CyberBRICS:

Cybersecurity Regulations in the BRICS Countries

Luca Belli, Editor

Prefaces by *Sergio Suchodolski* and *Sizwe Snail*

This draft may contain typos and imprecise, incomplete, or not up-to-date information, and **should not be considered as an official version.** To obtain the final, proofread, and updated version of this book, please visit the dedicated webpage of the Springer-Nature website. To learn more about CyberBRICS, please visit www.cyberbrics.info

CyberBRICS:

Cybersecurity Regulations in the BRICS Countries

Luca Belli, Editor

Prefaces by *Sergio Suchodolski* and *Sizwe Snail*

CONTENTS

Editor's Acknowledgment note:

The Editor would like to thank wholeheartedly Mr Luã Fergus for his substantial work, completing, correcting and proofreading the Chapter dedicated to Brazil, Dr Enrico Calandro for his revision of the Chapter dedicated to South Africa, and Mr Walter Britto, Ms Laila Lorenzon and Ms Carolina Telles and the entire CyberBRICS team for their substantial help in developing this volume.

PREFACE

Building universally accepted norms, standards and practices

Sergio Suchodolski

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, that 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 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 of Brazil, Russia, India, China and South Africa, 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, are at stake. 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 5 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.

PREFACE

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

Sizwe Lindelo Snail ka Mtuze

The advent of the Internet has brought about changes in the way that we communicate, 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 fifteen years as its applicability to Information and Communication Technologies is a key factor which 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 attend the seventh meeting of BRICS High Representatives for Security Issues in Beijing, China in 2017 where the parties agreed that,

> "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, that South

[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/>.

[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>.

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 which may result in serious data violations and other cyber security threats.

Cyber-war and cyber-terrorism are new frontiers in modern day warfare to which 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.

About the Authors

Luca Belli, PhD is Professor of Internet Governance and Regulation at Fundação Getulio Vargas (FGV) Law School, where I 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 which "De la gouvernance à la régulation de l'Internet" (Berger-Levrault, 2016); the "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 organisations 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 *i.a.* 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.

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 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 (LL.M.) from Harvard Law School, a Diplome (M.A.) from the Institut d'Etudes Politiques de Paris – Sciences-Po (Major in International Trade) and an LL.B. 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.

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 Masters 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. Sizwe Snail KA Mtuze was a member on the ICT REVIEW Panel of 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. Sizwe Snail Ka Mtuze also currently serves on the National Cyber Security Advisory Counsel of the DPTS.

Daniel Oppermann, PhD is a research coordinator at the NUPRI Research Centre for International Relations at the 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 of 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 at 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 A. 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 as a Project Coordinator to the Non-Governmental Organization 'Inter-regional Library Cooperation Centre', a working body of the UNESCO Information For All Programme. From 2011 onward, 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.

Anja Kovacs, PhD directs the Internet Democracy Project in Delhi, India. The Project works towards realising 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, and regarding 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 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, including 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, as well as having 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.

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, 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 U.S., she had 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.

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 organised 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). She 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 at age 25, Sagwadi was honoured as one of the Mail & Guardian 200 Young South Africans.

1. CyberBRICS:

A Multidimensional Approach to Cybersecurity for the BRICS

Luca Belli

Abstract

This chapter introduces the volume "CyberBRICS: Cybersecurity Regulations in the BRICS Countries", delimiting the concepts and issue areas that will be used to analyse the national framework of each BRICS (Brazil, Russia, India, China and South Africa) country. The chapter explains the rationale behind the approach developed by the CyberBRICS project – founded and directed by the author of this chapter – that identified five key dimensions of cybersecurity, which will be explored in the volume. The text presents such dimensions and the methodology used to analyse the national cybersecurity frameworks, moving from micro to macro, starting from data protection and then shifting to consumer protection, cybercrime, the preservation of public order and cyberdefense. 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.

Introduction

This book stems from the CyberBRICS project[3], 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[4], who are both the producers of large amounts of personal data, frequently referred to as "the new oil[5]", "the

[3] 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/>; <https://cyberbrics.info/>.

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

[5] 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).

new currency of the digital world,"[6] and "the world's most valuable resource[7]," 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[8] and businesses, but for the BRICS themselves, considering that these countries are facing a twofold "digital paradox[9]." The expansion and cost-reduction of connectivity allows 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 cyber threats, cybercrime and cyberattacks[10] 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 but also 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 state of play of BRICS

6 See Kuneva (2009).

7 See The Economist (2017).

8 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).

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

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

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 Goldman Sachs economist Jim O'Neill coined the expression BRICs[11] in 2001 – without the capital "S", as South Africa would join only at a later stage[12] – the acronym simply aimed at identifying Brazil, Russia, India and China in the context of an economic forecast. Yet, the BRICs, subsequently evolved into BRICS, seized the occasion to start debating how a "Post-western World"[13] 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[14].

BRICS countries are increasing their cooperation[15] 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.

---

11 See O'Neill (2001).

12 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 longstanding 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>.

13 See Stuenkel (2016).

14 See Brazilian Presidency of the BRICS. (2019).

15 See BRICS (14 August 2019).

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[16], including a the Memorandum of Understanding on Cooperation in Science, Technology and Innovation[17] 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[18] in 2016, the dedication of the 2018 Declaration of the BRICS Presidential Summit to a Collaboration for Inclusive Growth and Shared Prosperity in the 4th Industrial Revolution[19], and the elaboration of an Enabling Framework for the Innovation BRICS Network[20]. These efforts BRICS leaders have explicitly emphasised "the importance of continuing BRICS scientific, technical, innovation and entrepreneurship cooperation,"[21] and have already established concrete initiatives 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[22].

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 9th 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[23]." 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[24] and established a new BRICS 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;

16 For an analysis of such documents and their impact see Kiselev & Nechaeva (2018).

17 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).

18 See BRICS Working Group on ICT Cooperation. (11 November 2016).

19 See BRICS (2018).

20 See BRICS STIEP WG (May 2019).

21 See Itamaraty (27 June 2019).

22 Idem.

23 See BRICS (2017).

24 See BRICS (October 2019).

- 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; and
- ensuring wide and effective dissemination of information about BRICS STI activities amongst different stakeholders including policymakers, scientists, research organisations and a wider audience[25].

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[26]. 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[27] 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[28] and Shenzhen[29], 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[30] 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."[31] While the lack of a formal definition does not allow to officially labeling 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

[25] See BRICS (September 2019).

[26] 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).

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

[28] See Kunming (11 September 2019).

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

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

[31] See Belli (2016:347-358)

and responsibilities, in international public policy issues pertaining to the Internet"[32] 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 represent 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 "turbocharged climate-change"[33]. 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[34].

Cybersecurity was a largely ignored concept by the general public until former National Security Agency (NSA) contractor, Edward Snowden exposed the massive hacking and surveillance schemes by NSA and brought cybersecurity 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[35]."

---

[32] 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>.

[33] 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/>.

[34] Formal agreement on the necessity to adopt a multistakeholder model to properly address cybersecurity has already emerged since the World Summit on 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>.

[35] UNGA (2018:4).

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[36] – which, under some regulatory frameworks[37], 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[38], to transnational flows of personal data[39] or the security of 5G networking equipment[40].

As an important premise of this work, it must be clarified that the notion of cybersecurity is a very elastic[41] 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 frequently diverging perspectives and stressing that cybersecurity definitions often crystallise around specific issues, threats, activities and aspects[42]. 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*

[36] According to the cybersecurity analysis firm Gemalto, during the first six 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).

[37] 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. It 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."

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

[39] 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>.

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

[41] Since the World Summit on 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; harmonization 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).

[42] 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 conceptualizations of cybersecurity, see also Wolff (2016).

> *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*[43]*."*

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 [44]. 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 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[45]. Cyberattacks can also put

[43] See ITU-T (2009).

[44] 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.

[45] 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 he United States Cyber Command, the arm of the Pentagon that runs the military's offensive and defensive operations in the online world. See Sanger & Perlroth (2019).

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's in their elaboration phase[46], but they may utilise similar 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[47] 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 harmonization process.

This section provides an overview of the cybersecurity dimensions analysed in the volume, 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-

[46] As an instance, BRICS countries jointly agreed during the 9th 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.

[47] See BRICS (2017).

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[48] – 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[49] but also relevant risks.

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 USA, the countries currently having the most smartphone users in the world[50]. 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 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[51]".

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

[48] In China, significant government-led and policy-promoted investment in infrastructure are commonly acknowledged amongst the main driving forces that propelled the remarkable Internet growth undertaken by the country. See e.g. 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.

[49] The benefits derived from the expansion of connectivity as well as the advancement of the IoT can span from increased access to education, information and knowledge to gains in productivity, improved citizen participation, but also smoother transportations, more reliable electricity and cleaner environments. See e.g. World Bank (2016) and ITU (2016).

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

[51] See Tunis Agenda, paragraph 39.

destruction[52]. 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:

- The adoption of a new Brazilian General Data Protection Law and the final approval of the establishment of a new Data Protection Authority[53];
- The update of the Russian Data Protection legislation including data localisation provisions[54];
- The recognition of privacy as a fundamental right by the Indian Supreme Court and the ongoing elaboration of a new Data Protection Bill[55];
- 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[56];
- The creation of a Data Protection Regulator in South Africa and the upcoming enactment of the Protection of Personal Information Act[57].

The above-mentioned legislations present various similarities, such as for instance 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 among 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,[58] given that it specifies the more comprehensive – and binding – cybersecurity law..

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

[53] See Section 1 of the Brazilian Country Report, in Chapter 2.

[54] See Section 1 of the Russian Country Report, in Chapter 3.

[55] See Section 1 of the Indian Country Report, in Chapter 4.

[56] See Section 1 of the Chinese Country Report, in Chapter 5.

[57] See Section 1 of the South African Country Report, in Chapter 6.

[58] See Min Jiang's analysis in Chapter 8.

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 organizations' 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 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[59].

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 tha path to a different type of regulation based on concrete guidance to and effective monitoring of the entities to be regulated.[60] This may be an alternative option to be explored even beyond BRICS countries. Indeed, such 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[61]. 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[62] – including privacy, self-determination, and freedom of expression – but also promoting juridical certainty for businesses. Both rationales underpin data protection

---

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

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

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

[62] 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.) v. Union of India and Ors.

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 processing the personal data and society at large[63]. 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?

[63] See UNCTAD (2016).

11. Does the law provide any specific definitions with regards 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?
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[64] 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.

[64] See e.g. Gemalto (2018).

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 as well as 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 2025[65]. Indian e-commerce companies such as Snapdeal and Flipcart are already estimated to receive more than 70% of their orders via mobile phones[66]. 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[67].

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 utilizing (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 categorize the smart-home device supplier: a producer of connected objects or a supplier of digital services? This categorization may have relevant consequences in term of responsibility of the producer or provider, as it is evident in the Russian context, where free online services, they are used "at one's risk", as consumer protection applies only to services provided in exchange of a payment[68].

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[69].

---

65 In this sense, see Min Jiang Analysis in chapter 8.

66 See Bond (2019).

67 See <https://www.naspersreport2019.com/>.

68 See Andrey Shcherbovich's analysis in Chapter 4.

69 See Belli (2019).

Due to the number of already existing connected devices and their projected growth[70] 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[71] – or sometimes completely unsecured – devices are utilised by many users largely uninformed about cybersecurity. This proliferation of connected and potentially hackable devices raises the question as to what the most appropriate regulatory tool could be to prevent, mitigate or, ideally, eliminate the risks of cyberattacks.

It is important to note that the increase of cyberattacks is not only due to the numerical growth of connected devices. Indeed, the expansion of the IoT must be considered together with the simultaneous lack of security systems incorporated in the design of the connected products or services combined with the lack of consumer awareness regarding cybersecurity risks. IoT security is a major challenge. Attacks exploiting connected devices can be relatively easy to implement primarily because security is not the main preoccupation of product developers and investing in security raises development costs. The proliferation of connected devices from things we can wear to things we have in our homes further contributes to the vulnerability of cyberattack.

A telling example is the Mirai Botnet, a malicious software behind a series of massive distributed denial of service (DDoS) attacks in October 2016. Mirai infected hundreds of thousands of insecure consumer IoT devices that utilised the most common factory default usernames and passwords[72]. Both government portals and popular commercial services (such as Amazon, Netflix, Spotify and Twitter) were significantly disturbed and Brazil was among the most hit countries, alongside China, Russia and India in the top ten of the most affected[73].

An important observation to be made is that awareness-raising and education are essential to consumer protection in particular and to all cybersecurity dimensions in general. Major capacity building and awareness-raising efforts need to be organised to target all audiences: consumers and Internet users, especially children, teachers, researchers, governmental officials, and industrial actors. The Mirai example usefully illustrates the total unpreparedness of all stakeholders alike. Despite knowledge of the Mirai botnet, new variants keep on being discovered and attacks are mounting, primarily due to very poor security standards implemented by connected devices producers[74].

In this context, while personal data protection plays an essential role in preventing personal-data-related risks in the context of the IoT, the body of law that becomes essential to regulate the security

[70] 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/>.

[71] See Mosenia and Jha (2016).

[72] Marzano et al. (2018).

[73] See Antonakakis et al. (2017).

[74] See Pankov (2019).

of connected devices is consumer protection law. Both bodies of law are crucial, but user rights and consumer rights cannot be protected in the face of mounting risks if data subjects and consumers are not fully aware of their rights and risks involved or ways to mitigate such risks. As such, it is particularly relevant to map national consumer protection frameworks to have a clear understanding of what rights, obligations and security standards should consumers, producers and providers expect when choosing digital goods and services originating from the BRICS countries.

1.5.1. Consumer Protection Methodology

To facilitate the reader's comparison of the various consumer protection dimension, the same sub-dimensions utilised to map data protection frameworks were adopted, including the following five sets of questions tailored for consumer protection.

Scope

29. What national laws (or other types of normative acts) regulate consumer protection?
30. Is the country a party of any international consumer protection agreement?
31. To whom do consumer protection laws apply?
32. Do the laws apply to foreign entities that do not have a physical presence in the country?

Definitions

33. How is consumer protection defined?
34. How are consumers defined?
35. How are providers and producers defined?
36. Does the law provide any specific definitions with regards to consumer protection in the digital sphere?

Rights

37. Is the consumer protection law based on fundamental rights (defined in Constitutional law or International binding documents)?
38. What are the rights of the consumer defined by the law with reference to digital goods and services?
39. Is consumer protection law applicable to users of zero price services, *i.e.* free of charge?

Obligations and Sanctions

40. Does the law establish specific security requirements to provide digital services or goods?
41. What are the sanctions and remedies foreseen by the law for not complying with the obligations?

Actors

42. What bodies are responsible for the implementation of the consumer protection law?
43. Is there a specific consumer protection body? If so, what is its administrative structure?
44. What are the powers of the bodies responsible for the implementation of the consumer protection law?

1.6. Cybercrime

Cybercrime law is the body of law that defines what acts perpetrated via or against ICT systems should be considered as illegal and what measures and procedures should be followed to investigate such acts. As such, cybercrime can be considered either as a component of cybersecurity or at least as a field that largely juxtaposes to cybersecurity. Assuming that the main concern of cybersecurity is to foster security within ICT systems, thus protecting users and assets from any potential threats, it becomes useful to identify what activities should be categorised as malicious use of ICT systems and how they could be investigated and repressed. In this sense, the fact that the UN General Assembly, in its 2010 Resolution on Cybersecurity[75] addresses cybercrime as a core dimension of cybersecurity stresses the general tendency to consider them intimately intertwined issues.

In this perspective, the works of the ITU (2009; 2014) highlight cybercrime as an essential component of cybersecurity, stressing the importance of addressing it in national cybersecurity strategies. ITU clearly suggests that UN members adopt dedicated legislation addressing behaviours that can be categorised as criminal use of ICTs[76]. On the other hand, the UN members have agreed upon the benefits of multi-stakeholder[77] cooperation with regard to cybercrime[78]. Indeed, cybersecurity strategies and cybercrime frameworks, although crafted by public bodies, generally start with the consideration that cybercrime prevention, response and recovery need to rely on multi-stakeholder coordination, including private sector and individual users of ICT as partners in the implementation – and frequently also the elaboration – of public policies.

Furthermore, as pointed out by the ITU (2014), a general assumption of any cybersecurity or cybercrime strategy is that cyber threats are rarely national and generally have a cross-border nature. This is because the various intermediaries involved in the operation of the services and digital tools utilised to perpetrate a crime are rarely located all in the same jurisdiction[79]. In this perspective, the emergence of a shared –

[75] See UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[76] See ITU (2014).

