Luca Belli *Editor*

CyberBRICS

Cybersecurity Regulations in the BRICS Countries

cyberBRICS

FGV DIREITO RIO

Springer

CyberBRICS

Luca Belli
Editor

CyberBRICS

Cybersecurity Regulations in the BRICS Countries

Springer

Editor
Luca Belli
Center for Technology and Society
FGV Rio de Janeiro Law School
Rio de Janeiro, Rio de Janeiro, Brazil

To learn more about CyberBRICS, visit www.cyberbrics.info.

The opinions expressed in this volume are the sole responsibility of the authors and do not represent the position of the institutions that support this publication.

ISBN 978-3-030-56404-9 ISBN 978-3-030-56405-6 (eBook)
https://doi.org/10.1007/978-3-030-56405-6

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2021
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface: Building Universally Accepted Norms, Standards and Practices

Steam was the protagonist of the first industrial revolution in the late eighteenth century. A century later, oil, electricity and assembly lines made mass production possible. In the 1970s, automation, computers and connected networks generated the third revolution. Today, the digital and the real mix inseparably. We are aligning artificial intelligence, IoT (Internet of Things), blockchain, 5G technology and digital analytics to drive real-world actions. It is the synergy between technological innovations and high scalability that leads to cost savings and facilitates access to new consumers.

While expanding, connectivity and the emergence of new information and communication technologies (ICTs) have created opportunities for individuals and businesses, they also present a number of challenges, particularly regarding personal data regulation and cybersecurity governance. The increase in the number of new Internet users in the BRICS countries has been remarkable over the last decade. The projection for the coming years is that the regions with the highest user growth will be in Latin America, Africa and Asia. The next billion users will probably come from the BRICS, along with the innovation and data they will produce and the policy they will need. This growth is pointed as one of the main causes of concern about cybersecurity due to the process of adaptation and learning of the population and local institutions, which could be vulnerable to cyber threats such as cyber terrorism, espionage, information sharing security, incident management, and cybercrimes of different natures, including economic.

In this context, the BRICS countries are increasing their cooperation in the fields of science and technology and promoting synergies in relation to digital policies. Attention to issues that specifically involve cybersecurity, sovereignty and global governance has been growing in the BRICS countries in recent years. These subjects, which had been treated marginally at the official BRICS summits, became prominent from 2013. It was during the 5th BRICS Summit (2013) in Durban, South Africa, that countries signed the eThekwini Declaration recognizing the urgency of cybersecurity:

> We recognize the critical positive role the Internet plays globally in promoting economic, social and cultural development. We believe it's important to contribute to and participate in a peaceful, secure, and open cyberspace and we emphasize that security in the use of Information and Communication Technologies (ICTs) through universally accepted norms, standards and practices is of paramount importance.

Since then, the debate has intensified, enlarging the scope of cybersecurity through cooperation, capacity building, research & development, criminalization and global governance. Under these circumstances, the BRICS member countries must especially join forces, as we are in an increasingly liquid world. This VUCA (volatility, uncertainty, complexity and ambiguity) world faces a new technological revolution and challenges such as increased protectionism, the danger of terrorism and cybersecurity issues.

It is important to understand that not only the technological evolution and the economic progress of the members, Brazil, Russia, India, China and South Africa, are at stake but also the security of the 3.2 billion people who live in the BRICS countries, whose lives are being radically transformed by the digital revolution. Some cybersecurity experts often use the following expression: There are only three types of users – those who have been hacked, those who will be hacked and those who are currently being hacked.

As such, the pillar-based CyberBRICS project of mapping existing regulations, identifying best practices and developing policy suggestions related to personal data protection and cybersecurity governance in BRICS is extremely adherent to the common challenges of block member countries. In addition, it is a vector to leverage digital transformation in developing common or – at least – compatible solutions. CyberBRICS plays a key role in providing answers to these challenges by providing valuable – and as yet non-existent – information about BRICS digital policies, based on rigorously collected evidence that can be used by researchers, regulators and companies.

This work, didactically structured in five dimensions – protection of personal data, consumer protection, cybercrime, protection of public order and cyberdefence – is a turning point and a great legacy as a way of what the BRICS must follow in this 4.0 world! The first and biggest challenge facing cybersecurity is raising awareness. This study connects directly with this gap; it examines and conveys what the real problems are. One of the most famous hackers in history, Kevin Mitnick, now one of the most respected cybersecurity professionals, has already said that a company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and other encryption technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted.

Minas Gerais, Brazil Sergio Suchodolski

Preface: Cybersecurity to Achieve the Goals of the 4th Industrial Revolution in BRICS

The advent of the Internet has brought about changes in the way that we communicate, how we interact in our private lives and the way we trade. The use of electronic mail (e-mail), a variety of mobile services enabled by plain old SMS (short message service), and social media platforms such as Facebook and Twitter as an integral part of our personal lives, and the use thereof by government and their respective agencies, could never be anticipated.

Data protection as a facet of the fundamental human right to privacy has become the subject matter of much legal debate in the last 15 years as its applicability to information and communication technologies is a key factor that cannot be ignored. The fact that we are constantly giving away personal information to service providers raises the question as to what really happens with such personal information, whether it has been stored securely and who exactly has access to it.

The receipt and collection of personal information by various stakeholders has resulted in the analysis of big data which can be used for purposes that are not suitable with the collection thereof. The CyberBRICS Project shows that BRICS countries are increasingly considering data privacy regulations and other digital policies as a tool to curb the power of foreign technology companies and reassert their sovereignty[1].

BRICS countries are all emerging economies that face common opportunities and challenges in cyberspace, which sets a solid strategic foundation for their cyber security cooperation. Representatives dealing with cyber security issues from Russia, South Africa, India and Brazil attended the seventh meeting of BRICS High Representatives for Security Issues in Beijing, China, in 2017 where the parties agreed that

[1] Luca Belli (18 November 2019) BRICS countries to build digital sovereignty in OpenDemocracy <*https://www.opendemocracy.net/en/hri-2/brics-countries-build-digital-sovereignty/*>.

> a common strategic intention to reform global cyberspace governance has set a solid strategic foundation for cyber security cooperation among the BRICS countries, the major challenges ahead call for further development of their agenda to help raise the voice of developing countries in the governance system[2].

The birth of cybercrime has created ample opportunities for criminals to exploit cyber security vulnerabilities which result in the unlawful use and abuse personal information as well as information held by private entities and the state. The Council of Europe Convention on Cybercrime, which South Africa signed in 2001, has been used as an international benchmark for drafting cybercrime legislation to outlaw breaching cyber security measures that prevent the unlawful access to personal information.

The Convention on Cybercrime criminalizes unauthorized access to data and communications which, in turn, must be construed as outlawing the access of personal information. It is against this background that BRICS countries must ensure that their cybercrime, data protection and cyber security laws are up to date with evolving technologies to effectively deal with cyber security breaches that may result in serious data violations and other cyber security threats.

