

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 cyber-crimes 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 eThekweni 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 sovereignty¹.

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 system².

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

²Gao 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

1	CyberBRICS: A Multidimensional Approach to Cybersecurity for the BRICS	1
	Luca Belli	
2	Dimensions of Cybersecurity in Brazil	35
	Daniel Oppermann	
3	Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the “Sovereignization” of the Internet in Russia	67
	Andrey Shcherbovich	
4	Cybersecurity and Data Protection Regulation in India: An Uneven Patchwork	133
	Anja Kovacs	
5	Cybersecurity Policies in China	183
	Min Jiang	
6	Cybersecurity in South Africa: Towards Best Practices	227
	Sagwadi Mabunda	
7	BRICS Countries to Build Digital Sovereignty	271
	Luca Belli	

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 Mogoeng, 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.