[77] For an analysis of benefits as well as inconveniences determined by multistakeholder governance and models, see Belli (2015; 2016).

[78] Particularly, the Tunis Agenda, in its paragraph 40, affirms "the necessity of effective and efficient tools and actions, at national and international levels, to promote international cooperation among, inter alia, law-enforcement agencies on cybercrime [and] call[s] upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime."

[79] This situation has led Russia to enact "Internet Sovereignty" legislation, to reterritorialize digital environment, as illustrated by Andrey Shcherbovich analysis. See chapter 3 and the annexed Russian country report.

or at least convergent and compatible – BRICS legal framework on cybersecurity in general and cybercrime in particular seems to be a shared priority for BRICS that are increasingly exploring options to enhance their cooperation via the dedicated BRICS Working Group on Security in the Use of ICTs[80].

However, despite being a central aspect of cybersecurity, cybercrime may be challenging to delineate in research due to the lack of an international agreement on what elements compose it. This is particularly true since, despite the transnational nature of cybercrime, the definition of what activities in particular shall be deemed as criminal fall within the quintessentially national remit.

It may be argued that "cybercrime" encompasses a wide range of activities outlawed in specific jurisdictions and committed either by using ICT systems as an enabler in order to commit the crime or targeting specific ICT systems and the data that they store[81]. The ITU Global Programme on Cybercrime[82] offers two useful taxonomies of the offences that may be considered as cybercrimes. We consider two taxonomies for cybercrime below.

The first taxonomy is broader and considers whether digital technology is necessary to perpetuate the offence or simply enables the offence. To this central distinction, the ITU Global Programme on Cybercrime adds a third category, specially dedicated to online child sexual exploitation and abuse, as follows:

- Cyber-dependent crime: it requires an ICT infrastructure and involves the creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure (e.g. the cyber-takeover of a power-plant by an organised crime group) and taking a website offline by overloading it with data (a DDOS attack).
- Cyber-enabled crime: it can occur in the offline world but can also be facilitated by ICT. This typically includes online frauds, purchases of drugs online and online money laundering.
- Child sexual exploitation and abuse: it includes abuse on the clear Internet, darknet forums and, increasingly, the exploitation of self-created imagery via extortion – known as "sextortion".

The second taxonomy is based on the instrumental relationship between digital means and the specific offences. This categorization draws from the Convention on Cybercrime of the Council of Europe[83], better known as the Budapest Convention, clustering offences in four categories:

---

[80] Cybercrime and cyber-attacks are considered as transnational security issues to be maintained as "Main areas of cooperation" for BRICS countries. See <http://brics2019.itamaraty.gov.br/en/about-brics/main-areas-of-cooperation>.

[81] See World Bank (2017:66).

[82] See <https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html>.

[83] The Convention on Cybercrime of the Council of Europe (CETS No.185) is the only binding international instrument specially dedicated to framing cybercrime issue. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between treaty signatories. Interestingly, South Africa is the only BRICS member to be a signatory of the Budapest Convention while Russia, which is a Council of Europe member, is not a signatory. See <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

- Offences against the confidentiality, integrity and availability of computer data and systems;
- Computer-related offences;
- Content-related offences;
- Offences related to infringements of copyright and related rights.

As it emerges from the abovementioned taxonomies, the details of what can be considered cybercrime may – sometimes strongly – vary from country to country, especially when it comes to offences beyond the core of cybercrime. As pointed out by UNODC (2013), the core of cybercrime is composed of a limited number of acts against the confidentiality, integrity and availability of computer data or systems[84]. Beyond this core, whether a computer-related and computer content-related offence can be categorised as "cybercrime" is not universally agreed upon due to national juridical traditions and political sensitivities.

Given this context, the fact that BRICS countries have very different conceptions of cybercrime due to the different type and depth of the cybercrime debate in each country should not be a surprise. For instance, while in China the Criminal Law (1997) and Cybersecurity Law (2017) provide a very detailed list of what online behaviours shall be deemed as criminal[85], in Brazil only a few of the conducts that may be categorized as cybercrime are *de facto* penalized by law[86]. The Criminal law of Russia, in its general and special parts, also offers a rather detailed overview of cybercrimes[87] and related sanctions while in South Africa, until the new Cybercrime Bill will enter in force, cybercriminal conducts remain primarily defined only in a sectorial fashion by the Electronic Communications and Transactions Act[88]. India interestingly adopts a hybrid approach, providing sometimes detailed definitions of the constituent elements of the cybercrimes listed by the IT (Amendment) Act but remaining rather vague on the definition of the cybercrimes themselves[89].

To offer a better understanding of what behaviours can be considered as cybercrime and how criminal law de facto influences cybersecurity policy development in the BRICS, the CyberBRICS project has adapted its penta-dimensional framework adding a further sub-dimension dedicated to procedural law.

1.6.1. Cybercrime Methodology

Scope

45. What national laws (or other types of normative acts) regulate cybercrime?

[84] See UNODC (2013).

[85] See the Cybercrime section of the Chinese Country Report, annexed to Chapter 5.

[86] See Chapter 2 of this volume.

[87] See the Cybercrime section of the Russian Country Report, in Chapter 3.

[88] See Sagwadi Mabunda analysis in Chapter 6 and the cybercrime section of the annexed South African Country Report.

[89] See Anja Kovacs' Analysis in Chapter 4 and the Cybercrime section of the annexed Indian Country Report.

46. Is the country a party of any international cybercrime agreement?
47. What cybercrimes are regulated?
48. To whom do the laws apply?
49. Do the laws apply to foreign entities that do not have a physical presence in the country?

Definitions

50. How is cybercrime generally defined by the national law?
51. What are the cybercrimes provided for by the law and how are they defined?
52. How is a computer system defined?
53. How are computer data defined?
54. How are forensic data defined?
55. How are service providers defined?
56. Does the national law provide any other definitions instrumental to the application of cybercrime legislation?

Rights

57. Is the cybercrime law based on fundamental rights (defined in Constitutional law or International binding documents)?
58. What are the rights of the victim and the accused?

Procedures

59. Is there a specific procedure to identify, analyse, relate, categorize, assess and establish causes associated with forensic data regarding cybercrimes?
60. In the case of transnational crimes, how is cooperation between the national law enforcement agency and the foreign agents regulated?
61. Is there any exception to the use of mutual legal assistance procedure to investigate the crime?
62. Does the national law require the use of measures to prevent cybercrimes? If so, what are they?

Obligations and Sanctions

63. What obligations do law enforcement agencies have to protect the data of the suspect, the accused and the victim?
64. What are the duties and obligations of the National Prosecuting Authorities in cases of cybercrime?
65. Does the law impose any obligations on services providers in connection with cybercrime?
66. To which extent can a legal person be held liable for actions in connection with cybercrimes?

Actors

67. What bodies implement the cybercrime legislation?
68. Is there a special public prosecutor office for cybercrime? If so, how is it organised?
69. Does the cybercrime legislation create any specific body?

1.7. Public Order

The preservation of public order – frequently referred to using the French expression "*ordre public"* – is considered, under international law, as a rightful justification for imposing limitations to fundamental rights and freedoms. According to the International Covenant on Civil and Political Rights, for instance, a number of fundamental rights, including the right to freedom of expression, the right of peaceful assembly, the right to freedom of association with others, and the liberty of movement, can be rightfully restricted by law, when such restrictions are "necessary to protect public order[90]." The contours of the notion, however, are particularly fuzzy and, for this reason, the preservation of public order must be pursued within specific rule of law frameworks delineating when it is appropriate to invoke public order as a legitimate justification and which authorities can implement police functions and under what circumstances.

While the term "police" generally refers to bodies whose fundamental purpose is to preserve public order and public safety through the enforcement of rules and assisting the public, the police function may acquire a different nature when applied to the digital environment as it is increasingly delegated to non-public actors[91]. In this case, the rule of law requirement becomes even fuzzier in the context of an increasing delegation of police functions to private Internet intermediaries[92].

The protection and preservation of public order and morality are at the core of administrative policing, the objectives of which are unique to every country. On the other hand, judicial policing has a repressive character, aimed at recording offences against criminal law, gathering evidence and searching for the perpetrators of specific offences[93]. To distinguish between administrative and judicial policing, it is important to consider the intent for which police operations are undertaken. Particularly, it depends on the existence of a link between a police operation and a criminal offence: administrative policing is aimed at the general preservation of public order and morality; judicial policing is aimed at the special repression of given offences.

---

[90] See e.g. ICCPR (1966) art. 12, 19, 21 and 22. Importantly, the degree of "necessity" is generally evaluated considering the legitimacy of the goal established by law and the proportionality of the measures. In this perspective the UN Human Rights Council has consistently stated that "Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instruments amongst those, which might achieve the desired result; and they must be proportionate to the interest to be protected." See e.g. UNHRC General Comments No. 27/1999 and No. 34/2004.

[91] See Belli & Sappa (2017).

[92] See Belli, Francisco & Zingales (2017).

[93] Idem.

In this perspective, Internet intermediaries implementing specific content management measures – such as China's elaborate content management system[94] aimed at removing or disabling access to specific content in order to protect public order – act as administrative police. On the other hand, Internet intermediaries retaining personal data of (cyber)criminal offenders or blocking access to content in compliance with court decisions act as criminal police. As such, private intermediaries can act as cyber-police to monitor the implementation of national legislation.

To analyse the specific normative measures allowing for the preservation of public order as well as the existence of specific "cyber measures" involving private intermediaries in the implementation of national law, the methodology developed by the CyberBRICS project has included a specific dimension dedicated to public order.

1.7.1. Public Order Methodology

Definitions

70. How are public order, threats to public order and the protection of public order defined?
71. Is the protection of public order grounded in constitutional norms?

Measures

72. What cyber measures address threats to public order?

Actors

73. What public authorities are responsible for the implementation of surveillance techniques?
74. What are the obligations of these public authorities?
75. Can private actors be involved in the implementation of cyber measures to address threats to public order?

1.8. Cyberdefence

The last dimension considered by this volume is cyberdefence , which is essential to give force to the overall policy efforts and governance mechanisms aimed at improving each country's cybersecurity. Cyberdefence mechanisms and, particularly, the type measures necessary to handle cyberattacks and cyber threats are frequently developed and enacted as a reaction to disruptive events. This is the case for instance, of Brazil, where cyberdefence started to be a topic of interest in the aftermath of a series of web defacement attacks in 2011when a larger number of public service portals and government websites went offline for several hours[95].

[94] See Min Jiang's analysis in Chapter 5 as well as the Chinese Country Report.

[95] See Daniel Oppermann's analysis in chapter 2 of this volume.

This dimension typically falls under the purview of a country's national security policy, including operational actions deployed for offensive and counter-offensive combats in cyberspace. For this reason, cyberdefence is commonly linked to countries' military and intelligence services[96]. The country reports included in this book show that this tendency is also shared by BRICS countries, with a strong military presence.

Furthermore, a distinguishing trait of cyberdefence is that it is typically elaborated and implemented by the Executive. This means cyberdefence is usually shaped directly by the national defence ministry or administration and is closely intertwined with secret and classified aspects of government policy and activity[97]. This is particularly evident in the Russian case, where cyberdefence is primarily shaped by official doctrines defined by the President of the Russian Federation, acting in his constitutional role of Supreme Commander of the Armed Forces[98].

While the other cybersecurity dimensions are defined by policies typically released into the public domain, cyberdefence may have a non-public nature, due to its particular sensitivity. While some aspects of cyberdefence are public, such as what events shall be considered as a cyberattack, what are the criteria for attributability of the responsibility in cyberattacks and what measures will be taken as self-defence against such attacks, other elements may be much less clear and public such as to which extent cyber offence or interventions in other countries' systems or infrastructures are deemed as admissible and de facto undertaken. Therefore, it is important to acknowledge that, due to its highly sensitive nature, many elements of cyberdefence may be secret and this peculiarity makes it more challenging to have a complete picture and a clear understanding of the national frameworks.

It can be argued that cyberdefence strategies and frameworks primarily focus on two axes: on the one hand, the defensive measures that can improve robustness and resilience of national infrastructures and systems that are deemed as critical; on the other hand, the measures that can prevent and avoid cyber espionage, securing information systems and networks. As pointed out previously, cybersecurity in general – and cyberdefence in particular – have gained momentum due to increasing awareness of the potential that digital technologies offer for attacking, surveillance and meddling into national public affairs.

The revelations of NSA contractor Edward Snowden have been a particularly dire and palpable wakeup call for BRICS, with the Brazilian President's personal phone being wiretapped[99], together

[96] See Canongia & Mandarino (2012).

[97] See Dewar (2018).

[98] The Military Doctrine of the Russian Federation and the Russian Doctrine of Information Security are particularly relevant in this regard, as pointed out by Andrey Shcherbovich's analysis in Chapter 4.

[99] See Bridi & Greenwald (2013).

with the communications of a wide number of members of the Brazilian government[100], and Mr Snowden being in exile in Russia since the revelations.

In this perspective, as noted by Min Jiang's analysis in this book, cyberdefence and cybersecurity ultimately become instrumental to national sovereignty. The guarantee of network and information security and the capability to effectively defend critical infrastructure are essential components of national security. As stressed by Jiang, this calculation drives BRICS countries – and arguably any other country – to prioritize their technological development and national control over information communication infrastructures. Indeed, the increasing interconnection and digitalisation of national economies, government services and virtually any "thing" imposes the necessity to be able to prevent, stop and manage cyberattacks, intrusions, theft, online distribution of harmful information.

Effective control and protection of critical infrastructures, information systems and databases are not only instrumental to assure cybersecurity but also national sovereignty. In this perspective, a number of states, most notably the Russian Federation[101], have argued that, to guarantee national sovereignty and cyberdefence , nation-states have the right to independently set policies regulating Internet critical resources, such as globally unique identifiers, including Internet Protocol (IP) addresses, domain names and autonomous system numbers that allow the Domain Name System (DNS) to smoothly function.

It is important to point out that, while it is absolutely legitimate for a country to exercise national sovereignty and set policies that apply both offline and online, such policies may contribute to the fragmentation[102] of the global Internet into national intranets and consequently their impact – with particular regard to the costs and benefits of the policies upholding sovereignty but fostering fragmentation – should be carefully considered by BRICS leaders.

To map the BRICS cyberdefence frameworks and provide the reader with a better understanding of the cyberdefence conceptualisations of these countries, the following elaborates our mapping in this area.

1.8.1. Cyberdefence Methodology

Scope

76. Is there a national cyberdefence strategy or is cyberdefence mentioned in the national defence strategy?
77. What is the legal status of the national defence or cyberdefence strategy?
78. What national laws or other normative acts regulate cyberdefence in the country?
79. Is the country party of any international cooperation agreement in the sphere of cyberdefence?

[100] See O Globo (2015).

[101] See the Russian enactment of the "Internet Sovereignty" law, as highlighted by Andrey Shcherbovich's analysis in chapter 4.

[102] In this perspective, see Drake, Cerf & Kleinwächter (2016).

80. Does the national cyberdefence strategy provide for retaliation?

Definitions

81. How are national security and national defence defined?
82. How are cybersecurity and cyberdefence defined?
83. How are threats to national security and cyberthreats defined?
84. How is a cyberattack defined?
85. Does the national law provide any other definitions instrumental to the application of cyberdefence legislation?

National framework

86. Is cyberdefence grounded on the constitutional provisions and/or international law?
87. Which specific national defence measures are related to cybersecurity?
88. Is there a national defence doctrine and does the law or strategy refer to it?
89. What measures are mentioned in the national law and strategy in order to implement cyberdefence?
90. How can Internet users' online activities be limited for the reasons of protection of national security and cyberdefence?
91. Does the national law or strategy foresee any special regime to be implemented in case of emergency in the context of cyberdefence?
92. Is there any specific framework regulating threats to critical infrastructure?

Actors

93. What actors are explicitly mentioned as playing a role regarding cyberdefence in the law or national cyberdefence strategy or defence strategy?
94. Is there a specific cyberdefence body?
95. What are the tasks of the aforementioned actors?