Cyber-war and cyber-terrorism are new frontiers in modern-day warfare where the ordinary traditional rules of engagement may not be useful nor applicable. It has become imperative that BRICS states take steps to ensure that their legislative and policy frameworks are appropriate to also effectively deal with such threats, without unnecessarily infringing on individuals rights. While not an easy task, balancing the right to privacy with the interests of national security is imperative.

The editor and authors of this volume have been given a unique opportunity to do a comparative law and policy review of the global data protection, cyber security and cyber-crime as well as explore new legal concepts such as cyber defence and cyber warfare legislation in BRICS countries.

This publication contains up-to-date (2019) legal texts from diverse BRICS jurisdictions which are based upon their own constitutional and legal philosophical dispositions on privacy and state security in this digital age. These legal developments have brought about changes in the legal discourse relating to e-commerce, data protection, cyber security and cyber-crime legislation in the BRICS Countries over the last decade.

This book is an important and necessary study of relevant legislation and policy to ensure the BRICS goals and relating to 4th Industrial Revolution are achieved.

Pretoria, South Africa — Sizwe Lindelo Snail ka Mtuze

[2] Gao Wanglai (20 Jan 2010) BRICS Cybersecurity Cooperation: Achievements and Deepening Paths. in China International Studies. *<https://www.pressreader.com/china/china-international-studies-english/20180120/281513636564569>*.

Contents

About the Authors

Luca Belli, PhD is Professor of Internet Governance and Regulation at Fundação Getulio Vargas (FGV) Law School, where he also head the CyberBRICS project, and Associated Researcher at the Centre de Droit Public Comparé of Université Paris 2 Panthéon-Assas. Luca is also member of the Board of the Alliance for Affordable Internet (A4AI) and member of the Programming Committee of the Computers, Privacy and Data Protection Conferences (CPDP). Before joining FGV, Luca worked as an agent for the Council of Europe (CoE) Internet Governance Unit and served as a Network Neutrality Expert for the CoE. Over the past decade, he has coordinated several research projects dedicated to digital policy and Internet governance, producing research outputs in English, French, Italian, Portuguese and Spanish, amongst them are *De la gouvernance à la régulation de l'Internet* (Berger-Levrault 2016); *Net Neutrality Compendium* (Springer 2016); *Community Networks: the Internet by the People, for the People* and *Platform Regulations: How Platforms are Regulated and How They Regulate Us* (FGV 2017); *The Community Network Manual* (FGV-ITU-ISOC 2018); and *Governança e Regulações da Internet na América Latina* (FGV 2019). Luca has been consulted by various international organizations and national regulators, including the International Telecommunications Union, the Secretariat of the Internet Governance Forum, the Internet Society and the French Telecoms Regulators. His works have been quoted by the Organization of American States Report on Freedom of Expression and the Internet (2013), used by the CoE to elaborate the Recommendation of the Committee of Ministers on Network Neutrality (2016), featured in the French Telecoms Regulator (ARCEP) Report on the State of the Internet (2018), quoted by the Brazilian Telecoms Regulator (ANATEL) to define Community Networks (2020), and published or quoted by various media outlets, including The Economist, Le Monde, BBC, The Hill, China Today, O Globo, El Pais and La Stampa.

Min Jiang, PhD, is Associate Professor of Communication at UNC Charlotte and the 2019 CyberBRICS China Fellow at FGV Law School in Rio de Janeiro, Brazil. She is a Secretariat Member of the annual international Chinese Internet Research Conference (CIRC) and Associate Editor at Sage journal Communication & The

Public. Her research focuses on Chinese Internet technologies (search engine, social media, big data), politics (digital activism, online political satire, diplomacy), business (Chinese Internet giants, business ethics) and policies (real-name registration, privacy). She has co-edited 3 special journal issues and published over 30 journal articles and book chapters on the Chinese Internet, some of which have appeared in *Journal of Communication*, *New Media & Society*, *Information, Communication & Society*, *International Journal of Communication*, *International Communication Gazette*, and *Policy & Internet*. Media outlets including Reuters, Deutsche Welle, Foreign Policy, Financial Times, The New Scientist, The Chronicle of Higher Education and Al Jazeera English have interviewed her for her work. She was born and raised in China. Prior to pursuing her doctor's degree in the USA, she worked at China Central Television (CCTV) and Kill Bill I in her native country China. Dr Jiang received her bachelor's and master's degrees from Beijing Foreign Studies University and her PhD in Communication from Purdue University.

Anja Kovacs, PhD, directs the Internet Democracy Project in Delhi, India. The project works towards realizing feminist visions of the digital in society, by exploring and addressing power imbalances in the areas of norms, governance and infrastructure in India and beyond. Anja's research and advocacy currently focuses on questions regarding data governance, surveillance and cybersecurity as well as freedom of expression. This includes work on gender, bodies, surveillance, and dataveillance and gender and online abuse. She has also conducted extensive research on the architecture of Internet governance. Anja has been a member of the Investment Committee of the Digital Defenders Partnership and of the Steering Committee of Best Bits, a global network of civil society members, and is currently a member of the Board of Governors of Veres One. She has worked as an international consultant on Internet issues, for the Independent Commission on Multilateralism, the United Nations Development Programme Asia Pacific, and the UN Special Rapporteur on Freedom of Expression Mr. Frank La Rue, and has been a Fellow at the Centre for Internet and Society in Bangalore, India, and the 2019 CyberBRICS India Fellow at the Fundação Getulio Vargas (FGV) in Rio de Janeiro, Brazil. Prior to focusing her work on the information society, Anja researched and consulted on a wide range of development-related issues. She has lectured at the University of East Anglia, Norwich, UK, and Ambedkar University, Delhi, India, as well as guest lectured at universities in India and Brazil and has conducted extensive fieldwork throughout South Asia. She obtained her PhD in Development Studies from the University of East Anglia in the UK.

Sagwadi Mabunda is a PhD Candidate at the University of the Western Cape. Her doctoral thesis investigates the legislative responses of cybercrime by analysing and critiquing the South African Cybercrimes Bill. She is a prolific speaker who has presented papers in numerous conferences both in South Africa and internationally (Italy, Germany, Namibia and Botswana). She has published a number of papers on her research interests, which include cybercrime and economic crimes, such as International Anti-Money Laundering Law and International Anti-Corruption Law.

She has also successfully organized the first annual Economic Crime and Cybercrime Conference (ECCC) hosted at the University of the Western Cape in collaboration with the *Journal of Anti-Corruption Law* (JACL). Sagwadi has appeared as a guest lecturer at the University of the Western Cape, Cape Town and FGV Law School in Rio de Janeiro, Brazil, on topics on the relationship between law and cybersecurity. She is currently working at the South African Constitutional Court as a Law Researcher, firstly to retired Justice Edwin Cameron, then to the Chief Justice Mogoeng Mogeong, and currently to Acting Justice Margaret Victor. In 2018, aged 25, Sagwadi was honoured as one of the Mail & Guardian 200 Young South Africans.

