) (2019) Bill No 373 of 2019. Available at: https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf (accessed 7 September 2022).

United Nations Conference on Trade and Development (UNCTAD) (2021) Cross-Border Data Flows and Development: For Whom the Data Flow. Digital Economy Report 2021. Available at: https://unctad.org/system/files/official-document/der2021_en.pdf (accessed 7 September 2022).

Yang J. (2020) Bike Sharing in China: From Bicycle Graveyards to a Regulated Industry. *Georgetown Environmental Law Review*, 29 April. Available at: https://www.law.georgetown.edu/environmental-law-review/blog/bike-sharing-in-china-from-bicycle-graveyards-to-a-regulated-industry/ (accessed 7 September 2022).