1.9. Towards Cooperation and Convergence in BRICS Cyber-policies

As stressed by the BRICS leaders themselves, ICTs "provide citizens with new tools for the effective functioning of economy, society and state […] and the use and development of ICTs through international cooperation and universally accepted norms and principles of international law is of paramount importance in order to ensure a peaceful, secure and open digital and Internet space[103]." Since the Ufa Declaration, BRICS countries are prioritising digital policies in general and

[103] See BRICS. (9 July 2015).

cybersecurity in particular in their own national agendas, while also pursuing increasing compatible cybersecurity objectives.

The Goa Declaration highlights the potential for cooperation amongst the BRICS countries that could "work together for the adoption of the rules, norms and principles of responsible behaviour of States including through the process of the United Nations Group of Governmental Experts (UNGGE)"[104]. Further, BRICS leaders established a BRICS Working Group on ICT Cooperation so that "members could actively lead and cooperate to strategize synergies, [...] sharing of information and case studies on ICT policies and programs in creating enabling environment"[105]. Moreover, a BRICS Science & Technology Enterprise Partnership (BRICS-STEP) was created, subsequently renamed STIEP, to highlight the importance of cooperation on mutually beneficial innovation and, as noticed in the introduction, the recent approval of the new BRICS STI Architecture, explicitly aims at improving the coordination of the BRICS STI cooperation governance structure, establishing and monitoring actions and involving a wide range of stakeholders "including policy makers, scientists, research organisations and a wider audience[106]."

These initiatives make evident that BRICS have fostered both intergovernmental and multi-stakeholder cooperation. Importantly, BRICS countries have long recognized the value of multi-stakeholder partnerships to deal effectively with digital challenges, although of course each BRICS country may have a different perspective on how such partnerships must be implemented and what stakeholders should be involved. Over the past few years, BRICS have consistently affirmed that "the Internet is a global resource and that States should participate on an equal footing in its evolution and functioning, taking into account the need to involve relevant stakeholders in their respective roles and responsibilities[107]."

As mentioned previously, the Xiamen Declaration has clearly signalled the BRICS willingness to intensify intergovernmental cooperation to promote the "establishment of internationally applicable rules for security of ICT infrastructure, data protection and the Internet[108]." In spite of not being formally organised into a specific intergovernmental organisation, BRICS countries do not need to start their policymaking cooperation from scratch, as they can rely on solid bases grounded in binding international agreements and joint membership of several intergovernmental organisations such as the United Nations system, the World Trade Organization, the International Monetary Fund and the World Bank. Common membership to all these organization provides more than one suitable arena for dialogue, cooperation and coordination, norm development and conflict resolution as well as exercise of global influence.

---

104 Ibid.

105 Ibid.

106 See BRICS (September 2019).

107 Ibid.

108 See BRICS (2017).

The existing solid diplomatic relations and international frameworks on which such relations rely have allowed BRICS countries to demonstrate that, while the countries remain a very elastic and heterogeneous grouping, they are capable of achieving impressive results with concrete actions, including creating an entirely new global financial institution such as the New Development Bank where their perspectives and interests align. Such BRICS activities reflect not only these countries' interest to rebalance the existing international financial and economic architecture[109], but also their intention to develop convergent and legally interoperable digital policy frameworks.

The following chapters will present and map the five cybersecurity dimensions that have been introduced in the first chapter. Importantly, it can be argued that, even in the absence of formal cybersecurity agreements, the technological as well as regulatory, social and economic evolutions that BRICS countries are experiencing are triggering a process of spontaneous convergence in several sub-segments of the analysed dimensions. Such trends, which are already visible, deserve much more attention and scrutiny as we try to explore them in some detail in this volume[110].

Enhanced cooperation and legal interoperability amongst BRICS countries with regard to digital policy is increasingly possible and, to some extent, already happening. Given the importance and impact of BRICS digital policies for the entire world, it is the hope of the author of this chapter as founder and director of the CyberBRICS project that this volume will initiate much more needed research on such policies. Metaphorically, this book is laying the first brick on which CyberBRICS can be successfully built.

1.10. References

Antonakakis Manos *et al*. (2017). Understanding the Mirai Botnet. In Proceedings of the 26th USENIX Security Symposium August 16–18, 2017. Vancouver, BC, Canada <https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf>.

Banga, Rashmi & Jeet Singh, Parminder (2019). BRICS Digital Cooperation for Industrialization. Working Paper 4/2019. Centre for Competition Regulation and Economic Development. University of Johannesburg.

Belli, Luca. (2017). Net Neutrality, Zero-rating and the Minitelisation of the Internet. Journal of Cyber Policy. Routledge. Vol 2. nº 1. <https://doi.org/10.1080/23738871.2016.1238954>.

Belli Luca. (2019). The Need for a RIoT (Responsible Internet of Things): A Human Rights Perspective on IoT Systems. In Mullen M. et al (2019). Navigating a New Era in Business and Human Rights. Institute of Human Rights and Peace Studies and Article 30. Pp. 181-188. <https://article30.org/wp-content/uploads/2019/08/a_new_era.pdf>.

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

Belli, Luca. (2015). A heterostakeholder cooperation for sustainable Internet policymaking. Internet Policy Review, 4(2). <https://doi.org/10.14763/2015.2.364>.

[109] In this sense see Ziero (2015).

[110] The various facets of the BRICS digital policies will be analysed in the forthcoming works of the CyberBRICS project.

Belli, Luca; Francisco, Pedro & Zingales, Nicolo. (2017). Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police. In Belli, Luca & Zingales, Nicolo (Eds.) Platform regulations: how platforms are regulated and how they regulate us. Rio de Janeiro. FGV Direito Rio. Pp 41-64. <https://bibliotecadigital.fgv.br/dspace/handle/10438/19402>.

Belli, Luca & Sappa, Cristiana. (2017). The Intermediary Conundrum: Cyber-regulators, Cyber-police or both? JIPITEC (Journal of Intellectual Property, Information Technology and Electronic Commerce Law) Special Issue: Intermediary Liability as a Human Rights Issue. Vol. 8, n° 3. Pp 183-198. <https://www.jipitec.eu/issues/jipitec-8-3-2017/4620>.

Belli, Luca & Venturini, Jamila. (2016). Private ordering and the rise of terms of service as cyber-regulation. Internet Policy Review, 5(4). <https://doi.org/10.14763/2016.4.441>.

Bond. (2019). Internet Trends 2019. <https://www.bondcap.com/report/itr19/#view/1>.

Boston Consulting Group (September 2017). Decoding the Chinese Internet. A white paper on China's Internet economy.

Brazilian Presidency of the BRICS. (2019). What is BRICS? <http://brics2019.itamaraty.gov.br/en/about-brics/what-is-brics>.

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

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

BRICS. (14 August 2019). Declaration of the BRICS Ministers of Science, Technology and Telecommunications, Brasilia, Brasil. <http://brics2019.itamaraty.gov.br/images/documentos/Declarao_da_5_Reunio_de_Comunicao_dos_Ministros_do_BRICS.pdf>.

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

BRICS. (4 September 2017). 9th BRICS Summit. BRICS Leaders Xiamen Declaration. Xiamen, China. <http://www.itamaraty.gov.br/en/press-releases/17427-9th-brics-summit-brics-leaders-xiamen-declaration-xiamen-china-september-4-2017>.

BRICS. (16 October 2016). 8th BRICS Summit: Goa Declaration. Goa, India. <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/14931-viii-cupula-do-brics-goa-india-15-e-16-de-outubro-de-2016-declaracao-e-plano-de-acao-de-goa>.

BRICS. (18 March 2015). BRICS Memorandum of Understanding on Cooperation in Science, Technology and Innovation. Second BRICS Science, Technology and Innovation Ministerial Meeting. Brasília, 18 March, 2015. <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/8342-ii-reuniao-de-ministros-de-ciencia-tecnologia-e-inovacao-do-brics-documentos-aprovados-brasilia-18-de-marco-de-2015#mos>.

BRICS. (9 July 2015). Ufa Declaration, VII BRICS Summit. Ufa, Russian Federation. <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/10465-vii-cupula-do-brics-declaracao-de-ufa-ufa-russia-9-de-julho-de-2015#eng>.

BRICS Competition Centre. (2019). Digital Era Competition BRICS Report. <https://cyberbrics.info/digital-era-competition-brics-report/>.

BRICS STIEP WG. (May 2019). Minutes of the BRICS Working Group on Science Technology Innovation and Entrepreneurship Partnership (STIEP WG). Foz do Iguaçu, Brasil 12-15 May 2019. <http://brics2019.itamaraty.gov.br/images/documentos/Minutes_of_the_3rd_Meeting_of_the_STIEP_WG_-_Complete_version.pdf>.

BRICS Working Group on ICT Cooperation. (11 November 2016). Digital Partnership – Transformation through ICTs. ICT Development Agenda and Action Plan. 2nd Meeting of BRICS Ministers of Communications.

Bridi, Sonia & Greenwald, Glenn (1 September 2013). Documentos revelam esquema de agência dos EUA para espionar Dilma. O Globo. <http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html>.

Canongia, Claudia & Mandarino; Raphael. (2012). Cybersecurity: The new challenge of the information society. Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions. IGI Global.

Cisco. (2017). Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2016 2021. White Paper. San Jose, CA: Cisco. <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html>.

Department of Telecommunications and Postal Services, South Africa. (2017). Cybersecurity Readiness Report 2017. <https://www.cybersecurityhub.gov.za/images/docs/Cyber-Readiness-Report.pdf>.

Dewar, Robert S. (Ed.) (2018) National Cyberdefence Policy Snapshots. Cyber Defence Project (CDP). Zürich, September 2018. Centre for Security Studies (CSS).

Drake, William J.; Cerf Vinton G. & Kleinwächter, Wolfgang. (January 2016). Internet Fragmentation: An Overview. Future of the Internet Initiative White Paper. <http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf>.

Ewing, Reese. (27 July 2016) Brazil prosecutor freezes $11.7 million of Facebook funds due to WhatsApp case. Reuters. <https://www.reuters.com/article/us-brazil-facebook-whatsapp-idUSKCN10801Q>.

European Union Chamber of Commerce in China (2019). The Digital Hand: How China's Corporate Social Credit System Conditions Market Actors. <https://www.europeanchamber.com.cn/en/publications-archive/709/The_Digital_Hand_How_China_s_Corporate_Social_Credit_System_Conditions_Market_Actors>

Fichtner, L. (2018_). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, *7*(2), 1-19. <https://doi.org/DOI:10.14763/2018.2.788>.

Gemalto. (2018). Breach Level Index. <https://breachlevelindex.com/request-report>.

Kolomychenko, Maria. (30 August 2018). Russia tries more precise technology to block Telegram messenger. Reuters. <https://www.reuters.com/article/us-russia-telegram/russia-tries-more-precise-technology-to-block-telegram-messenger-idUSKCN1LF1ZZ>.

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

Kiselev, Vladimir & Nechaeva, Elena. (2018). Priorities and Possible Risks of the BRICS Countries' Cooperation in Science, Technology and Innovation, 5(4) BRICS Law Journal 33–60 <https://doi.org/10.21684/2412-2343-2018-5-4-33-60>.

Kuneva, Meglena. (31 March 2009). Keynote Speech. Rundtable on Online Data Collection, Targeting and Profiling. Brusseks, European Commission. <http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm>.

Marzano, Artur *et al*. (2018). The Evolution of Bashlite and Mirai IoT Botnets. in 2018 IEEE Symposium on Computers and Communications (ISCC). <https://ieeexplore.ieee.org/document/8538636>.

Mosenia, Arsalan & Jha, Niraj K. (2016). A Comprehensive Study of Security of Internet-of-Things. in IEEE Transactions on Emerging Topics in Computing. Vol. 5 N° 4 <https://ieeexplore.ieee.org/document/7562568>.

NIST (National Institute of Standards and Technology) (August 2003). Special Publication 800-59. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf>.

ICCPR (International Covenant on Civil and Political Rights). (1966). Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976. <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

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

ITU. (2016). Harnessing the Internet of Things for Global Development: A Contribution to the.

ITU. (2014) Understanding cybercrime: Phenomena, challenges and legal response Geneva: ITU Telecommunication Development Bureau. <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf>.

ITU. (2005). ITU WSIS Thematic Meeting on Cybersecurity. Chairman's Report. ITU Headquarters, Geneva, Switzerland. 28 June – 1 July 2005.

ITU-T. (2009). Recommendation X.1205 (04/08): Overview of cybersecurity. Approved in 2008-04-18. <https://www.itu.int/rec/T-REC-X.1205-200804-I>.

UN Broadband Commission for Sustainable Development. Geneva: International Telecommunication Union. <https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf>.

O Globo. (4 July 2015). EUA grampearam Dilma, ex-ministros e avião presidencial, revela WikiLeak. <http://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html>.

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

Pankov, Nikolay. (19 March 2019). Mirai goes Enterprise. Karspersky Daily. <https://www.kaspersky.com/blog/mirai-enterprise/26032/>.

Sanger, David E. & Perlroth, Nicole. (June 15, 2019). U.S. Escalates Online Attacks on Russia's Power Grid. <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?smid=nytcore-ios-share>.

Sevastopulo, Demetri & Bond, David. (17 February 2019) UK says Huawei is manageable risk to 5G. Financial Times. <https://www.ft.com/content/619f9df4-32c2-11e9-bd3a-8b2a211d90d5>.

Statista. (2019). Number of smartphone users by country as of September 2019 (in millions). <https://www.statista.com/statistics/748053/worldwide-top-countries-smartphone-users/>.

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

The Economist. (6 May 2017). The world's most valuable resource is no longer oil, but data. <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>.

UNCTAD (United Nations Conference on Trade and Development). (2016). Data protection regulations and international data flows: Implications for trade and development. <https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf>.

United Nations' High Level Panel on Digital Cooperation (2019). The Age of Digital Interdependence: Report of the High-Level Panel on Digital Cooperation. <https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf>.

UNGA (United Nations General Assembly). (1 March 2018). Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels. Report of the Secretary-General. A/73/66–E/2018/10.

UNODC (United Nations Office on Drugs and Crime). (2013). Comprehensive Study on Cybercrime. Vienna: UNODC. <https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf>.

Vaidya, Tavish. (July 2015). 2001-2013: Survey and Analysis of Major Cyberattacks. Department of Computer Science, Georgetown University. <http://arxiv.org/pdf/1507.06673.pdf>.

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

Wolff, J. (2016). What we talk about when we talk about cybersecurity: Security in Internet governance debates. Internet Policy Review, 5(3). <https://doi.org/doi:10.14763/2016.3.430>.

World Bank. (2016). World Development Report 2016: Digital Dividends. Washington, DC: World Bank. <http://pubdocs.worldbank.org/en/391452529895999/WDR16-BP-Exploring-the-Relationship-between-Broadband-and-Economic-Growth-Minges.pdf>.

World Bank (2017). Combatting Cybercrime Tools and Capacity Building for Emerging Economies. Washington, DC: The World Bank. <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf>.

Ziero, Gabriel Webber. (December 2015). Looking for a BRICS perspective on international law. Revista de Direito Internacional, Brasília. Vol. 12. N. 2. Pp. 303-322. <https://doi.org/10.5102/rdi.v12i2.3678>.

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

Editor's Acknowledgment note:

The Editor would like to thank wholeheartedly Mr Luã Fergus for his substantial work, completing, correcting, and proofreading the country report annexed to this chapter.

2. Dimensions of Cybersecurity in Brazil

Daniel Oppermann

2.1. Introduction

Cybersecurity is a term with a variety of meanings. A term that at this point has received little attention as a concept in academia although it is used by countless organizations and individuals of different professional backgrounds. Observing debates on cybersecurity in diverging academic environments it becomes clear that increasing understanding and acceptance of multidisciplinarity would improve the debates as they are taking place so far. This chapter is a reflection on an initial but not fully debated attempt to create subcategories for cybersecurity from a legal perspective in which the concept itself serves as the main category subdivided into data protection, consumer protection, cybercrime, public order and cyberdefence , all with a focus on Brazil as a national case.

In 2019, the Brazilian Statistics Institute IBGE estimated that about 210 million people are currently living in Brazil[111]. 2018 data collections of CETIC, the research department of the country's ccTLD registry NIC.BR, stated that 76% of the Brazilian population (at the age of 10 and above) were classified as Internet users[112]. Being an Internet user in these statistics does not equate to daily or permanent access, however, it indicates frequent use of the Internet[113]. While nowadays online consumption through e-commerce providers (including the use of online payment services) and information or infotainment providers are among the leading online services used in Brazil, social media providers already had a special position among the country's user community since the early days of Orkut and Fotolog[114]. These virtual vanguards kept the first generation of Internet users in front of their monitors – especially after 00h on weekdays, after 14h on Saturdays and all day long on Sundays, when dial-up connections had the lowest rates. Even before some of today's market

[111] See IBGE (2019).