Daniel Oppermann, PhD, is a Research Coordinator at the NUPRI Research Centre for International Relations, University of São Paulo (NUPRI-USP), and a Postdoctoral Researcher and Lecturer at the Fluminense Federal University in Niterói (UFF). In 2019, he was a Research Fellow at the FGV Law School CyberBRICS project. Daniel is a Researcher in the Pró-Defesa IV Program of the Brazilian Ministry of Defence and the public research foundation CAPES. His research is focused on different aspects of Internet governance and cybersecurity. In 2018, Daniel edited the book *Internet Governance in the Global South – History, Theory and Contemporary Debates* published by the University of São Paulo. Daniel studied Political Science at the Free University of Berlin and holds a PhD in International Relations from the University of Brasília (UnB). He was a Researcher at the OPSA Research Centre for South American Politics at the State University of Rio de Janeiro (UERJ), a Postdoctoral Researcher at the Institute of Economy of the Federal University of Rio de Janeiro (UFRJ), a Postdoctoral Researcher at the School of Command and General Staff of the Army (ECEME) in Rio de Janeiro, and a Guest Lecturer at the University of Los Andes in Bogotá, Colombia. As Chair of the Program Committee of the Global Internet Governance Academic Network (GigaNet), he coordinated the annual GigaNet Symposia in Brazil (2015) and Mexico (2016). Daniel has lectured on Internet governance, cybersecurity, geopolitics and data protection at the Federal University of Rio de Janeiro, at the DiGI School on Internet Governance (San Andrés University Buenos Aires) and at FGV Law School.

Andrey Shcherbovich, PhD, graduated from the National Research University, Higher School of Economics, Faculty of Law (Department of International Law) in 2008. He completed his postgraduate studies at the National Research University, Higher School of Economics (Moscow, Russia), Faculty of Law (Department of Constitutional and Municipal Law) in 2011. From 2008 to 2010, he was affiliated to the Non-Governmental Organization 'Inter-regional Library Cooperation Centre' as a Project Coordinator, a working body of the UNESCO Information for All Programme. From 2011 onwards, he has been Associate Professor at the National Research University, Higher School of Economics, Faculty of Law (Department of Constitutional and Municipal Law). From February to July 2019, he was a CyberBRICS Research Fellow at the Getulio Vargas Foundation Law School, Rio de Janeiro, Brazil.

Sizwe Lindelo Snail ka Mtuze is Commissioner at the Information Regulator of South Africa and holds a Baccalareus Legum (LLB) from the University of Pretoria with Tax Law and Cyber-Law electives and also a Master's Degree (LLM) in Information Technology Law from the University of South Africa. Mr. Snail is Member of the CyberBRICS Advisory Board. He is a practising attorney with the law firm Snail Attorneys at Law and International Co-ordinator of the African Centre for Cyberlaw and Crime Prevention based in Kampala, Uganda. He is the author of various articles on cyberlaw in accredited and non-accredited journals both locally and internationally and has given ad hoc lectures for the LSSA, ACFE, University of Johannesburg, Fort Hare University and University of Pretoria and comments on cyberlaw in various South African newspapers and radio talk shows. He also presents papers and attends both local and international conferences. He is also co-editor and author of the 3rd Edition of *Cyberlaw @ SA*. Mr. Snail was a member of the ICT REVIEW Panel in the Department of Telecommunications & Postal Services (DTPS), serving as a Chair of the E-commerce Committee (Digital Society as renamed) within the panel sub-committees. S Mr. Snail also currently serves on the National Cyber Security Advisory Counsel of the DPTS.

Sergio Gusmão Suchodolski is the President of the Development Bank of Minas Gerais (BDMG), Brazil. Previously he was Director General, Strategy and Partnerships, at the New Development Bank, in Shanghai, China. Mr. Suchodolski is Member of the CyberBRICS Advisory Board. He has served as Chief of Staff at BNDES – the Brazilian Development Bank. Prior to that, Mr. Suchodolski was Vice President for Corporate Development at Arlon Capital Partners, a New York based Global Private Equity Firm focused in food and agriculture investments. He holds a Master's of Laws Degree (LLM) from Harvard Law School, a Diplome (MA) from the Institut d'Etudes Politiques de Paris – Sciences-Po (Major in International Trade) and an LLB from the University of Sao Paulo Law School. Formerly, Mr. Suchodolski also held the positions of Special Advisor and Chief Foreign Policy Advisor at the Secretariat of Strategic Affairs, under the Office of the President of Brazil.

Chapter 1
CyberBRICS: A Multidimensional Approach to Cybersecurity for the BRICS

Luca Belli

This book stems from the CyberBRICS project,[1] which is the first initiative to develop a comparative analysis of the digital policies developed by BRICS (Brazil, Russia, India, China and South Africa) countries. BRICS have been chosen as a focus not only because their digital policies are affecting more than 40% of the global population – i.e. roughly 3.2 billion individuals living in such countries – but also all the individuals and businesses willing to use technologies developed in the BRICS or trading digital goods and services with these countries.

Digital policies and institutions elaborated and implemented by the BRICS are particularly interesting considering that such countries are already home to almost 40% of existing Internet users,[2] who are both the producers of large amounts of personal data, frequently referred to as "the new oil[3]", "the new currency of the

[1] The author thanks wholeheartedly the entire CyberBRICS team for their excellent work. The author would like to especially acknowledge the very useful feedback received from Dr. Min Jiang and Mr. Walter Britto as well as the tremendous editorial work of Mr. Luã Fergus, Ms. Laila Lorenzon, Ms. Carolina Telles and, once again, Mr. Walter Britto. The author expresses sincere gratitude for their friendship, feedback and very constructive comments, all along the development of the CyberBRICS project, to Dr. Ivar Hartmann, Ms. Hannah Draper, Dr. Ian Brown, Dr. Alison Gillwald, Dr. Marcelo Thompson, Ms. Elonnai Hickok, Mr. Sunil Abraham, Dr. Enrico Calandro, Ms. Anri van der Spuy, Dr. Alexey Ivanov, Dr. Shen Yi, Mr. Sergio Suchodolski, Mr. Sizwe Snail, Dr. Nicolo Zingales, Dr. Danilo Doneda and Mr. Bruno Ramos. The CyberBRICS project is an incredible collective effort, hosted by Fundação Getulio Vargas (FGV) Law School and developed in partnership with the Higher School of Economics, in Moscow, Russia; the Centre for Internet and Society, New Delhi, India; the Fudan University, Shanghai, China; and the University of Cape Town, Cape Town, South Africa. For further information, see <https://cyberbrics.info/>

[2] See <http://www.internetlivestats.com/internet-users-by-country/>.