[112] See CETIC.BR (2018).

[113] CETIC uses the ITU definition of Internet users, which are "considered to be individuals who have used the Web at least once in the three months prior to the interview" (NIC.BR, 2018:211).

[114] Orkut and Fotolog were both social networks with a large number of users in Brazil.

leaders like Facebook, YouTube, Instagram or Twitter were created, the first generation of Brazilian Internet users was already taking early lessons on uncontrolled sharing of personal data.

The fascination for social media in combination with specific Brazilian cultural characteristics of untroubled exchange of personal information gave Internet companies access to large amounts of personal data, leaving Brazilian online users alone without sufficient legal protection of their data. Awareness regarding the need for data protection started growing over the years, also due to the activities of organizations like the Brazilian Internet Steering Committee (CGI) and the national Internet Governance Forum (Fórum da Internet no Brasil), and the participation of the country on the global level by hosting not just the NetMundial Meeting in 2014 but also two editions of the UN Internet Governance Forum in Rio de Janeiro (2007) and João Pessoa (2015). Besides that, capacity building initiatives like Internet governance courses of different formats[115], the engagement of civil society organizations like SaferNet[116] and a number of policy research initiatives contributed to the attempt of educating online users on security challenges and data protection on the Internet.

On the following pages, this chapter will give a short reflection on the five cybersecurity dimensions identified by the CyberBRICS project – namely data protection, consumer protection, cybercrime, public order and cyberdefence – with regard to the Brazilian context.

2.2. Data Protection

Data protection is much more than a technical process or a legal challenge. It includes further variables like, for example, user behaviour which is heavily influenced by cultural norms that have developed over generations. The question of if and how individuals share information over computer networks can be considered a reflection of their offline behaviour spiced with the often-delusive variable of anonymity. As it is common in the social sphere, these cultural norms are as well influenced by public discourse and debates that are shaping both offline and online behaviour.

In the case of Brazil, information sharing is a widespread everyday behaviour where curiosity about the lives of others often meets the desire of the individual to become part of wider or public debates. Information in this context is not limited to public debates on politics and economy but includes, to an extensive level, personal information and data about oneself and other individuals and private citizens. It is not surprising that in the early 2000s social networks like Orkut or Fotolog were celebrating major successes in Brazil[117]. These junior tools of digitalization of the private lives of ordinary citizens, most of them between the ages of 15 and 30, were almost the perfection of a digital symbiosis where curious and astonished users met the new honeypots of companies that tried to tie users to their tools

[115] Examples are courses organized by NIC.br, the InternetLab or the Governance Primer classes.

[116] Besides other activities, SaferNet has created anonymous communication channels which citizens can use to report cybercrimes, online hate speech and other offenses. More information can be found on their website <https://www.safernet.org.br>.

[117] For more details on Orkut's position in Brazil see: M. Bezerra and E. Araújo (2011); S. Sales e M. Paraíso (2010); R. Silva; A. Nichel; A. Martins, and C. Borchardt (2011).

(nowadays also called platforms) to create traffic, benefit from advertisements and, in the end, collect different types of user data.

Since the late 2000s, Brazilians started switching from these early tools to the latest generation of social media including Facebook, Instagram, Twitter and others. Over the years, the experiences of the early user community had created a small but growing consciousness regarding the impact of uncontrolled public display on the Internet. Especially the experiences of the Orkut-years in combination with a growing number of professional events and awareness campaigns by organizations like NIC.br, Safernet and others had strengthened the nevertheless still weak debates on data protection in the country.

In parallel to the growth of social media platforms, other types of online providers started to collect growing amounts of user data, including e-commerce providers, which over the years adopted more sophisticated manners of analysing the online behaviour of their clients. Besides that, the development of the Brazilian Internet Civil Rights Framework, better known as *Marco Civil da Internet*, which was signed by then-President Dilma Rousseff during the NetMundial Meeting in São Paulo in 2014, contributed to the growing awareness of the need for data protection and user rights. This would then culminate in the development of the data protection law (LGPD, *Lei Geral de Proteção de Dados*, n. 13.709/2018), signed by then-President Michel Temer in 2018[118].

Highly influenced by the development process of the 2016 European General Data Protection Regulation (GDPR), the LGPD is an extensive law of 65 articles offering definitions for a number of terms used throughout the document, including data processors and operators, data quality, transparency, security, databases, data sharing and more[119]. The law addresses the questions of user rights and obligations of data controllers and processors. Besides that, it approaches questions of privacy and certain security measures. In July 2019, the Brazilian government under President Jair Bolsonaro created the National Data Protection Authority, a public organ mentioned in the law, which will be responsible for specific tasks including supervision and sanctioning in the context of data protection in the country, once the law comes into force in August 2020[120].

2.3. Consumer Protection

In the digital age, the challenges of consumer protection have gained additional dimensions. Over the years, Internet users in Brazil have become users and consumers of paid digital services, e-commerce providers and other types of consumption-oriented offers. Traditional Brazilian organizations for consumer protection (like PROCON and IDEC, plus a number of smaller initiatives) which were already struggling to keep up with the offline world were thrown into an additional setting that required

[118] See B. Caram and T. Fernandes (2018).

[119] See Presidência da República (2018).

[120] See Agência Senado (2019).

rethinking many of the previous mechanisms and which, especially in the 1990s and the 2000s, opened the doors for fraudulent online behaviour. The lack of knowledge regarding good and bad practices of electronic commerce and the absence of any specific regulation addressing digital goods and services left consumers, police and jurists in a difficult position.

While throughout the 2010s a number of e-commerce providers managed to establish themselves as leading and trustful online consumption suppliers, the first years of the new century showed a different picture. The absence or low dispersion of both reliable online payment systems and trustworthy established e-commerce companies opened the gap for small and mid-sized actors who managed to commit fraud by announcing and selling physical products online that were never delivered. Consumers who became victims of such kinds of fraud had little chance to retrieve their expenses since hardly any public service was prepared to react.

Although online fraud and other forms of exploiting consumers on the Internet has not disappeared (and there is no serious chance that it will), Brazilian consumers and public services have increased awareness over the past ten years. The traditional consumer protection legislation, such as the 1990 consumer protection law[121] (n. 8.078/1990), was enhanced by the 2013 decree n. 7.962/2013, which addresses the challenges of electronic commerce[122]. Following this decree, e-commerce providers need to fulfil a number of requirements including providing clear information about products and their possible health and security risks, time and form of delivery, payment methods and more. Consumers started enjoying a number of rights including the right to complain or to cancel their purchase.

Consumer protection, however, cannot be reduced to e-commerce services. It also includes challenges of data protection as they were addressed before in this chapter. For this reason, consumer protection in Brazil is also regulated by the data protection law.

It is also important to remind that, from an international perspective, Brazil is part of the Santa Maria Protocol of the MERCOSUL which was signed in 1996 but not ratified. The Santa Maria Protocol was an initiative of the governments of Argentina, Brazil, Paraguay and Uruguay to address consumer rights on a common basis as part of the regional integration process. The objective of the negotiations was to make sure consumers in the MERCOSUL had the same level of protection and the same rights in all of the four countries. Diverging political interests have led to the stagnation of the process. Despite the failure of the Santa Maria Protocol, Brazil has signed the Montreal Convention on international carriage by air (1999) and the Warsaw Convention of 1929. Both treaties address the rights of consumers in specific questions of air transportation.

[121] See Presidência da República (1990).

[122] See Presidência da República (2013).

2.4. Cybercrime

Cybercrime, just as other forms of criminal activity, needs to be approached in an objective manner to avoid sensationalist portrayals of illicit actions, as it is common in Brazilian media outlets. The securitizing discourse on criminal activities, hardly ever accompanied by a more profound analysis, can be observed in Brazilian media outlets also when it comes to cyber or online delicts. Headlines showing high numbers of leaked data sets and large amounts of financial losses for national economies are the pictures that call attention and generate clicks on the Internet. However, compared to 2014, the 2018 data of CERT.br show an impressive reduction of cybersecurity incidents[123], including mostly scans (taken as a preparation for future attacks), denial of service attacks, malware, fraud, invasions and others[124]. The numbers impress even more taking into consideration the parallel increase of Internet users in the country. Nevertheless, cybercrime continues to be a serious challenge on the Internet and Brazilian networks continue to be home to both victims and perpetrators of illicit online activities.

Different from the data protection law LGPD, the Brazilian cybercrime law (n. 12.737/2012) addresses only a reduced number of issues that are commonly related to cybercrime[125]. In fact, in its merely 4 articles this 2012 law focuses mostly on the invasion of IT devices, the interruption of telecommunication and similar services, plus the falsification of bank and credit cards. Considering the comprehensiveness of cybercrime activities, this law covers just a small portion of what cybercrime analysts and investigators are confronted with on a daily basis. The fact that the law also carries the name of a Brazilian celebrity whose very personal data (private photos) were leaked in the year the document was signed shows the level of public sensitivity (or the lack thereof) that accompanied the debate on the cybercrime law[126]. A law that was supposed to protect victims of specific online crimes became a symbol for double victimization.

Besides the cybercrime law, online crimes in Brazil are also addressed by the Penal Code[127], the Child Protection Law[128], the *Marco Civil Internet*[129] and the above-mentioned Data Protection Law. This makes cybercrime an issue whose means of investigation are (at least on the legal basis) widely dispersed. Since no dedicated law extensively approaches the topic on a more profound level, no definitions of terms focusing exclusively on the realms of cybercrime can be found in the Brazilian legislation. In an additional law (12.735/2012), also known as Azeredo Law[130], the creation of

123 See CERT.BR (2018).

124 See CERT.BR (2018).

125 See Presidência da República (2012).

126 See Israel, E. (2013).

127 See Presidência da República (1940).

128 See Presidência da República (1990).

129 See Presidência da República (2014).

130 See Presidência da República (2012).

cybercrime police units was demanded in 2012. So far, at least 16 of those units were established in different parts of the country.

On the international level, Brazil supported the 2010 Salvador Declaration on Crime Prevention[131] developed by the respective United Nations congress, which partly addressed cybercrime challenges. However, Brazil has refused to sign the Budapest Convention on Cybercrime[132], which was presented in 2001 by the Council of Europe and a number of partner governments from different regions in the world.

The Budapest Convention is often considered to be the only large international treaty to address cybercrime. However, having been developed by the Council of Europe, it has been criticized for being a regional and not an international or global initiative. In an official statement submitted to the UN in May 2015, Brazil gave preference to the negotiations of an international treaty on cybercrime within the United Nations, as a legitimate body representing all countries in the world. Mutual legal assistance agreements and other forms of cooperation were mentioned in this context by Brazilian official representatives as important aspects for such an international treaty, while the definition of individual types of cybercrime should be left to domestic legislation. In the statement, Brazil also underlined the importance of respect for human rights and privacy in this matter[133].

2.5. Public Order

In Brazil, matters of public order are addressed in national security laws that were developed in several iterations, since 1935. These laws were and still are (in a current edition) directed at crimes against the state and political or social order. Since they were developed years or decades before the first Internet connection was established in the country and at times when also computer crimes in their early stages were unknown to most lawmakers in the world, there is hardly any connection between these laws and the challenges of the digital age.

One of the few aspects that could be interpreted as addressing digital challenges of the 21st century are those articles mentioning means of communication. Article 27 of the 1953 law (1.802/1953) prohibits the use of communication devices with the objective of endangering national defence of the country. Other passages can be found in the 1983 national security law (7.170/1983), where article 13 prohibits espionage and article 15 the sabotage of communication media. However, none of these laws is explicitly addressing questions of public order in a digital age, they are the reflection of times in which non-democratic and authoritarian governments attempted to suppress political opposition in the country. A

131 See United Nations (2010).

132 See United Nations (2015).

133 Ibidem.

clear mark of this is the fact that, to this day, the courts of military justice are responsible for judging the crimes mentioned in these laws.

While not explicitly addressed in the national security law, public surveillance measures can also be considered as part of the public order section. Besides the fact that Brazilian police is frequently filming political manifestations and also individuals in public places during daily controls, there is a large number of surveillance cameras installed in public and private environments that are taken with indifference by large parts of the population. Almost all residential, commercial and administrative buildings are equipped with cameras from the entrance to the elevators and on the individual floors and corridors. Also, public transportation busses, train stations and trains are equipped with cameras. The public and private investment in these and similar measures has created space for an industry of security companies and providers of the respective technologies.

Institutions and organizations installing surveillance cameras need to take into consideration, for example, the protection of privacy and intimacy as declared in article 5 of the Brazilian constitution. Once the data protection law comes into effect in August 2020, the debates on personal data captured by surveillance cameras are likely to intensify as well.

In addition to conventional surveillance cameras, Brazilian public administration has recently shown increased interest in facial recognition technologies. Following initial reports of the Brazilian non-governmental organization Instituto Igarapé, the country has been experimenting and using facial recognition devices since the year 2011[134]. This tendency has increased since the year 2018 with a focus on public security and transportation. According to reports of the organization, at least 37 of the roughly 5500 municipalities in the country have used facial recognition technologies in the year 2019[135]. Since these are initial reports mostly based on individual observations in capitals and a few additional larger cities in the country, it is very likely that more rigorous research would result in higher numbers.

2.6. Cyberdefence

The Brazilian debates on cyberdefence are primarily focused on the question of national defence under the management of the military and the Ministry of Defence. Discussing cybersecurity in this context often requires ignoring large parts of the legal understanding as provided in this book and instead orienting oneself toward the studies of national security in a classical sense as it appears in the studies of International Relations and Security Studies. Although cybersecurity in the context of traditional security studies could include different academic approaches, this is (so far?) hardly the case in Brazil. Since the 2011 web defacement attacks on a number of Brazilian public servers, taking

[134] See Instituto Igarapé (2019).

[135] See J. Valente (2019).

a larger number of ministries, public services and local governments offline for several hours[136], the interest in cyberdefence research has increased in the country. Especially in the academic fields of Political Science and International Relations an increase in publications on the topic can be observed, partly stimulated by the Pró-Defesa Program of the Ministry of Defence[137], in cooperation with the CAPES research foundation of the Ministry of Education[138].

Besides the academic work, a number of policy documents were published in Brazil over the past decade, which are partly or entirely focusing on cyberdefence , even before the incidents of 2011. An important initial step was the mentioning of cyberspace (or the "cybernetic sector") in the 2008 National Defence Strategy (which was republished as an updated version in 2012[139]). In this document, the "cybernetic sector" was defined as one of the new crucial areas to be included in the strategic planning of the Ministry of Defence[140]. Also important, although not further developed into a broader strategy, was the 2010 Greenbook on Cybersecurity published by the Presidency of the Republic[141]. It can be read as a first attempt to address a number of security challenges and opportunities in cyberspace. The year after the web defacement attacks, the Ministry of Defence published the updated version of the 2008 National Defence Strategy plus two further documents crucial for the debates on cyberdefence , being the White Book of National Defence[142] and the Cyberpolicy of Defence (*Política Cibernética de Defesa*)[143].

In the White Book of National Defence, the newly established focus on the "cybernetic sector" received further attention underlining, amongst others, the necessity of capacity building, intelligence, scientific research, and doctrines[144]. It is, as its title indicates, a broader document touching on a wider number of topics of which cyberdefence is just one that, however, is listed high on the ranking of priorities for the coming years[145]. The Cyberpolicy of Defence, on the other hand, is exclusively focussing on the topic of cyberdefence . At the beginning of the document, it is pointed out that successful cooperation requires measures of collaboration between different actors of Brazilian society like the Ministry of Defence, the academic community, the public and the private sector, including the

136 See D. Oppermann (2014).

137 See Pró-Defesa Program: <https://www.defesa.gov.br/ensino-e-pesquisa/defesa-e-academia/pro-defesa>.

138 A deeper analysis of the academic literature on the topic is currently under development at the ECEME University of Rio de Janeiro and will be published in early 2020.

139 See Ministério da Defesa (2012a).

140 Id., p. 32f.

141 See R. Mandarino Jr. e C. Canongia (2010).

142 See Brasil (2012).

143 See Ministério da Defesa (2012b).

144 See Brasil (2012:69).

145 Id., p. 197.

defence industry[146]. Just as mentioned in the White Book before, the proposed policy also stresses the importance of capacity building to develop efficient measures of cyberdefence . It furthermore underlines the importance of including all three forces (army, navy and air force) into strategic planning for cyberdefence research and development, and announces the objective to define basic principles for the respective regulatory development processes.

Two years after the publication of the Cyberpolicy, the Brazilian Ministry of Defence presented the first Military Doctrine on Cyberdefence . In a more comprehensive manner than the previous documents, the doctrine approaches cyberdefence defining different levels of decision making from the office of the President over the Ministry of Defence to the operational and tactical levels of the armed forces. To develop a clearer understanding of different elements and terms of cyberdefence , the doctrine offers a larger number of definitions including cyberdefence , cyberspace, cyberwar, critical infrastructure and more[147]. Among the possibilities of cyberdefence the document lists three types of actions, these being offensive, defensive and exploratory measures, and does point out that active measures can be taken against stronger opponents as well. The activation of cyberdefence measures depends on the level of cyber alerts ranging in 5 stages from white to red, whereas white is defined as “normal situations” in cyberspace and red describing scenarios of high impact damages caused on national critical infrastructure.

2.7. Conclusion

Defining cybersecurity is a challenging task that requires taking into consideration a number of dimensions and perspectives from diverse academic areas. In an attempt to look at the topic by splitting it up into a number of subcategories this chapter gave a broad overview of recent developments in Brazil regarding data protection, cybercrime, protection of public order, cyberdefence and consumer protection.

Among these areas, two stand out: data protection and cyberdefence . While the remaining areas are of no less importance, the two leading categories are marked by more extensive policy development processes that have resulted in a comprehensive data protection law which will come into force in August 2020, and in a number of policy documents on cyberdefence , mostly developed by the Ministry of Defence. The web defacement attacks mentioned earlier in this chapter should not be considered a trigger for the development of Brazilian cyberdefence strategy documents, since at that moment they were already in preparation. It is, however, one of the coincidences in history that took place in a specific moment to convince even the last sceptics about the necessity of addressing cybersecurity and cyberdefence on a higher governmental level.

[146] See Ministério da Defesa (2012b:11).

[147] See Ministério da Defesa (2014).

What has to come next is the realization of what is written, for example, in the strategy papers of the Ministry of Defence: giving special focus to capacity building on a higher level, plus the creation of more flexible career models to attract highly capable professionals into strategic positions in the military and in other critical areas. However, to improve the overall situation, efforts have to be made on all levels of education, starting with the youngest Internet users who need to learn the basics of data protection and secure online behaviour already as early as in fundamental school.

Public investment has to be directed to train students and parents of all income levels about safe online behaviour. Although important steps have been taken, there is still an enormous lack of awareness within the user community regarding all types of secure online conduct including the handling and sharing of personal data. Research organizations like CAPES and CNPq need to receive an extensive budget to finance research and development projects in the area, and the private sector needs to invest in capacity building of employees, especially those frequently in contact with client and user data. These are some but certainly not all measures that need to be taken in Brazil to create a more secure environment in which users can access the Internet with less concern.

2.8. References

Agência Senado (2019). Lei que cria Autoridade Nacional de Proteção de Dados é sancionada com vetos. 09 julho 2019. <https://www12.senado.leg.br/noticias/materias/2019/07/09/lei-que-cria-autoridade-nacional-de-protecao-de-dados-e-sancionada-com-vetos>. Accessed 12 Sep 2019.

Bezerra, M. & Araújo, E. (2011). Reflexões epistemológicas no contexto do Orkut: ética da informação, sociabilidade, liberdade e identidade. Perspectivas em Ciência da Informação, 16(2), 50-66.

Brasil (2012). Livro Branco de Defesa Nacional. Brasil. <https://www.defesa.gov.br/estado-e-defesa/livro-branco-de-defesa-nacional>. Accessed 12 Sep 2019.

Caram, B. & Fernandes, T. (2018). Temer sanciona lei de proteção de dados e veta autoridade fiscalizadora. Folha de São Paulo. 14 Aug 2018. <https://www1.folha.uol.com.br/mercado/2018/08/temer-sanciona-lei-de-protecao-dados-e-veta-autoridade-fiscalizadora.shtml>. Accessed 12 Sep 2019.

CERT.BR (2018a). Estatísticas dos Incidentes Reportados ao CERT.br. <https://www.cert.br/stats/incidentes/>. Accessed 12 Sep 2019.

CERT.BR (2018b). Incidentes Reportados ao CERT.br. Janeiro a Dezembro de 2018. <https://www.cert.br/stats/incidentes/2018-jan-dec/tipos-ataque.html. Accessed 12 Sep 2019.

CETIC.BR (2018). TIC Domicílios 2018. Indicador C2A. Usuários de Internet. <https://cetic.br/pesquisa/domicilios/indicadores>. Accessed 12 Sep 2019.

Instituto Brasileiro de Geografia e Estatística (2019). Estimativas da População. <https://www.ibge.gov.br/estatisticas/sociais/populacao/>. Accessed 12 Sep 2019.

Instituto Igarapé (n.d.). Reconhecimento Facial no Brasil. Instituto Igarapé Website. <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>. Accessed 30 Sep 2019.

Mandarino Jr., R. & Canongia, C. (2010). Livro Verde: Segurança Cibernética no Brasil. Presidência da República. Gabinete de Segurança Institucional. Secretaria Executiva. Departamento de Segurança da Informação e Comunicações. <http://www.biblioteca.presidencia.gov.br/presidencia/dilma-vana-rousseff/publicacoes/orgao-

essenciais/gabinete-de-seguranca-institucional/livro-verde-seguranca-cibernetica-no-brasil/view>. Accessed 12 Sep 2019.

Ministério da Defesa (2012a). Estratégia Nacional de Defesa. 2a ed. Brasil. <https://www.defesa.gov.br/estado-e-defesa/estrategia-nacional-de-defesa>. Accessed 12 Sep 2019.

Ministério da Defesa (2012b). Política Cibernética de Defesa. MD31-P-02. 1a ed. Brasil. <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf>. Accessed 12 Sep 2019.

Ministério da Defesa (2014). Doutrina Militar de Defesa Cibernética. MD31-M-07. Brasil. <https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf>. Accessed 12 Sep 2019.

NIC.BR (2018). Survey on the use of information and communication technologies in Brazilian households: ICT households 2017. São Paulo: Comitê Gestor da Internet no Brasil, 2018. <https://cetic.br/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2017/>. Accessed 18 Sep 2019.

Oppermann, D. (2014). Internet Governance and Cyber Security in Brazil. Multilateral Security Governance, KAS, Rio de Janeiro, 167–181. <https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_39113_2.pdf>. Accessed 12 Sep 2019.

Presidência da República (1940). Casa Civil. Subchefia para Assuntos Jurídicos. Código Penal. Law 2848. 07 Dec 1940. <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Accessed 12 Sep 2019.

Presidência da República (1990a). Casa Civil. Subchefia para Assuntos Jurídicos. Estatuto da Criança e do Adolescente. Law 8069. 13 Jul 1990. <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Accessed 12 Sep 2019.

Presidência da República (1990b). Casa Civil. Subchefia para Assuntos Jurídicos. Proteção do Consumidor. Law 8078. 11 Sep 1990. <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Accessed 12 Sep 2019.

Presidência da República (2012a). Casa Civil. Subchefia para Assuntos Jurídicos. Law 12735. 30 Nov 2012. <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Accessed 12 Sep 2019.

Presidência da República (2012b). Casa Civil. Subchefia para Assuntos Jurídicos. Law 12737. 30 Nov 2012. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Accessed 12 Sep 2019.

Presidência da República (2013). Casa Civil. Subchefia para Assuntos Jurídicos. Decree 7962. 15 Mar 2013. <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm>. Accessed 12 Sep 2019.

Presidência da República (2014). Casa Civil. Subchefia para Assuntos Jurídicos. Marco Civil da Internet. Law 12965. 23 Apr 2014. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Accessed 12 Sep 2019.

Presidência da República (2018). Secretaria-Geral. Subchefia para Assuntos Jurídicos. Lei Geral de Proteção de Dados Pessoais (LGPD). 14 Aug 2018. <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Accessed 12 Sep 2019.

Israel, E. (2013). Brazil aims to bring order to lawless cyberspace. Reuters. 26 Feb 2013. <https://www.reuters.com/article/brazil-cyberfraud/brazil-aims-to-bring-order-to-lawless-cyberspace-idUSL1N0BP52J20130226>. Accessed 04 Nov 2019.

Sales, S. & Paraíso, M. (2010). Escola, Orkut e juventude conectados: falar, exibir, espionar e disciplinar. Pro-Posições, 21(2), 225-242.

Silva, R.; Nichel, A.; Martins, A. & Borchardt, C. (2011). Discursos de ódio em redes sociais: jurisprudência brasileira. Revista Direito GV, 7(2), 445-468.

United Nations (2010). Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World. n.d. <https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf>. Accessed 10 Oct 2019.

United Nations (2015). Non-paper submitted by Brazil reflecting its views on the issue of cybercrime. Commission on Crime Prevention and Criminal Justice. E/CN.15/2015/CRP.5. 18 May 2015. <https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_24/ECN152015_CRP5_e_V1503408.pdf>. Accessed 30 Sep 2019.

Valente, J. (2019). Tecnologias de reconhecimento facial são usadas em 37 cidades no país. Agência Brasil. 19/09/2019. <http://agenciabrasil.ebc.com.br/geral/noticia/2019-09/tecnologias-de-reconhecimento-facial-sao-usadas-em-37-cidades-no-pais>. Accessed 12 Sep 2019.

Annex

Country Report: Brazil

1. Data Protection

▪ Scope

1. What national laws (or other types of normative acts) regulate the collection and use of personal data?

The collection and processing of personal data is regulated by the Brazilian General Data Protection Law – LGPD (n. 13.709/18). But it is also important to note that such law is embedded in a set of rules that address, at least in some respect, issues relating to privacy and protection of personal data, as the following:

- General Telecommunications Law (Federal Law n. 9,472 of 1997)
- Criminal Identification Law (Federal Law n. 12,037 of 2009)
- Freedom of Information Act (Federal Law n. 12,527 of 2011)
- Civil Rights Framework for the Internet (Federal Law n. 12,965 of 2014).

2. Is the country a part of any international data protection agreement?

Brazil is not part of any international data protection agreement.

3. What data is regulated?

The LGPD regulates personal data (online and offline).

[Art. 1, Art. 3]

4. Are there any exemptions?

The law does not apply when data is treated by natural persons for private and non-economic interests.

The law does not apply when data is treated for the following reasons or interests: journalists, artistic, academic, public security, national defence, state security, criminal investigation/repression.

[Art. 4]

5. To whom do the laws apply?

The LGPD will apply to all natural persons or legal entities incorporated or doing business in Brazil that collect personal data about Brazilian nationals. They will have to comply with the new law, as long as:

- The processing operation is carried out in Brazil;

- The purpose of the processing activity is to offer or provide goods or services, or the processing of data of individuals located in Brazil;
- The personal data was collected in Brazil.

The law will not apply to data processing:

- Carried out by a natural person exclusively for private and non-economic purposes;
- Performed for journalistic, artistic or academic purposes;
- Carried out for purposes of public safety, national security and defence or activities of investigation and prosecution of criminal offenses (which will be regulated by specific legislation);
- Originated outside the Brazilian territory and are not the object of communication; Shared data use with Brazilian processing agents or the object of international transfer of data with another country that is not the country of origin, as long as the country of origin offers a level of personal data protection adequate to that established by LGPD.

[Art. 3]

6. Do the laws apply to foreign entities that do not have physical presence in the country?

The law applies to any natural or legal person, irrespective of their location, whenever:

- Processing is done in Brazilian territory;
- The processing activity aims at offering goods, services or data processing to individuals located in the country; or
- The personal data used in the processing activities have been collected in national territory.

[Art. 3]

▪ Definitions

7. How are personal data defined?

Personal data are defined as information related to an identified or identifiable natural person.

[Art. 5]

8. Are there special categories of personal data (e.g. sensitive data)?

A specific classification is made for sensitive personal data being information related to specifically defined categories like race, ethnicity, religion, political orientation or activities and others. There is also a classification for anonymized data, which is defined as data relating to an data subject who cannot be identified, considering the use of reasonable technical means available at the time of the processed thereof.

[Art. 5]

9. How is the data controller and the data processor/operator defined?

A data controller is a natural or legal person governed by public or private law, responsible for taking decisions on the processing of personal data.

A data operator is a natural or legal person governed by public or private law, executing the processing of personal data in the name of the data controller.

[Art. 5]

10. What are the data protection principles and how are they defined?

The LGPD law lists the following data processing principles.

Purpose limitation: realisation of data processing for intentions that are legitimate, specific, explicit and with knowledge of the data subject, without the possibility of a later processing that does not consistent with these objectives;

Appropriateness: compatibility of the processing in accordance with the objectives informed to the data subject, in consistence with the context of the processing;

Necessity: limitation of the processing to the necessary minimum to achieve the objectives, covering the specific data in a proportional but not excessive manner in relation to the objectives of the data processing;

Free access: the guarantee for the data subject to easily and freely receive information regarding the manners and period of the processing, just as regarding the integrity of its personal data.

Data quality: the guarantee for the data subject regarding accuracy, clarity, relevance and actualisation of the data, according to the necessity and the compliance of the objectives of the processing;

Transparency: the guarantee for the data subject regarding clear, precise and easily accessible information about the data processing, about the respective agents of the process and the respect for commercial and industrial secrets;

Security: the utilisation of technical and administrative measures to protect personal data against unauthorised access and accidental or illicit situations of destruction, loss, alteration, communication of diffusion;

Prevention: adoption of measures to prevent the occurrence of harm in the context of personal data processing;

Non-discrimination: the impossibility of realizing data processing for discriminatory, illicit or abusive objectives;

Responsibility and accountability: a demonstration of the agent regarding the adoption of efficient measures to prove the compliance of personal data protection norms and of the efficiency of those measures;

[Art. 6]

11. Does the law provide any specific definitions with regards to data protection in the digital sphere?

Yes, the law defines database as structured set of personal data, established in one or several sites, in electronic or physical support.

[Art. 5]

12. Is the data protection law based on fundamental rights (defined in Constitutional law or International binding documents)?

Yes, article 2 of the data protection law refers to fundamental rights, including (but not limited to) privacy, freedom of expression, free initiative and human rights.

13. What are the rights of the data subjects according to the law?

Data subjects have the right to receive facilitated access to information regarding the treatment of their personal data.

Article 9 of the data protection law states the manner this information has to be provided including information on the objectives of the process, its duration, the identification of controllers and its contact information, information regarding data sharing, the responsibilities of the processing agents and the rights of the data subject.

Art. 17: Every natural person is assured ownership of her/his personal data, with the fundamental rights of freedom, intimacy and privacy being guaranteed, under the terms of this Law;

Art. 18: The personal data subject has the right to obtain the following from the controller, regarding the data subject's data being processed by the controller, at any time and by means of request:

I – confirmation of the existence of the processing;

II – access to the data;

III – correction of incomplete, inaccurate or out-of-date data;

IV – anonymisation, blocking or deletion of unnecessary or excessive data or data processed in noncompliance with the provisions of this Law;

V – portability of the data to another service or product provider, by means of an express request and subject to co-regulation of the controlling agency;

VI – deletion of personal data processed with the consent of the data subject, except in the situations provided in Art. 16 of this Law;

VII – information about public and private entities with which the controller has shared data;

VIII – information about the possibility of denying consent and the consequences of such denial;

IX – revocation of consent as provided in §5 of Art. 8 of this Law.

§1 The personal data subject has the right to petition, regarding her/his data, against the controller before the national authority.

§2 The data subject may oppose the processing carried out based on one of the situations of waiver of consent, if there is noncompliance with the provisions of this Law.

§3 The rights provided in this article shall be exercised by means of express request by the data subject or her/his legally constituted representative to the processing agent.

§4 If it is impossible to immediately adopt the measure mentioned in §3 of this article, the controller shall send a reply to the data subject in which she/he may:

I – communicate that she/he is not the data processing agent and indicate, whenever possible, who the agent is; or

II – indicate the reasons of fact or of law that prevent the immediate adoption of the measure.

§5 The request as mentioned in §3 of this article shall be fulfilled without costs to the data subject, within the time periods and under the terms as provided in regulation.

§6 The responsible shall immediately inform the processing agents with which she/he has carried out the shared use of data of the correction, deletion, anonymisation or blocking of data, so that they can repeat an identical procedure.