[3] The phrase was coined by the British mathematician Clive Humby, in 2006, and was subsequently made popular by the World Economic Forum 2011 report on personal data. See WEF (2011).

L. Belli (✉)
Center for Technology and Society, FGV Rio de Janeiro Law School, Rio de Janeiro, Brazil
e-mail: luca.belli@fgv.br

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2021

L. Belli (ed.), *CyberBRICS*, https://doi.org/10.1007/978-3-030-56405-6_1

digital world[4]" and "the world's most valuable resource[5]", as well as the potential developers and consumers of the technologies that will shape the evolution of the digital world.

Given the complexity of digital policies in general and cybersecurity in particular – not to mention the specificities of BRICS countries – this work aims at laying the foundation on which more research on cybersecurity and digital policy in the BRICS can and will be developed. To this end, the mapping exercise that this volume aims at conducting is truly fundamental, as it aims at laying the grounds upon which future comparative studies on BRICS digital policies can build and develop. It is indeed astonishing that, despite the relevance of BRICS countries in today's evolving geopolitics, the weight of their digital economies and the influence of their digital policies, no comprehensive comparative study of the BRICS digital policies exists to date.

This work is of particular importance, not only for researchers, digital policymakers, Internet users[6] and businesses, but for the BRICS themselves, considering that these countries are facing a twofold "digital paradox[7]". The expansion and cost reduction of connectivity allow governments and businesses to offer a wide range of services, more efficiently than ever before, creating incredible social and economic opportunities through digital technologies. Yet, at the same time, such technologies enable cyberthreats, cybercrimes and cyberattacks[8] that limit the benefits promised by digital technologies and create a wide range of negative externalities that must be addressed by sound policies and regulations.

Furthermore, while recognising that digital technologies bring both significant benefits and serious threats, public bodies and businesses in the BRICS are only beginning to implement – and in some cases are still elaborating – their digitalisation and cybersecurity strategies. The fact that strategies, regulations and institutions aimed at framing digital technologies in the BRICS have been – and are being – developed only very recently, and their impact is so potentially wide, provides an incredible opportunity for novel research in an incredibly stimulating area.

In this spirit, this volume represents the first important effort to systematise and analyse BRICS digital policies. This seminal CyberBRICS publication will focus on cybersecurity, while future research will explore two areas that are intimately intertwined with cybersecurity and are essential for the evolution of BRICS countries: connectivity policies and strategies for digitalisation of public administrations. This first work will provide an initial mapping, necessary to understand the

[4] See Kuneva (2009).

[5] See *The Economist* (2017).

[6] The term Internet user is utilised in this in its double nature of prosumer, i.e. both producer and consumer of digital products and services. See Belli (2017:98).

[7] This concept has gained particular relevance at the South African level, as highlighted by Sagwadi Mabunda's analysis in Chap. 10 of this volume. See also Department of Telecommunications and Postal Services, South Africa (2017).

[8] See, for instance, Vaidya (2015); Department of Telecommunications and Postal Services, South Africa (2017); Gemalto (2018).

state of play of BRICS digital policies and compare them, thus laying the foundations on which BRICS can build the future of digital policy research. The main goal of this volume is, therefore, to provide an understanding of how cybersecurity is conceptualised and structured in the BRICS, mapping the normative frameworks that regulate the various dimensions of cybersecurity in the BRICS and the institutions that implement these normative frameworks.

1.1 From BRICS to CyberBRICS: A Case of Enhanced Cooperation

When the Goldman Sachs economist Jim O'Neill coined the expression BRICs[9] in 2001 – without the capital "S", as South Africa would join only at a later stage[10] – the acronym simply aimed at identifying Brazil, Russia, India and China in the context of an economic forecast. Yet, the BRICs - that evolved into BRICS, with the inclusion of South Africa - seized the occasion to start debating how a "Post-Western World"[11] might look like, established dedicated diplomatic channels, promoted increasing synergies and coordination through dedicated working groups and partnerships in a wide range of diverse fields, culminating their joint aspirations with the creation of a joint institution, the New Development Bank, as well as the BRICS Contingent Reserve Agreement (CRA) in 2014.

Almost a decade in the making, BRICS are no longer a mere acronym but have become a reality with progressively more intense relationships, a shared institution and a continuously expanding agenda. Brazil, Russia, India, China and South Africa together represent over 40% of the world population, being home to 3.2 billion individuals, while generating 23% of the global GDP and 18% of the global trade. In addition to the presidential meetings, arranged through an annual summit and the informal meeting in the margins of the G20, the rotating presidency of the BRICS organises nearly 100 official meetings every year, including approximately 15 ministerial meetings and dozens of gatherings of senior officials, discussing a wide spectrum of issues well beyond the original economic cooperation, such as digital technologies, climate change, cultural cooperation, education and many more.[12]

[9] See O'Neill (2001).

[10] The inclusion of South Africa in the group can be largely explained by the existence of the India-Brazil-South Africa Dialogue Forum or IBSA Trilateral, established in June 2003, as a mechanism for permanent coordination between the countries. The creation of IBSA signalled the strong political will to establish a long-standing partnership, collaborating to "the construction of a new international architecture; bring their voice together on global issues; deepen their ties in various areas". See <http://www.ibsa-trilateral.org/background.html>.

[11] See Stuenkel (2016).

[12] See Brazilian Presidency of the BRICS (2019).

BRICS countries are increasing their cooperation[13] in the field of digital policy and, especially, cybersecurity, which are becoming global priorities. Indeed, while the expansion of connectivity and the rise of new information and communications technologies (ICTs) are generating opportunities for individuals and businesses, they also pose several challenges, with particular regard to cybersecurity governance in its various dimensions, which can be addressed through shared and efficient policies. Since the BRICS ministers for science, technology and innovation met for the first time in 2014, the BRICS have remarkably intensified discussions in their areas of common interest and have started defining cooperation and partnerships, while adopting a number of shared documents,[14] including the Memorandum of Understanding on Cooperation in Science, Technology and Innovation[15] to design the legal framework within which the various branches of their cooperation can develop and expand.

Since 2014, the discussion of digital matters amongst the five countries has acquired notable prominence, including the promotion of a BRICS Digital Partnership[16] in 2016, the dedication of the 2018 Declaration of the BRICS Presidential Summit to a Collaboration for Inclusive Growth and Shared Prosperity in the Fourth Industrial Revolution[17] and the elaboration of an Enabling Framework for the Innovation BRICS Network.[18] Through these efforts, BRICS leaders have explicitly emphasised "the importance of continuing BRICS scientific, technical, innovation and entrepreneurship cooperation."[19] In this sense, they have already established concrete initiatives, including in this sense, including the BRICS Partnership on New Industrial Revolution (PartNIR), the Innovation BRICS Network (iBRICS Network) and the BRICS Institute of Future Networks.[20]

BRICS's willingness to cooperate has recently shifted to the realm of digital policies, norms and standards as highlighted by the Xiamen Declaration, issued after the Ninth BRICS Summit in 2017, according to which the countries committed to jointly "advocate the establishment of internationally applicable rules for security of ICT infrastructure, data protection and the Internet".[21] In this spirit and with the aim to foster research collaboration and promote synergy regarding technology and policy development, BRICS have recently adopted a new BRICS Science, Technology and Innovation Work Plan 2019–2022[22] and established a new BRICS

[13] See BRICS (14 August 2019).