§7 The portability of personal data referred to in Item V of the lead sentence of this article does not include data that have already been anonymised by the controller.

§8 The right referred to in §1 of this article may also be exercised before consumer-defence entities.

Art. 19: Confirmation of the existence of or access to personal data shall be provided by means of request by the data subject:

I – in a simplified format, immediately; or

II – by means of a clear and complete declaration that indicates the origin of the data, the nonexistence of record, the criteria used and the purpose of the processing, subject to commercial and industrial secrecy, provided within a period of fifteen (15) days as from the date of the data subject's request.

§1 Personal data shall be stored in a format that facilitates the exercise of the right to access.

§2 Information and the data may be provided, at the data subject's discretion:

I – by an electronic mean that is safe and suitable to this purpose; or

II – in printed form.

§3 When processing originates from the consent of the data subject or from a contract, the data subject may request a complete electronic copy of her/his personal data, subject to commercial and industrial secrecy, in accordance with regulations of the national authority, in a format that allows its subsequent use, including for other processing operations.

§4 The national authority may provide differently regarding the time periods provided in Items I and II of the lead sentence of this article for specific sectors.

Art. 20: The data subject has the right to request review of decisions taken solely on the bases of automated processing of personal data that affects her/his interests, including decisions intended to define her/his personal, professional, consumer or credit profile or aspects of her/his personality.

§1 Whenever requested to do so, the controller shall provide clear and adequate information regarding the criteria and procedures used for an automated decision, subject to commercial and industrial secrecy.

§2 If there is no offer of information as provided in §1 of this article, based on commercial and industrial secrecy, the national authority may carry out an audit to verify discriminatory aspects in automated processing of personal data.

Art. 21: Personal data concerning the regular exercise of rights by the data subject cannot be used to her/his detriment.

Art. 22: The defence of the interests and rights of data subjects may be carried out in court, individually or collectively, as provided in pertinent legislation regarding the instruments of individual and collective protection.

- **Obligations and Sanctions**

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

Controllers need specific additional consent of the data subject before sharing their data with other controllers.

[Art. 7, I and par 5]

The controller has the responsibility to prove that consent was given by the user to process their data.

***[Art. 8, par* 2]**

The controller needs to inform the data owner/subject regarding specific changes which are defined in Art 9 (e.g. objectives and means of data processing, identification of controller etc.). The data subject has the right to not accept the changes and withdraw his consent.

[Art. 8, par 6; Art. 9, par 2]

The controller can only process data for legitimate objectives as defined in Art 10 (e.g. promotional and service activities). In this context, processing is limited to those data which are necessary for the specific objective. The controller must adopt measures to guarantee transparency during the processing of data.

[Art. 10]

Controllers are not allowed to share or communicate sensitive personal health care data with other controllers without consent of the data subject.

[Art. 11, par. 4]

Controllers are obligated to have the consent of at least one parent or another legally responsible person before treating data of children (Art 14, par 1 and 5). In this context, controllers have to inform what data are collected, how they are used. This information has to be provided by the controller in a simple and clear manner to meet the needs and specific context and intellectual level of understanding of the users. This can include audiovisual means.

[Art. 14, par. 6]

Exceptions are made in case data collection is necessary to protect children or to contact parents or legally responsible persons.

[Art. 14, par. 3]

Controllers are not allowed to set access to personal data as a condition to children accessing games, Internet applications or other activities, unless the data is necessary to provide their services.

[Art. 14, par. 4]

Personal data is to be deleted by the controller when data processing is completed. Exceptions can be defined by legal or regulatory obligations, in the case of research organizations (which are obliged to keep personal data anonymous if possible), data transfers to third-parties or exclusive use by the controller (anonymization required).

[Art. 16]

When requested by the data subject, the controller has to inform the data subject about the existence of data treatment processes, to give access to the data, to correct incomplete or outdated data, to anonymize, block or delete data unnecessary or excessive data or data treated disrespecting the legal requirements. The controller must provide the data to other controllers if requested by the data subject. He has to delete personal data (unless deleting would interfere with other legal requirements), to inform the data subject about third controllers who received access to the data and to inform the data subject about the possibilities of not giving consent including possible consequences regarding this decision. Furthermore, controllers must inform data subjects about the right to withdraw consent upon request by the data subject.

[Art. 18]

The data subject can hand in complaints at no charge about data controllers at the national data authority or consumer protection agencies.

[Art. 18, par.]

The controller has the right to respond to complaints by the data subject at the national authority.

[Art 18]

The data subject has the right to request a review of decisions taken exclusively based on automated personal data treatment if the treatment affects his interests, including the definition of personal, professional, financial or consumer profiles;

Whenever requested by the data subject, the controller has to provide clear information regarding criteria and processes of automated decisions;

If the data controller does not provide the information the national data authority can investigate the controller.

[Art. 20]

The defence of the interests and rights of the data subject may be exercised in court, individually or collectively, in the form of the provisions of the applicable law, about the instruments of individual and collective protection.

[Art. 22]

The controller and the operator must store records of personal data treatment conducted by them.

[Art. 37]

If requested by the national data authority the controller has to report on his data protection procedures.

[Art. 38]

The operator has to conduct data processing as instructed by the controller.

[Art 39]

The controller has to nominate a person responsible for personal data treatment and communication with data subjects and national authorities. The controller has to provide the public with name and contact of this person (e.g. on his website). The person is also responsible for informing employees and partners of the controller regarding personal data protection procedures.

[Art. 41]

The controller and the operator are responsible to compensate for individual, collective, moral and patrimonial harm caused by personal data treatment.

[Art. 42]

The controller has to inform the national data authority and the data subject in case of security incidents that could cause harm to the data subject. Article 48 defines further details of this procedure.

[Art. 48]

The national data authority has to verify the seriousness of security incidents and if necessary take measures to inform the public and to reduce damage.

[Art 48, par. 2]

15. Is notification to a national regulator or registration required before processing data?

In specific situations, notification to a national regulator is required. This includes data transfer from public to private actors ***[Art. 26 par. 2]*** and modifications of specific procedures for international data transfers ***[Art. 36].***

16. Does the law require privacy impact assessment to process any category of personal data?

The law establishes that the national authority may require the controller to prepare a data protection impact assessment, including sensitive data, relating to its data processing operations, as provided for by the regulations, with due regard for trade and industrial secrets. The report shall contain at least a description of the types of data collected, the methodology used for collection and as guarantee of security of the information, and an analysis of the controller in relation to the measures,

safeguards and risk mitigation mechanisms adopted.

[Art. 38]

17. What conditions must be met to ensure that personal data are processed lawfully?

- The legal bases for data processing are: receiving consent from the data subject;
- To fulfil legal or regulatory requirements by the controller;
- For public administration to execute public policies;
- For the realisation of studies conducted by research organs;
- For the execution of contracts;
- For the execution of legal processes;
- To protect the life of data subjects and other individuals;
- To enable specific health care activities;
- To attend legitimate interests of controllers or others; or
- For credit protection.

[Art. 7]

18. What are the conditions for the expression of consent?

Consent has to be given in a written or any other form that expresses the agreement of the data subject. The controller is obligated to prove that consent was given. The consent has to refer to specific objectives. Consent can be cancelled at any moment by the data subject.

[Art. 8]

19. If the law foresees special categories of data, what are the conditions to ensure the lawfulness of processing of such data?

There are specific requirements for the treatment of sensitive personal data. This procedure can lawfully occur when the data subject or a legal representative gives consent to the specific objectives of the process. Exceptions are made in a number of cases, among them legal necessities of controllers and of public administration, for the purpose of research and medical treatment, for security reasons, and others.

[Art. 11]

20. What are the security requirements for collecting and processing personal data?

Data processing actors have to establish security measures to protect personal data. The national authority can define technical security standards for data processing actors.

[Art. 46]

Data processing actors are obliged to guarantee security for personal data during and after processing them.

[Art. 47]

The controller has to inform the national authority and the data subject in case of security incidents that could cause relevant harm to the data subject.

In this context, the controller has to provide information including the nature of the affected data, the affected data subjects, the data protection measures taken, the risks related to the incident, an explanation in case of delayed communications, and the measures taken to solve the situation.

The national authority will analyse the incident and, if necessary, take measures to protect the rights of the data subject. This can include (but is not limited to) a public announcement of the incident and measures to reduce harm caused by the incident.

[Art. 48]

21. Is there a requirement to store (certain types of) personal data inside the jurisdiction?

There is no such requirement.

22. What are the requirements for transferring data outside the national jurisdiction?

The transfer of data to outside the national jurisdiction is allowed in case the receiving country or organization offers adequate data protection measures as provided by the Brazilian law. The data controller has to provide guarantees to comply with the principles and the rights of the data subject and the data protection regime of the law.

In specific cases, international data transfer is allowed which includes international juridical cooperation, the protection of life, transfers authorized by the national authority, the compliance with international cooperation agreements besides others.

[Art. 33]

The level of data protection of the foreign entity is evaluated by the national authority.

[Art. 34]

23. Are data transfer agreements foreseen by the law?

Yes, the law has a chapter dedicated to international data transfer (Chapter V). Article 33 sets out the cases in which transfer is permitted, which are as follows:

I – to countries or international organizations that provide the appropriate level of protection of personal data provided for by the Brazilian Law.

II – where the controller provides and demonstrates guarantees of compliance with the principles, rights of the data subject and data protection regime established in the Brazilian Law.

III – where the transfer is required for international legal cooperation between government intelligence, investigation and police bodies, in accordance with the international law instruments.

IV – where the transfer is required for life protection or physical integrity of the data subject or any third party.

24. Does the relevant national regulator need to approve the data transfer agreements?

Yes, the national regulator needs to evaluate the level of data protection in the foreign country or entity.

[Art. 34]

25. What are the sanctions and remedies foreseen by the law for not complying with the obligations?

The data protection law provides a number of sanctions and remedies including warnings, fines, publication of the occurrences, the temporary blocking or deletion of personal data.

[Art. 52]

- **Actors**

26. What actors are responsible for the implementation of the data protection law?

The national authority called "Autoridade Nacional de Proteção de Dados" (ANPD) is responsible for the implementation.

[Art. 55]

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

The ANPD is being created by the Presidency of the Republic. It has a transitory nature: at first it will be a branch of Federal Government, but within two years it may be transformed into an independent Regulatory Agency

[Art. 55-A]

28. What are the powers of the actors responsible for the implementation of the data protection law?

ANPD has a series of powers, including oversight, elaborating guidelines and regulations, conducting or ordering audits, receiving complaints from data subjects against controllers, among others.

[Art. 55-J]

2. Consumer Protection

- **Scope**

29. What national laws (or other types of normative acts) regulate consumer protection?

Consumer protection is regulated by the Consumer Protection Law (*Código de Defesa do Consumidor*, 8078/1990). Decree 7962/13 is regulating electronic commerce.

30. Is the country a party of any international consumer protection agreement?

Brazil is part of the Santa Maria Protocol of the MERCOSUL which was signed in 1996 but not ratified, yet. Brazil has signed the Montreal Convention (international carriage by air) and the Warsaw Convention of 1929.

31. To whom do consumer protection laws apply?

The consumer protection law applies to physical person and corporate entity.

32. Do the laws apply to foreign entities that do not have physical presence in the country?

The law refers to foreign actors for example as producers or distributor ***[Art. 3, Art. 12]*** but has no specific reference to actors located outside the Brazilian jurisdiction.

- **Definitions**

33. How is consumer protection defined?

The law does not provide a definition of consumer protection.

34. How are consumers defined?

The law defines consumers as physical person and corporate entities who acquire products or services as final user.

35. How are providers and producers defined?

The law defines providers as physical person and corporate entities, public or private, national or foreign, who produce, assemble, create, construct, transform, import, export, distribute or commercialize products or services.

36. Does the law provide any specific definitions with regards to consumer protection in the digital sphere?

The law does not contain definitions regarding the digital sphere.

- **Rights**

37. Is the consumer protection law based on fundamental rights (defined in Constitutional law or International binding documents)?

Yes, the consumer protection law refers do articles 5, 48, 170 of the Brazilian Constitution.

38. What are the rights of the consumer defined by the law with reference to digital good and services?

The consumer protection law does not refer to rights of the consumer in reference to digital goods and services. However, decree 7962/13 (e-commerce law) states that consumers have the right to choose ***[Art. 4]*** and the right of withdrawal ***[Art. 5].***

39. Is consumer protection law applicable to users of zero price service i.e free of charges?

Neither the consumer protection law nor the decree on e-commerce refer to zero price services.

- **Obligations and Sanctions**

40. Does the law establish specific security requirements to provide digital services or goodies?

The consumer protection law does not refer to activities in the digital sphere. However, it does mention security aspects in a general sense. Therefore, products and services shall not present a

security issue for consumers ***[Art. 8]***. Providers have to inform consumers about potential security issues ***[Art. 9]***. Providers are not allowed to offer products or services that contain high security risks ***[Art. 10]***. Public authorities on all levels are obligated to inform consumers regarding security issues with products and services whenever they take notice. Decree 7962/13 on the regulation of electronic commerce states that commercial websites need to inform consumers on possible security risks of products and services ***[Art. 2]***. ***Article 4*** of the same decree demands providers to apply secure measures for payment options and consumer data processing.

41. What are the sanctions and remedies foreseen by the law for not complying with the obligations?

Article 56 of the consumer protection law specifies the following sanctions and remedies: fines; product confiscation; product destruction; confiscation of product licenses; prohibition of product manufacturing; suspension of product supply; temporary suspension of professional activities; suspension of permissions or concessions of usage; suspension of licences of establishments or activities; prohibition of establishments, constructions or activities; administrative interventions, imposition of counterstatements. The same article furthermore informs that other methods including criminal and civil prosecutions are possible.

▪ Actors

42. What bodies are responsible for the implementation of the consumer protection law?

Article 39 states that specific organs are responsible for technical product standards required to provide products and services, which includes Brazilian Technical Norms Association – ABNT or another entity accredited by the National Metrology, Normalization and Industrial Quality Council (Conmetro). ***Article 82*** of the consumer protection law defines the following bodies for being responsible for the implementation of consumer protection: Public Prosecution Service (*Ministério Público*), the Union, the states, the municipalities, the Federal District, different organs of public administration, consumer protection associations. ***Article 105*** specifies that the National System of Consumer Protection is made up of federal, state, and municipal organs, the Federal District, and private consumer protection entities. It furthermore lists the National Department of Consumer Protection (*Departamento Nacional de Defesa do Consumidor*) at the Ministry of Justice as the coordinating organ of national consumer protection.

43. Is there a specific consumer protection body? If so, what is its administrative structure?

Article 105 of the consumer protection law defines the **National Department of Consumer Protection** (Departamento Nacional de Defesa do Consumidor) at the Ministry of Justice as the coordinating organ of national consumer protection policies. This is the structure stipulated in the 1990 Consumer Code, but there have been changes over the years, such as the creation of the **National Consumer Secretariat (Senacon)** and the rebranded **Department of Consumer Protection and Defence .**

The **National Consumer Secretariat (Senacon),** created by Decree No. 7,738, of May 28, 2012, is part of the Ministry of Justice and its duties are established in art. 106 of the Consumer Protection Code, in art. 3 of Decree No. 2,181/97 and in art. 17 of Decree No. 9,662, of January 1, 2019, Annex I.

Structure:

- National Consumer Protection secretary;
- Chief of Staff;
- General Coordination of Administration, Budget and Finance;
- General Coordination of Articulation and Institutional Relations;
- National Council on Combating Piracy and Intellectual Property Crimes.

The **Department of Consumer Protection and Defence** has its competence established in art. 18 of Decree nº 9.662, of January 1, 2019, Annex I, with the following structure:

- Board of the Department of Consumer Protection and Defence ;
- General Coordination of Market Studies and Monitoring;
- General Coordination of Technical Consultancy and Administrative Sanctions;
- General Coordination of the National.