[14] For an analysis of such documents and their impact, see Kiselev and Nechaeva (2018).

[15] 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).

[16] See BRICS Working Group on ICT Cooperation (11 November 2016).

[17] See BRICS (2018).

[18] See BRICS STIEP WG (May 2019).

[19] See Itamaraty (27 June 2019).

[20] Idem.

[21] See BRICS (2017).

[22] See BRICS (October 2019).

Science, Technology and Innovation (STI) cooperation mechanism called BRICS STI Architecture, 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 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 on society
- Ensuring wide and effective dissemination of information about BRICS STI activities amongst different stakeholders including policymakers, scientists, research organisations and a wider audience[23]

It should be noted that BRICS countries have been chosen not only for their size and increasing economic and geopolitical relevance but also because, over the next decade, Internet growth is expected to occur massively in these countries, particularly in India, China and Brazil.[24] Hence, the technology, policy and governance arrangements defined by BRICS are likely to impact not only the 3.2 billion people that inhabit such countries but also the individuals and businesses that will choose to utilise increasing popular applications and services, as well as connected devices and networking equipment developed within BRICS countries based on BRICS standards.

The joint development of the BRICS Institutes of Future Networks, the BRICS Technology Transfer Cooperation and an Enabling Framework for the Innovation BRICS Network[25] concretely signal the group's willingness to enhance technological cooperation with particular regard to digital matters. Furthermore, the creation of both the first BRICS Technology Transfer Centre and the first BRICS Institute of Future Networks in China, respectively, in Kunming[26] and Shenzhen,[27] denotes the strong Chinese interest, proactiveness and financial commitment to promote and strengthen BRICS technological cooperation.

On the one hand, these evolutions highlight the mounting relevance[28] of and reliance on digital technology and digital economy for the BRICS and the pressing need for structured analyses on how such countries are addressing the challenges of digitality. On the other hand, the initiatives exposed above clearly demonstrate that BRICS can be considered as a telling example of what, in Internet governance parlance, is deemed as "enhanced cooperation".[29] While the lack of a formal definition

[23] See BRICS (September 2019).

[24] Three BRICS countries, i.e. China, India and Brazil, are the most populated countries of the regions where Internet growth is expected to be the most relevant. See Cisco (2017).

[25] See BRICS STIEP WG (May 2019).

[26] See Kunming (11 September 2019).

[27] The first Institute has been established in Shenzhen, China, in August 2019. See XinhuaNet (2019).

[28] See, for instance, Banga and Jeet Singh (2019); BRICS Competition Centre (2019).

[29] See Belli (2016:347–358).

does not allow to officially labelling specific processes as enhanced cooperation, "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"[30] was explicitly recognised by Article 69 of the Tunis Agenda for the Information Society, endorsed by the General Assembly of the United Nations in its Resolution 60/252.

The ample range of BRICS initiatives to improve their cooperation on digital matters represents a noticeable example of how enhanced cooperation can work in practice. Indeed, the past decade has witnessed the construction of a stable process enabling the development of productive discussions about digital policy priorities and the gradual elaboration of mechanisms and solutions through which enhanced cooperation on those issues might be pursued.

1.2 Why Focus on Cybersecurity?

The reason why cybersecurity has been chosen as the first broad theme to be analysed by the CyberBRICS project is that this topic has become a general concern for literally everyone in BRICS as well as non-BRICS countries alike. All citizens, businesses, public administrations, education institutions and decision-makers must address cybersecurity in its various dimensions before some major risks and threats become reality. To borrow a very suited metaphor, cybersecurity is like "turbo-charged climate-change".[31] It is an issue affecting everyone and everything, although few realise its importance, and even fewer have a plan to address its challenges. Most start developing cybersecurity plans only after major accidents, substantial losses or disruptions. Critically, exactly like climate change, the only way to address cybersecurity efficiently and effectively is through cooperation involving all affected stakeholders.[32]

Cybersecurity was a largely ignored concept by the general public until the former National Security Agency (NSA) contractor Edward Snowden exposed the massive hacking and surveillance schemes by NSA and brought cybersecurity

[30] See paragraph 69 of the Tunis Agenda for the Information Society (18 November 2005). WSIS-05/TUNIS/DOC/6(Rev. 1)-E. <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>.

[31] I thank my friend Henrique Paiva for sharing this metaphor during his presentation at the CyberBRICS event on 5G and New Digital Infrastructures in the BRICS, held at FGV Law School on 30 August 2019. See <https://cyberbrics.info/event-5g-and-new-digital-infrastructures-in-the-brics/>.

[32] Formal agreement on the necessity to adopt a multistakeholder model to properly address cybersecurity has already emerged since the World Summit on the Information Society, culminating in the adoption of the Tunis Agenda, whose paragraph 39 states that UN members "reaffirm the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of cybersecurity, as outlined in UNGA Resolution 57/239 and other relevant regional frameworks". See Tunis Agenda for the Information Society (18 November 2005). WSIS-05/TUNIS/DOC/6(Rev. 1)-E. <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>.

issues that were previously reserved to a niche of specialists to the mainstream. Over the past few years, a number of institutions have recognised, as pointed out by the United Nations General Assembly, cybersecurity "is an increasingly important theme in international policy concerned with the digital economy and other aspects of the Information Society" primarily due to the fact "[t]here has been a growing incidence of serious cybersecurity attacks, some of which have had significant impacts on individuals and public services".[33]

To date, cybersecurity still is not a universally defined notion, and its various dimensions and implications are largely ignored by the general public. Worryingly, such situation exists despite frequent cyberattacks, publicly disclosed data breaches[34] – which, under some regulatory frameworks,[35] are now mandatory – and the juridical disputes between national governments and large companies, for a variety of cybersecurity-related issues, spanning from the usage of encryption techniques[36] to transnational flows of personal data[37] or the security of 5G networking equipment.[38]

As an important premise of this work, it must be clarified that the notion of cybersecurity is a very elastic[39] one and may lead to deeply different interpretations, depending on the context. Several authors have explored how different approaches to cybersecurity are constructed, highlighting the existence of complementary but

[33] UNGA (2018:4).

[34] According to the cybersecurity analysis firm Gemalto, during the first 6 months of 2018, "almost 1 billion records were compromised" only considering the breach incident of Indian digital identify programme Aadhaar, including the leak of Indian citizen names, addresses and a wide range of other personally identified information. See, for instance, Gemalto (2018).