The National Consumer Secretariat is responsible for:

- Formulate, promote, supervise and coordinate the national consumer protection and defence policy;
- Integrate, articulate and coordinate the National Consumer Protection System;
- Articulate with federal public administration bodies with attributions related to consumer protection and defence ;
- Guide and coordinate actions for consumer protection and defence ;
- Prevent, investigate and prosecute violations of consumer protection rules;
- Promote, develop, coordinate and supervise actions to disseminate consumer rights, with a view to the effective exercise of citizenship;
- Promote actions to ensure the rights and interests of the consumer;
- Inspect and apply the administrative sanctions provided for in Consumer Defence Code, and in other rules relevant to consumer protection;
- Adopt measures to maintain and expand the national consumer protection information system and guarantee access to information;
- Receive and forward consultations, complaints or suggestions made by consumers, representative entities or legal entities governed by public or private law;
- Enter into agreements with public bodies and entities and with private institutions to execute plans and programs, in addition to acting in defence of compliance with federal rules and measures;

- Encourage, even with financial resources and special programs, the creation of state, district and municipal consumer protection agencies and the formation, by citizens, of entities with this objective;
- Enter into conduct adjustment commitments, as provided by law;
- Exercise the powers established in Consumer Defence Code;
- Elaborate and disclose the complementary list of contractual clauses and unfair practices, under the terms of Consumer Defence Code;
- Direct, guide and evaluate actions for training in consumer protection aimed at members of the National Consumer Protection System;
- Determine consumer market monitoring actions to support public consumer protection and defence policies;
- Request the collaboration of bodies and entities of notable technical-scientific specialization to achieve their objectives;
- Monitor regulatory processes, with a view to the effective protection of consumer rights; and
- Represent the Ministry of Justice in the participation in national and international bodies, forums, commissions and committees that deal with consumer protection and defence or with matters of interest to consumers, unless there is a specific designation of the Minister of State that provides otherwise.

44. What are the powers of the bodies responsible for the implementation of the consumer protection law?

Article 106 defines the following powers of the National Department of Consumer Protection:

- Planning, elaborating, proposing, coordinating, and executing national data protection policies;
- Receive, analyse, evaluate, and send consultations, incriminations or suggestions presented by representative entities or legal persons of public or private law;
- Advice consumers regarding rights and guaranties;
- Inform, raise awareness and motivate consumers through different means of communication;
- Request the initiation of police investigations in case of delicts against consumers;
- Inform responsible organs about infractions violating consumer interests
- Work with public prosecution to adopt procedural measures where necessary;
- Overseeing prices, supply, quantity and security of goods and services;
- Encourage the creation of consumer protection organisations by citizens and public entities on the state and municipality levels.

3. Cybercrime

▪ Scope

45. What national laws (or other types of normative acts) regulate cybercrime?

Brazil does not have a general cybercrime law, only the sparse prediction of several crimes that mention electronic means. These are the federal laws that establishes such crimes:

- Law 7.716/1989 (as amended by Law 9.459/1997, Law 12.288/2010, Law 12.735, 2012)
- Child and Adolescent Statute - Law 8.069/1990 (as amended by Law 11.829, of 2008)
- Law 9.296/1996 (as amended by Law 13.964/2019)
- Law 9.504/1997 (Electoral Law)
- Law 9.983/2000 (inserted in the Penal Code)
- Law 10.685/2003 (inserted in the Penal Code)
- Law 12.737/2012 (inserted in the Penal Code)
- Law 13.772/2018 (inserted in the Penal Code)

46. Is the country a part of any international cybercrime agreement?

Brazil has not signed any international cybercrime agreement.

47. What cybercrimes are regulated?

Law 7.716/1989 (as amended by Law 9.459/1997, Law 12.288/2010, Law 12.735, 2012) addresses the practice of neo-Nazism and measures to stop the disclosure of such crime content resulting from racial or color prejudice.

The Child and Adolescent Statute - Law 8.069/1990 (as amended by Law 11.829, of 2008) addresses pornographic material of children and adolescents and online sexual grooming.

Law 9.296/1996 (as amended by Law 13.964/2019) addresses illegal interception of communications.

Law 9.504/1997 addresses unauthorized access to electoral data systems.

The Penal Code (as amended by Law 9.983/2000) addresses false data entry into information system as well unauthorized modification or alteration of information system performed by public servant against public administration.

The Penal Code (as amended by Law 10.685/2003) addresses copyright infringement.

The Penal Code (as amended by Law 12.737/2012) addresses illicit access (hacking) of IT equipment and networks. This law also regulates the establishment of police units investigating cybercrime.

The Penal Code (as amended by Law 13.772/2018) addresses unauthorized record and disclosure of sexual intimacy.

48. To whom do the laws apply?

Only Law 9.983/2000 has a specific target, regulating crimes committed by public servants. All the other laws are applicable to all citizens.

▪ Definitions

49. Do the laws apply to foreign entities that do not have physical presence in the country?

The law does not address this question.

50. How is cybercrime generally defined by the national law?

The law does not address this question.

51. What are the cybercrimes provided for by the law and how are they defined?

The cybercrime law addresses illicit access to IT devices and electronic communications

52. How is a computer system defined?

Marco Civil da Internet defines "Terminal" as the computer or any device that connects to the Internet.

53. How are computer data defined?

The law does not address this question.

54. How are forensic data defined?

The law does not address this question.

55. How are service providers defined?

The law does not provide any specific definition of providers. However, Brazilian law (Marco Civil) deals specifically with two types of providers: Internet connection providers and Internet application providers.

56. Does the national law provide any other definitions instrumental to the application of cybercrime legislation?

The cybercrime law does not provide further definitions.

▪ Rights

57. Is the cybercrime law based on fundamental rights (defined in Constitutional law or International binding documents)?

The cybercrime law does not provide further definitions.

58. What are the rights of the victim and the accused?

Majorities of rights related to crimes are established in general legislation, such as the Penal Code and the Code of Criminal Procedure, and are applicable to all crimes, cyber or analog.

Nevertheless, the Child and Adolescent Statute states the following:

> *Art. 3. Without prejudice to the full protection treated of in this Law, the child and adolescent enjoy all the fundamental rights inherent to the human person and, by law or other means, are*

ensured of all opportunities and facilities so as to entitle them to physical, mental, moral, spiritual and social development, in conditions of freedom and dignity.

(...)

Art. 5. No child or adolescent will be subject to any form of negligence, discrimination, exploitation, violence, cruelty and oppression, and any violation of their fundamental rights, either by act or omission, will be punished according to the terms of the Law.

- **Procedures**

59. Is there a specific procedure to identify, analyse, relate, categorize, assess and establish causes associated with forensic data regarding cybercrimes?

The cybercrime law does not define any of these procedures.

60. In case of transnational crimes, how is cooperation between the national law enforcement agency and the foreign agents regulated?

Brazil (e.g. the Federal Police) is cooperating with foreign agents based on cooperation agreements including MLATs. In 2016, the Federal Police inaugurated the cooperation centre CCPI to enhance its international joint investigations.

61. Are there any exceptions to the use of mutual legal assistance procedure to investigate the crime?

The law does not address this question.

62. Does the national law require the use of measures to prevent cybercrimes? If so, what are they?

The law does not address this question.

- **Obligations and Sanctions**

63. What obligations do law enforcement agencies have to protect the data of the suspect, the accused and the victim?

The cybercrime law does not address this question. Further processes are defined in the data protection law.

64. What are the duties and obligations of the National Prosecuting Authorities in cases of cybercrime?

The law does not address this question.

65. Does the law impose any obligations on service providers in connection with cybercrime?

The law does not address this question.

66. To which extent can a legal person be held liable for actions in connection with cybercrimes?

The law does not address this question.

- **Actors**

67. What bodies implement the cybercrime legislation?

Brazil has established a number of cybercrime police agencies as defined in Law 12735/2012.

68. Is there a special public prosecutor office for cybercrime? If so, how is it organised?

The law does not address this question.

69. Does the cybercrime legislation create any specific body?

Law 12735/2012 has established cybercrime police agencies.

4. Public Order

- **Definitions**

70. How are public order, threats to public order and the protection of public order defined?

Law 7170/1983 (National Security Law) does not define any of those concepts.

71. Is the protection of public order grounded in constitutional norms?

The law falls under the rule of military justice.

- **Measures**

72. What cyber measures address threats to public order?

The law does not address this question.

- **Actors**

73. What public authorities are responsible for the implementation of surveillance techniques?

The law does not address this question.

74. What are the obligations of these public authorities?

The law does not address this question.

75. Can private actors be involved in the implementation of cyber measures to address threats to public order?

The law does not address this question. Generally speaking, private actors are providing technology and services to public institutions in Brazil.

5. Cyberdefence

- **Scope**

76. Is there a national cyberdefence strategy or is cyberdefence mentioned in the national defence strategy?

In 2012, Brazil has published Cyberdefence Policies (*Política Cibernética de Defesa*). In 2014, Brazil has published a Military Doctrine on Cyberdefence (*Doutrina Militar de Defesa Cibernética*).

77. What is the legal status of the national defence or cyberdefence strategy?

Both the Brazilian cyberdefence policy and the military doctrine are normative regulations (*portaria normativa*) issued by the Ministry of Defence.

78. What national laws or other normative acts regulate cyberdefence in the country?

Brazil has no specific law on cyberdefence . Other relevant documents are mentioned above.

79. Is the country party of any international cooperation agreement in the sphere of cyberdefence ?

Brazil is not part of international cyberdefence agreements.

80. Does the national cyberdefence strategy provide for retaliation?

Neither the cyberdefence policies, nor the military doctrine cover the topic of retaliation.

▪ Definitions

81. How are national security and national defence defined?

The 2012 National Defence Policies (*Política Nacional de Defesa*) define security as the condition that permits the country to preserve its sovereignty and territorial integrity, to promote its national interests, free of pressures and threats, and to guarantee its citizens the exercise of constitutional rights and obligations. In the same document, national defence is defined as the entirety of measures and activities of the state, focused on the field of the military, to defend territory, sovereignty, and national interests against potential or clear predominantly external threats.

82. How are cybersecurity and cyberdefence defined?

The 2012 military doctrine defines cybersecurity as the art of assuring the existence and continuation of a nation's information society, guaranteeing and protecting in cyberspace, its information assets and its critical infrastructure. The same document defines cyberdefence as the entirety of offensive, defensive, and exploratory actions realised in cyberspace, in the context of national and strategical planning coordinated and integrated by the Ministry of Defence, with the objective to protect the information systems of national defence, obtain data to produce intelligent knowledge, and to harm the opponent's information systems.

83. How are threats to national security and cyberthreats defined?

The military cyberdefence doctrine defines cyberthreats as potential events of an undesired incident which could harm interests in cyberspace.

84. How is a cyberattack defined?

The military cyberdefence doctrine defines cyberattacks as actions to interrupt, reject, degrade, corrupt or destroy information or computational systems stored on devices and computational and communication networks of an opponent.

85. Does the national law provide any other definitions instrumental to the application of cyberdefence legislation?

The military cyberdefence doctrine provides definitions for cyber artefacts, information assets, cybernetic, day-zero, operational dominions, cyberspace, cybersource, cyberwar, critical information infrastructure, critical infrastructures, information operation, cyber power, cyber resilience, cyber risk, information and communication security, cyber protection, cyber exploration.

▪ National Framework

86. Is cyberdefence grounded on the constitutional provisions and/or international law?

The military cyberdefence doctrine is based on the Brazilian constitution.

87. Which specific national defence measures are related to cybersecurity?

The military cyberdefence doctrine includes the following cyberdefence measures: offensive, defensive and exploratory actions in cyberspace, striking against opponents' critical infrastructure, different forms of cooperation to produce knowledge and intelligence (also with actors outside the Ministry of Defence), exploring weaknesses in opponents' information systems. Furthermore, the doctrine refers to cyberattacks (as defined above), cyber protection measures to neutralize attacks, and cyber explorations to collect data.

88. Is there a national defence doctrine and does the law or strategy refer to it?

Brazil has a military cyberdefence doctrine.

89. What measures are mentioned in the national law and strategy in order to implement cyberdefence ?

(see above)

90. How can Internet users' online activities be limited for the reasons of protection of national security and cyberdefence ?

No such measure is defined at this moment.

91. Does the national law or strategy foresee any special regime to be implemented in case of emergency in the context of cyberdefence ?

No such measure is defined at this moment.

92. Is there any specific framework regulating threats to critical infrastructure?

Decree 9573/18 is regulating national policies for critical infrastructure security.

Actors

93. What actors are explicitly mentioned as playing a role regarding cyberdefence in the law or national cyber defence strategy or defence strategy?

The overall responsible actor for cyberdefence is the Ministry of Defence. The military cyberdefence doctrine defines the armed forces to be the main actor responsible for cyberdefence . Also mentioned in the doctrine are the Office of the President, the Brazilian Internet Steering Committee (CGI), the Cyberdefence Centre (*Centro de Defesa Cibernética*, CDCiber), the CTIRs (*Centros de Tratamento de Incidentes de Redes*), CERT.br, CTIR Gov, ministries, governmental agencies (without further specification).

94. Is there a specific cyber defence body?

Following the military cyberdefence doctrine a number of public organs are establishing cyberdefence departments. At this moment, the CDCiber is the most elaborated cyberdefence body in Brazil.

95. What are the tasks of aforementioned actors?

CDCiber is responsible for observing and securing national networks, developing capacity building programs, conducting research and the development of security tools.

3. Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the "Sovereignization" of the Internet in Russia

Andrey A. Shcherbovich

This chapter discusses Russian governmental attitudes for regulation and governance of the Internet in terms of cybersecurity and, particularly, data protection. The analysis of these areas is extremely important for understanding the entire Internet governance framework in Russia.

Russian legislation in the field of information technologies and the Internet is constantly changing. One of the goals of this chapter is to reflect on the existing regulatory provisions and evaluate their effect on the fundamental rights of Internet users defined by the Constitution of the Russian Federation as well as by International Law on Human Rights.

Importantly, this chapter will stress that the principle of ensuring information security of the Russian Federation in the sphere of information systems, their operation and protection of the information is increasingly coming to the fore in the development of Internet governance in Russia. This subject becomes dominant in the development of new laws in the abovementioned areas. To a large extent, this trend can be associated with a general tendency towards the adoption of an ample range of restrictive measures, which were taken by Russia as well as against Russia by foreign nations, in connection with the conflict in Ukraine and the controversial international legal status of Crimea, annexed by Russia in 2014. In such context, Russian officials have been referring to the concept of the "digital" or "information" sovereignty of Russia to justify the proposal of restrictive legislative provisions[148].

To illustrate this tendency, we can consider the number of recent legislative initiatives aimed at regulating the behaviour of Internet users. Such initiatives include extrajudicial blocking of the web resources containing "extremist information"[149], legal provisions mandating the localization of the personal data, and the adoption of the Yarovaya law[150], which de-facto introduces takedown of user-generated content. All these initiatives could be linked with the general policy promoting the establishment of the "digital" or "information sovereignty" of Russia[151].

---

[148] See Transcript of the State Duma (2019). <http://transcript.duma.gov.ru/node/5115/>; A. Shcherbovich (2019), available at <https://cyberbrics.info/sovereign-internet-law-signed-by-the-president-of-russia/>.

[149] Federal Law of December 28, 2013 N 398-FZ "On Amendments to the Federal Law "On Information, Information Technologies and the Protection of Information" entered into force on February 1, 2014. // ConsultantPlus Legal Reference System.

[150] Federal Law of 06.07.2016 N 374-FZ "On Amendments to the Federal Law "On Countering Terrorism" and certain legislative acts of the Russian Federation regarding the establishment of additional counter-terrorism measures and ensuring public safety" // ConsultantPlus Legal Reference System.

[151] Saveliev A.I. Commentary to the Federal Law of July 27, 2006, No. 149-FZ "On Information, Information Technologies and Protection of Information" (itemized). Moscow, Statute, 2015. 320 p.

3.1. Data Protection

Although Russia is a member of the Council of Europe and a signatory of the Council of Europe Convention on the protection of individuals in the automated processing of personal data[152], the Russian personal data legislation has been criticized for not complying with the Convention[153]. According to the Convention, the ability to ensure adequate protection of personal data relies on the existence of one or more authorities to be responsible for ensuring compliance with data protection provisions. Importantly, article 15 of the Convention also prescribes that the supervisory authorities "shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions". According to such criteria, Russia cannot be deemed as a country that provides adequate protection of personal data, since the authorized body, the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications, better known as Roskomnadzor, is structurally dependent from the Ministry of Communications.

Furthermore, one of the main causes of concern, as regards the Russian data protection framework, has been the introduction of legislative provisions mandating the localization of the personal data of Russian citizens.

Localization of personal data of all Russian citizens was indeed introduced by amendments to the Federal Law on Personal Data. The data localization law (hereinafter – Law No. 242-FZ) regulates the obligations of operators to ensure that the recording, systematization, accumulation, storage, refinement (updating, modification) and retrieving of personal data of citizens of the Russian Federation are undertaken in databases located in the territory of the Russian Federation, as well as specifying the physical place where data is located.