[35] Article 33 of the General Data Protection Regulation that entered in force in the European Union in May 2018 determines that personal data breach incidents must be notified to the supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it". This norm, by itself, is at the origin of a much greater awareness of the number of breaches occurring on a daily basis. This provision has also directly inspired the drafters of the Brazilian General Data Protection Legislation that, in its Article 48 foresees – in a less constringent tone than the EU Regulation – that "data breach notifications must occur within a reasonable time, to be defined by the national authority".

[36] See, for instance, Ewing (2016); Kolomychenko (2018).

[37] See, for instance, the reasoning of the Court of Justice of the European Union declaring that the EU Commission's US Safe Harbour Decision is invalid, stressing that "the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country". Case C-362/14. Maximillian Schrems v Data Protection Commissioner. Press Release No 117/15. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>.

[38] See, for instance, Sevastopulo and Bond (2019).

[39] Since the World Summit on the Information Society, cybersecurity has been considered as an overarching concept encompassing a wide range of items and practices, including information sharing of national and regional approaches, good practices and guidelines; development of warning and incident response capabilities; establishment of suitable technical standards and industry solutions; harmonisation of national legal approaches and establishment of international legal coordination; definition of sound privacy, data and consumer protection systems; and promotion of cybersecurity capacity building. See ITU (2005).

frequently diverging perspectives and stressing that cybersecurity definitions often crystallise around specific issues, threats, activities and aspects.[40] The Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) provides a useful and overarching definition of cybersecurity, which is noteworthy for being a rare example of consensual cybersecurity definition at the international level, stating that:

> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.[41]

The amplitude provided by the above definition explains the need to have a more focused approach to define the boundaries for the discussions developed in this book. In this regard, the book concentrates on national frameworks defined and implemented by BRICS public bodies and purposely avoids exploring business practices, technical tools and assurances and a potentially infinite list of diverse topics.

In this context, this volume starts from the premise that five key dimensions of cybersecurity can be identified as fundamental pillars that will orient our analysis. Such policy and governance dimensions will be presented in five chapters dedicated to each BRICS country and, subsequently, mapped in five country reports, which are annexed to the chapters. Notably, the focus of our analysis will move from micro to macro, starting from data protection and then shifting to consumer protection, cybercrime, the preservation of public order and cyberdefence.[42] These five dimensions have been chosen as the core avenues of our methodology. The goal of this publication is, therefore, to explore, map and present them so that, based on this work, a comparative approach can be developed.

This first chapter will introduce the volume, delimiting the concepts and issue areas that will be used in the country analyses while trying to identify general trends across BRICS countries. This chapter will be followed by five country-specific analyses, where the cybersecurity dimensions of each BRICS country are presented and subsequently analysed in detail, by five country reports providing valuable

[40] For a recent and well-structure overview, see Fichtner (2018), discussing four approaches to cybersecurity, based on data protection, safeguards of financial interests, protection of public and political infrastructures and control of information and communication flows. For an analysis of different conceptualisations of cybersecurity, see also Wolff (2016).

[41] See ITU-T (2009).

[42] The authors acknowledge that telecoms regulation and capacity building programmes are also two further dimensions that need to be explored, to have a complete picture of cybersecurity policy frameworks. However, these dimensions are not analysed in this volume, as they will be explored within the 2020–2021 CyberBRICS workflow, dedicated to Internet access policies and the digitalisation of public administrations in the BRICS.

insight on the various elements composing the cybersecurity frameworks of the BRICS.

To understand the relevance of BRICS digital policies in general and of this work in particular, the following section will provide an introduction to briefly explore the five cybersecurity dimensions mentioned above. Such presentation is instrumental in understanding the methodology used in this book and to taking the first step necessary to realise that BRICS are rapidly transitioning into CyberBRICS.

1.3 Cybersecurity Dimensions

Cybersecurity is a major concern for BRICS countries and beyond. States and their interconnected infrastructures – more recently dubbed as "smart" – may be potential targets, especially in the case of critical infrastructures that can become vulnerable when interconnected.[43] Cyberattacks can also put companies – from micro-enterprises to major players – at high risk. Further individual users are constantly lured into new connected services and devices with very little knowledge of the risks they face by increasingly exposing their lives to data collection with no precautions against potentially harms spanning from the abusive collection and usage of their personal data to a wide range of cybercrimes and cyberattacks.

While our awareness, preparation and protection levels are still largely inadequate, in BRICS as well as non-BRICS countries alike, the cybersecurity dimensions we analyse in the volume are increasingly – though still insufficiently – appreciated by various stakeholders who seem to be demanding and driving change. As the chapters and country reports dedicated to each specific BRICS country will highlight in this volume, several elements within the cybersecurity dimensions we identified are converging, and BRICS countries are increasingly adopting similar solutions to cope with shared challenges. On the one hand, such tendency towards compatible digital polices is largely due to the fact that digital technologies are distributed and utilised globally and therefore present global challenges to which all countries, including BRICS, are called upon elaborating efficient responses. On the other hand, BRICS may end up elaborating very similar digital policy and governance mechanisms as they not only influence each other in their elaboration phase,[44] but they may utilise similar

[43] As an instance, in June 2019, the United States were reportedly "stepping up digital incursions into Russia's electric power grid in a warning to President Vladimir V. Putin and a demonstration of how the Trump administration is using new authorities to deploy cybertools more aggressively". According to the *New York Times*, "current and former [US] government officials described the previously unreported deployment of American computer code inside Russia's grid" by the United States Cyber Command, the arm of the Pentagon that runs the military's offensive and defensive operations in the online world. See Sanger and Perlroth (2019).

[44] As an instance, BRICS countries jointly agreed during the Ninth BRICS Summit, in 2017, to jointly advocate for data protection and, after the 2017 Xiamen Declaration, all BRICS adopted or updated their data protection regimes.

models as sources of inspiration, especially when they do not have an existing policy in place to regulate specific digital issues.

The convergence of BRICS digital policies is illustrated, for instance, by the national data protection frameworks in the BRICS countries, which are becoming increasingly compatible on many fronts. This phenomenon is not due to any existing BRICS binding agreement on the matter. On the contrary, since the Xiamen Declaration, BRICS countries have expressed their willingness to jointly enhance their cooperation towards the definition of shared data protection norms[45] and, at the same time, they have considered the most comprehensive data protection frameworks that already exist – notably, the European Union's General Data Protection Regulation (GDPR) and the Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, best known as Convention 108 – as a reference to shape their own national frameworks. The consideration of the same source of reference and the simultaneous recognition of the importance of data protection frameworks are therefore producing an interesting harmonisation process.

This section provides an overview of the cybersecurity dimensions analysed in the volume and the methodology utilised to identify key elements of such dimensions as well as of the main BRICS tendencies that can be identified. We hope this first step in BRICS digital policy analysis can kick-start a much wider, deeper and articulated effort, shedding light on a wide range of digital policy issues which are essential for the evolution of digitality in the BRICS countries and beyond.

1.4 Data Protection

Although much has yet to be accomplished in terms of affordability and availability of Internet access in BRICS countries, the past decade has witnessed an incredible increase not only in fixed Internet access – in some cases, due to massive public investments in network infrastructure[46] – but also in mobile coverage. This tendency together with the simultaneous adoption of smartphones and creation of systems of connected devices – in the context of the so-called Internet of Things (IoT) – allows for ubiquitous and permanent data collection, bringing important benefits[47] but also relevant risks.

[45] See BRICS (2017).

[46] In China, significant government-led and policy-promoted investments in infrastructure are commonly acknowledged amongst the main driving forces that propelled the remarkable Internet growth undertaken by the country. See, for example, Boston Consulting Group (2017). A deeper analysis into the BRICS frameworks related to Internet access will be undertaken by the CyberBRICS project starting from 2020.

[47] The expansion of connectivity as well as the advancement of the IoT can trigger an ample range of benefits, spanning from increased access to education, information and knowledge to gains in

In fact, the growing adoption of and reliance on digital services and devices increases significantly the potential for data collection and processing. Particularly, China, India, Brazil and Russia are, together with the United States, the countries currently having the most smartphone users in the world.[48] On the one hand, these evolutions have enormously increased the opportunities for data collection and exposed the potential that data, notably personal data, have in order to generate knowledge and value. On the other hand, they have also revealed that personal data should be considered as a key strategic resource whereas the lack of strong data protection frameworks, including effective implementation, may allow for an ample range of misbehaviours, spanning from privacy violation to interference in national governance. In this perspective, the lack of protection and security obligations regarding the collection and processing of personal data may have detrimental consequences not only for individuals but also for national economies, security and democracy.

Since the adoption of the Tunis Agenda for the Information Society (2005), during the second phase of the World Summit on the Information Society, UN member states have agreed that cybersecurity "culture requires national action and increased international cooperation to strengthen security while enhancing the protection of personal information, privacy and data[49]".

Data protection has therefore turned into an essential policy priority for BRICS countries as it is the central element of cybersecurity policy allowing to effectively regulate the security of personal information. Information security is commonly referred to as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.[50] The analysis of BRICS data protection frameworks has therefore been considered as the first essential step to understand the complete picture of cybersecurity in the BRICS. While it must be acknowledged that a complete study of data protection requires the consideration of its legal, economic and sociological dimensions, the analysis developed in the various country reports featured in this book will only focus on the regulatory aspects of data protection in the BRICS. This is an explicit choice aimed at narrowing the focus to a specific aspect that can be more easily mapped and, subsequently, compared.

Aware of the fundamental importance of data protection for their economies, security and even sovereignty, all BRICS countries have recently established or updated their data protection frameworks and legislation. Major recent changes include:

---

productivity, improved citizen participation, but also smoother transportations, more reliable electricity and cleaner environments. See, for example, World Bank (2016) and ITU (2016).

[48] These BRICS countries are respectively first, second, fourth and fifth nation with most smartphone users in the world. See Statista (2019).

[49] See Tunis Agenda, paragraph 39.

[50] This definition was originally proposed by the National Institute of Standards and Technology. See NIST (2003).

- The adoption of a new Brazilian General Data Protection Law and the final approval of the establishment of a new Data Protection Authority[51]
- The update of the Russian Data Protection Legislation, including data localisation provisions[52]
- The recognition of privacy as a fundamental right by the Indian Supreme Court and the ongoing elaboration of a new Data Protection Bill[53]
- 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 Personal Information Security Specification[54]
- The creation of a Data Protection Regulator in South Africa and the upcoming enactment of the Protection of Personal Information Act[55]

The above-mentioned legislations present various similarities, such as the shared set of data subject rights and data protection principles. This is primarily due to the fact all BRICS countries considered European data protection as a reference to shape their national frameworks, either because they are directly affected – such as Russia, as a member of the Council of Europe – or because regulation compatible with European standards is increasingly essential to facilitate the free flow of information in digital economy. However, BRICS data protection frameworks also present many differences amongst each other and when compared to the European framework. A clear example is the Chinese Personal Information Security Specification that stands out of the BRICS data protection frameworks for being a non-binding document,[56] given that it specifies the more comprehensive – and binding – cybersecurity law. Interestingly, while it could be criticised for its limited force, the Specification includes a noteworthy "Privacy Policy Template" providing a concrete blueprint for companies to meet data protection standards, revealing a different cultural approach based on "guiding by example".

The Chinese regulatory approach is fascinating as it differs from traditional regulatory techniques based on the elaboration of a regulation and the creation of a regulator. Differently, the Chinese approach strives to orient organisations' behaviours by providing a model that allows the regulated entity to understand how to ideally comply, rather than delegating the regulatory task to the sole existence of data protection regulation and regulator. The Chinese seem to acknowledge that regulation includes a wide range of complicated provisions which may be very challenging to understand, comply with and enforce. Furthermore, this approach should be considered in conjunction with the recent announcement that the Chinese government will create a new National "Internet + Monitoring" System also called "China's

[51] See Sect. 2.1 of the Brazilian Country Report, in Chap. 2.

[52] See Sect. 3.1 of the Russian Country Report, in Chap. 3.

[53] See Sect. 4.1 of the Indian Country Report, in Chap. 4.

[54] See Sect. 5.1 of the Chinese Country Report, in Chap. 5.

[55] See Sect. 6.1 of the South African Country Report, in Chap. 6.

[56] See Min Jiang's analysis in Chap. 8.

Corporate Social Credit System" to monitor how all companies comply with the law and raise sanctions for those who fail to comply or work with partners involved with fraudulent activities.[57]

The provision of concrete indications via a model, matched with a database listing all the entities that must comply with the regulation and, therefore, follow the provided model, as China is experimenting, opens the path to a different type of regulation based on concrete guidance to and effective monitoring of the entities to be regulated.[58] This may be an alternative option to be explored even beyond BRICS countries. Indeed, such an alternative regulatory approach may prove more effective than the traditional one, considering that a conspicuous number of digital businesses frequently disrespect data protection provisions, both in their business practices and their terms of service, despite the binding force of data protection regulation.[59] An alternative regulatory approach offering concrete guidance on how to properly frame business self-regulation, including guidance for data security, may be very useful to facilitate business compliance and avoid problems due to ignorance of the regulatory framework or lack of comprehension of proper implementation. In this sense, the study of BRICS solutions may be useful for BRICS and non-BRICS countries alike.

The adoption of data protection frameworks by all BRICS countries illustrates the double purpose of data protection regulations, which play an essential role in not only preserving individuals' capability to enjoy an ample spectrum of rights[60] – including privacy, self-determination and freedom of expression – but also promoting juridical certainty for businesses. Both rationales underpin data protection frameworks in BRICS countries, but their relevance may vary depending on the legal tradition of the specific country. As such, the emergence of a data protection culture in the BRICS stems from these two different but complementary visions of data protection as a body of law rooted in, on the one hand, the protection of individuals' rights and, on the other hand, the definition of clear rules fostering legal certainty for businesses and facilitating cross-border data flows. Importantly, in both perspectives, data protection plays an essential role as the main body of legislation fostering data security, not only as a principle but also through a concrete set of obligations and correspondent data subject rights.

As noted by UNCTAD, data protection is the body of law that defines the technical and organisational security measures that are indispensable to protect individuals against accidental loss, destruction of data and deliberate acts of misuse. It provides threefold protection for the interests of individual data subjects, the entity

[57] See European Union Chamber of Commerce in China (2019).

[58] This alternative regulatory technique will be the object of a future study.

[59] This phenomenon is particularly evident as regards terms of service of digital platforms. See Belli and Venturini (2016).

[60] In the BRICS context, this approach has been very vocally reasserted by the Supreme Court of India, in 2017, with the adoption of its landmark Puttaswamy Judgement, stating that "the Right to Privacy is an integral part of Right to Life and Personal Liberty guaranteed in Article 21 of the Constitution". See WP (C) 494 of 2012, Justice K.S. Puttaswamy (Retd) vs Union Of India.

processing the personal data and society at large.[61] Indeed, the existence of adequate personal data protection is essential not only for the cybersecurity of individuals but also for fostering trustworthy businesses environments and, by extension, national economies where risks are prevented and mitigated and responses to accidents and attacks are immediately enacted.

1.4.1 Data Protection Methodology

Questions for data protection methodology are grouped into five sub-dimensions: scope, definitions, rights, obligations and sanctions and actors. To facilitate a better understanding and comparison of BRICS data protection frameworks, we invite readers to carefully consult the list of questions that every data protection section of the country report explores.

Scope

1. What national laws (or other types of normative acts) regulate the collection and use of personal data?
2. Is the country a party of any international data protection agreement?
3. What data is regulated?
4. Are there any exemptions?
5. To whom do the laws apply?
6. Do the laws apply to foreign entities that do not have a physical presence in the country?

Definitions

7. How are personal data defined?
8. Are there special categories of personal data (e.g. sensitive data)?
9. How are the data controller and the data processor/operator defined?
10. What are the data protection principles and how are they defined?
11. Does the law provide any specific definitions with regard to data protection in the digital sphere?

Rights

12. Is the data protection law based on fundamental rights (defined in Constitutional law or International binding documents)?
13. What are the rights of the data subjects according to the law?

Obligations and Sanctions

14. What are the obligations of the controllers and processors/operators?

[61] See UNCTAD (2016).

15. Is notification to a national regulator or registration required before processing data?
16. Does the law require a privacy impact assessment to process any category of personal data?
17. What conditions must be met to ensure that personal data are processed lawfully?
18. What are the conditions for the expression of consent?
19. If the law foresees special categories of data, what are the conditions to ensure the lawfulness of processing of such data?
20. What are the security requirements for collecting and processing personal data?
21. Is there a requirement to store (certain types of) personal data inside the jurisdiction?
22. What are the requirements for transferring data outside the national jurisdiction?
23. Are data transfer agreements foreseen by the law?
24. Does the relevant national regulator need to approve the data transfer agreements?
25. What are the sanctions and remedies foreseen by the law for not complying with the obligations?

Actors

26. What actors are responsible for the implementation of the data protection law?
27. What is the administrative structure of actors responsible for the implementation of the data protection law (e.g. independent authority, executive agency, judiciary)?
28. What are the powers of the actors responsible for the implementation of the data protection law?

1.5 Consumer Protection

Frequent data breaches[62] stemming from an ample range of vulnerabilities as a result of widespread adoption of connected devices underline the need for data protection and consumer protection.

The rise of digital technologies in the BRICS and beyond has not only created entirely new markets and digital marketplaces but has also substantially changed the ways in which consumers interact and transact with (digital) good producers and service providers. Digital innovation has transformed both the nature of goods, services and commerce and the relations between consumers and producers/providers. Such a transformation is taking place at an impressive rate. In China, e-commerce represents already more than 35% of the country's retail sales, and the country's "Made in China 2025" strategy is planning to develop 95% of connected devices by

[62] See, for example, Gemalto (2018).

2025.[63] Indian e-commerce companies such as Snapdeal and Flipkart are already estimated to receive more than 70% of their orders via mobile phones.[64] The South African technology investor Naspers has invested billions in BRICS start-ups over the past decade, substantially contributing to the success of some BRICS "unicorns" such as the Chinese technology giant Tencent and the Brazilian fintech Nubank.[65]

In a context of increasing adoption of digital goods and services, consumer law frameworks are going to be essential to determine the degrees of security that individuals can expect when purchasing and utilising (digital) goods and services. Furthermore, one can argue that consumer law will be increasingly tested as e-commerce and the IoT evolve in a symbiotic fashion further reducing the distinction between a good producer and a service provider, as all "thing" increasingly collect and process data and may include the capability to provide services. For instance, smart home devices and appliances, besides acting as connected products automating domestic tasks, can also serve as portals to communication or e-commerce services (such as smart speakers and virtual assistants). The growing adoption of such devices raises the question of how to properly categorise the smart-home device supplier: a producer of connected objects or a supplier of digital services? This categorisation may have relevant consequences in terms of responsibility of the producer or provider, as it is evident in the Russian context, where free online services are used "at one's risk", as consumer protection applies only to services provided in exchange of a payment..[66]

The rise of the IoT is also a particularly relevant phenomenon, justifying the inclusion of consumer law as an essential cybersecurity dimension to be analysed in this book. Indeed, the IoT is increasingly multiplying the number of connected devices and the points of access for connected services while fostering new opportunities for interconnectivity between products and services. While this scenario can create many advantages for producers and consumers, it is also a growing cause for concern as any connected device represents a potential vulnerability that could be exploited by malevolent actors.[67]

Due to the number of already existing connected devices and their projected growth[68] in the context of the IoT, the risk for cyberattack has considerably increased, moving from the digital environment to the physical environment where an ample range of poorly secured[69] – or sometimes completely unsecured – devices are utilised by many users largely uninformed about cybersecurity. This proliferation of

[63] In this sense, see Min Jiang's analysis in Chap. 8.

[64] See Bond (2019).

[65] See <https://www.naspersreport2019.com/>.

[66] See Andrey Shcherbovich's analysis in Chap. 4.

[67] See Belli (2019).

[68] According to the consultancy Statista, the "total installed base of Internet of Things (IoT) connected devices is projected to amount to 75.44 billion worldwide by 2025, a fivefold increase in ten years". See <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>.

[69] See Mosenia and Jha (2016).