Starting from 1 September 2015, Internet service providers that process personal data of Russians have been required to do so by using databases located in Russia[154]. The data localization provisions concerned, first of all, e-commerce services, social networks, travel booking services, and other services where users must indicate their citizenship. Such provisions target both Russian companies that may store data abroad and foreign organizations that deal provide services to Russian customers.

Moreover, this law establishes the Roskomnadzor's power to restrict access to information processed in violation of the legislation of the Russian Federation in the field of personal data. The law defines the procedure for restricting access to information processed in violation of the data protection legislation. For this purpose, an automated information system entitled "Register of violators of the rights of personal

[152] Convention on the protection of individuals in the automated processing of personal data. Concluded in the city of Strasbourg on 28 January 1981. // ConsultantPlus Legal Reference System.

[153] See Ivanov A.A. Storage of personal data abroad from the point of view of Russian law // The Law. 2015. No. 1. P. 134–143.

[154] See Federal Law of July 21, 2014 No. 242-FZ "On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Clarification of the Procedure for Processing Personal Data in Information and Telecommunication Networks" (as amended on 31.12.2014) // ConsultantPlus Legal Reference System.

data subjects" has been created. This registry, the responsibility of which is assigned to Roskomnadzor, is created in order to restrict access to information on the Internet that is processed in violation of the legislation of the Russian Federation in the field of personal data. The registry includes domain names on the Internet and network addresses containing information processed in violation of the law, an indication of an effective judicial act on the adoption of measures to restrict access to information, and the date and time of such measures[155].

Importantly, the justification for adopting data localization provisions is formulated by its authors as follows. Many citizens are registered on social networks, buy goods and receive services via the Internet. A significant part of such services is located abroad, mainly in the USA and Europe. As a result, credit card data, passport data, the content of private correspondence, including by email and instant messaging applications, are accumulated by service providers based in foreign jurisdictions. This situation may jeopardize individual and national security.

As stated by Vadim Dengin, one of the proponents of the Law and First Deputy Chairman of the State Duma Committee of the Russian Federation on Information Policy, Information Technology, and Communications, the majority of Russians are opposed to the storage of their data abroad and wish it to remain in the territory of Russia[156]. If not stored in Russia, such information may fall into the hands of malicious actors, including fraudsters and foreign intelligence services[157].

Academic Director of the Higher School of Economics Faculty of Law, Anton Ivanov, suggests that Law No. 242-FZ prohibits the cross-border transfer of personal data to databases located abroad[158]. However, the Convention on the Protection of Individuals in the Automatic Processing of Personal Data and the Law on Personal Data generally allow the cross-border transfer of personal data.

Furthermore, the law has been criticized for being counterproductive. According to the European Centre for International Political Economy (ECIPE), the entry into force of the Law on the Localization of Personal Data will lead to a decrease in Russia's GDP, which is equivalent to an annual loss of 286 billion roubles (roughly 5 billion USD)[159].

Also, according to an European diplomatic source, the Russian Law on the localization of personal data can create problems when issuing Schengen visas. The source explained that the servers that store data on European visas for Russian citizens are located in Europe[160].

---

155 Rules for the creation, formation and maintenance of the automated information system "Register of violators of the rights of personal data subjects". Approved by Decree of the Government of the Russian Federation of August 19, 2015 N 857// ConsultantPlus Legal Reference System.

156 See Filimonov A. (2014).

157 See Filimonov A. Ibid.

158 See Ivanov A. Storage of personal data abroad from the point of view of Russian law // Law. 2015. No. 1. P. 134-143.

159 See RBC News Agency (2015).

160 See Interfax News Agency (2014).

Lastly, it should be noted that the list of resources that may be blocked by Roskomnadzor, due to inconsistency with the law on the localization of personal data, does not mention the need for consideration of any specific technical elements as foreign domain names, URLs, and IP addresses, which may be instrumental for the transmission of personal data. On the one hand, the application of Law No. 242-FZ to the databases containing these objects could paralyze the entire Russian segment of the Internet because the basic mechanisms enabling the smooth functioning of the Internet are located outside the Russian Federation. On the other hand, it is important to stress that any kind of website blocking within one country is very challenging to implement, from a technical perspective, due to workarounds such as Virtual Private Networks (VPN) and anonymizers. The law concerns online services such as social networks, airline reservation services, and other services that might have a foreign origin and transnational scope and such services may prove hard to block on a national basis, as tellingly explained by the LinkedIn case.

3.2. The LinkedIn Case

The case of the ban and blocking of the social network LinkedIn in the Russian Federation is particularly noteworthy.

As many Russian companies, LinkedIn stores data on servers located out of Russia, as this is a cheaper and more convenient option. Besides, utilizing servers in non-Russian countries facilitates access to these resources for all individuals who are not in Russia.

Roskomnadzor filed a lawsuit against the LinkedIn Corporation on the recognition of the activities of its Internet resources for the collection, use, and storage of personal data of Russian citizens, indicating the claim was justified by the fact that Roskomnadzor, in accordance with its Internet monitoring attributions, identified a violation of the rights and legitimate interests of citizens of the Russian Federation as personal data subjects. According to Roskomnadzor, LinkedIn violated the requirements of the legislation of the Russian Federation in the field of personal data, specifically of law No. 152-FZ on personal data, by collecting information about LinkedIn users, as well as citizens of the Russian Federation who are not LinkedIn users, and by processing and transmitting such information without proper consent.

The Tagansky District Court of Moscow established that the administrator of the domain name of the website (LinkedIn.com) is a company, LinkedIn Corporation, located outside the Russian Federation and recognized LinkedIn's collection, use and storage of personal data of citizens of the Russian Federation as violating the requirements of the Law on Personal Data and citizens' rights to privacy, personal and family secrets. Accordingly, the Court ordered Roskomnadzor to take measures to restrict access to information on the Internet that has been processed in violation of the legislation of the Russian Federation in the field of personal data[161].

[161] The decision of the Tagansky District Court of Moscow dated 04.08.2016 in case No. 2-3491/2016 // ConsultantPlus Legal Reference System.

Lastly, even though data localization as mandated by the Russian law may be technically possible, many questions arise regarding the implementation of the constitutional rights and freedoms of citizens. Indeed, it may be argued that Law No. 242-FZ could be deemed unconstitutional. By restricting the right of a citizen to the cross-border transfer of personal data, even if an individual has given his consent to such a transfer, the Law conflicts with Art. 23 (privacy of correspondence) and Art. 29 p. 4 (freedom of information) of the Constitution of the Russian Federation[162].

The right to the cross-border transfer of personal data is not directly enshrined in the Russian Constitution, but it should be protected by the general constitutional rules. Human rights provided in the international legal instruments should be protected by the Constitution and legislation of the Russian Federation. According to Art. 15 of the Constitution of the Russian Federation, the universally recognized norms of international law and international treaties and agreements of the Russian Federation shall be a component part of its legal system. According to Art. 17, in the Russian Federation recognition and guarantees shall be provided for the rights and freedoms of man and citizen according to the universally recognized principles and norms of international law and according to the Constitution.

3.3. Consumer Protection

Russian consumer protection is a general body of law, applying to the offline and online environment alike, with no special legal provisions governing consumer protection on the Internet. As an example, in this perspective, Consumers International, which keeps the Digital Index of digital consumers rights, does not have any relevant record on the Russian Federation[163].

Russian legislation on consumer protection is regulated by the Law of the Russian Federation "On Protection of Consumer Rights" and general provisions of the civil legislation. The Law adopted in 1992 is generally outdated and does not have comprehensive consumer protection frameworks[164].

The legal basis for consumer protection is the Constitution of the Russian Federation, Federal laws, regulations of the President of the Russian Federation and the Government of the Russian Federation[165]. According to the Constitution of the Russian Federation, the state protection of the rights and freedoms of man and citizen in the Russian Federation is guaranteed.

According to the Law, consumer protection refers to the relationship between consumers and manufacturers, performers, importers, sellers, owners of aggregators of information about goods in

---

[162] Constitution of the Russian Federation (adopted by popular vote on 12.12.1993, with the amendments made by the Laws of the Russian Federation on amendments to the Constitution of the Russian Federation of 30.12.2008 No. 6-FKZ, of 30.12.2008 No. 7-FKZ, of 02.05.2014 N 2-FKZ, of 21.07.2014 N 11-FKZ).

[163] See Digital Index <https://digitalindex.consumersinternational.org/>.

[164] Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) "On Protection of Consumer Rights". // ConsultantPlus Legal Reference System.

[165] Decree of the Government of the Russian Federation of 27.09. 2007 No. 612 (as amended on 04.10.2012) "On the approval of the Rules for the sale of goods by remote means". // ConsultantPlus Legal Reference System.

the sale of goods. The law establishes the rights of consumers to purchase goods of adequate quality and safe for life, health, the property of consumers and the environment, obtaining information about goods and their manufacturers. The Law also establishes the consumer right to obtain information on aggregators and sellers of goods and services, state and public protection of the interests of the consumers, and also determines the mechanism for the realization of these rights. In accordance with the Law on Consumer Protection, the aggregator is only an information intermediary between the consumer and the seller. Guaranteed consumer rights in relation to aggregators consist of the owner of the aggregator being obliged to give the consumer information about the product and its seller. The owner of the aggregator posts information about the seller by posting it on his website on the Internet, or by posting on his website a hyperlink to the seller's website[166].

Federal state supervision in the field of consumer protection is carried out by an authorized federal executive body in this area, which is the Federal Service for Supervision of Consumer Rights Protection and Human Welfare.

The only legal definition concerning consumer relations carried out through the Internet is the "remote selling of goods". This concept refers to selling goods under a retail sale contract concluded on the basis of the buyer's familiarization with the goods offered by the seller, through a description contained in catalogues, brochures, or any other media, including the Internet. The remote selling excludes the possibility of direct familiarization of the buyer with the goods or sample of goods at the conclusion of such a contract[167]. This provision is similar to Brazilian law, which provides a 7-day no questions asked period of annulment of the purchase.

According to the terms of service of most Russian free online services, they are used "as is" or at one's risk, and service providers' liability is extremely limited. In this case, the Law on consumer protection does not apply. Indeed, consumer protection applies only to businesses that can be defined as "performer of services", which is any type of organization providing services to consumers *in exchange for payment*.

Lastly, the Russian Federation is part of the Agreement on the main areas of cooperation of the States members of the Commonwealth of Independent States in the field of consumer protection[168], although this agreement does not refer to digital issues in particular. It is worth noting that the two most relevant international documents in the area of consumer protection are the OECD Guidelines and the UN Guidelines. These OECD Guidelines for consumer protection in the context of electronic commerce are one of the most comprehensive frameworks in the area. The document states that consumers who

[166] Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) "On Protection of Consumer Rights". // ConsultantPlus Legal Reference System.

[167] See Decree of the Government of the Russian Federation of 27.09. 2007 No. 612 (as amended on 04.10.2012) "On the approval of the Rules for the sale of goods by remote means". // ConsultantPlus Legal Reference System.

[168] See Agreement on the main areas of cooperation of the States members of the Commonwealth of Independent States in the field of consumer protection (concluded in Moscow on 25.01.2000). // ConsultantPlus Legal Reference System.

participate in electronic commerce should enjoy transparent and effective consumer protection that should not be more limited than the level of protection afforded in the context of offline commerce. Importantly the Guidelines suggest that governments, businesses, consumers, and their representatives should work together to achieve such protection and determine what changes may be necessary to address the special circumstances of electronic commerce[169]. The United Nations Guidelines for Consumer Protection[170] are also a particularly authoritative document, representing the consensus of the United Nations General Assembly that adopted the document on December 22, 2015, by resolution No 70 / 186.

3.4. Cybercrime

According to the Russian legal doctrine, a crime in the field of computer information is defined as a socially dangerous act under a criminal law that causes harm or creates danger of harm to the safety of production, storage, use or dissemination of information or information resources[171]. According to official statistics produced by the Office of the Prosecutor General of the Russian Federation, in 2017 the number of crimes in the field of information and telecommunication technologies increased from 65,949 in the previous year to 90,587[172]. However, these figures represent only 4.4% of the total number of criminal acts recorded in Russia. This is almost 1 cybercrime for every 20 criminal acts recorded[173]. It can be argued that the current growth of cybercrime is caused not only by the shortcomings of the regulatory framework but also by the refusal of law enforcement agencies to initiate and investigate criminal cases.

An essential point to clarify, to be able to frame cybercrime properly, is the precise identification of the object of computer crimes. The correct definition of an object has not only theoretical but also practical significance. It is important to determine what is subject to criminal law protection, and the legislative development of this issue should be aimed at removing obstacles in the fight against such crimes as a global phenomenon.

As regards the Russian context, it must be noted that the legislative definition of terms used in conducting operational search and investigative measures is still needed. There is also a strong need for modernization of Chapter 28 of the Criminal Code of the Russian Federation in terms of clarifying the concepts used and responsibility for cybercrime, expanding the evidence base through digital evidence and unambiguous description of the requirements for them under an established practice.

---

169 See OECD (2009) <https://www.oecd.org/ict/econsumerconference/44047583.pdf>.

170 See United Nations Guidelines for Consumer Protection adopted by the United Nations General Assembly on December 22, 2015, by resolution N 70 / 186. // ConsultantPlus Legal Reference System.

171 See Criminal law of Russia. General and Special parts: textbook / A.A. Aryamov, TB Basova, E.V. Blagov et al.; rep. ed. Yu.V. Gracheva, A.I. Chuchaev. M.: Contract, 2017. 384 p.

172 See Office of the Prosecutor General of the Russian Federation (2018) <https://genproc.gov.ru/smi/news/genproc/news-1431104/>.

173 Idem.

The last additions to Chapter 28 of the Criminal Code introduced items that establish responsibility for the creation, distribution and use of computer programs or other "computer information"[174] that are intended to have an unlawful impact on the critical information infrastructure of the Russian Federation, including for the destruction, blocking, modification, copying of the information contained in it, or neutralizing the means of protection of this information.

The Chapter also defines provisions on the unauthorized access to computer information, including using computer programs or other computer information that are intended to cause illegal impact on the critical information infrastructure of the Russian Federation, or other malicious computer programs, if they entailed damage to critical information[175]. It also established criminal liability for violation of the rules of usage of the storage, processing or transmission of protected computer information contained in the critical information infrastructure of the Russian Federation[176].

A further aspect to be considered is that, to date, Russia has not acceded to the Council of Europe Convention on Cybercrime[177], better known as the Budapest Convention, despite being a member of the Council of Europe. The Russian Federation's statement on the refusal to accede to this convention indicated that "guided by clause 'a' of Article 18 of the Vienna Convention on the Law of Treaties of 1969, it would refrain from actions that would deprive the Budapest Convention of its object and purpose"[178].

At the time of the elaboration of the Budapest Convention, the Russian Federation understanding of Article 32, paragraph b of the Convention was that the provision was formulated in such a way that might damage the sovereignty and national security of member states, the rights and legitimate interests of their citizens and legal entities[179]. This paragraph deals with transborder access to stored computer data with consent or where publicly available:

> *Article 32 – Transborder access to stored computer data with consent or where publicly available.*
>
> *A Party may, without the authorization of another Party:*

[174] According to the Criminal Code of the Russian Federation, computer information refers to information (messages, data) presented in the form of electrical signals, regardless of their means of storage, processing, and transmission.

[175] See Criminal Code of the Russian Federation dated 13.06.1996 No. 63-FZ (as amended on 23.04.2019) // ConsultantPlus Legal Reference System.

[176] See Criminal Code of the Russian Federation dated 13.06.1996 No. 63-FZ (as amended on 23.04.2019) // ConsultantPlus Legal Reference System.

[177] See Convention on Computer Crime (ETS No. 185). It was concluded in the city of Budapest on November 23, 2001 (as amended on January 28, 2003) // ConsultantPlus Legal Reference System.

[178] Order of the President of the Russian Federation of 15.11.2005 N 557-rp "On the signing of the Convention on Cybercrime"// ConsultantPlus Legal Reference System.

[179] See Crime Research Center (2008) <http://www.crime-research.org/news/28.03.2008/3277/>

> *a)*
>
> *Access publicly available (open source) stored computer data, regardless of where the data is located geographically; or*
>
> *b)*
>
> *Access or receive through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.*

Initially, the Russian Federation considered adopting the Convention if, through the revision process mentioned in article 46, p. 3, the issue with paragraph b of article 32 could be resolved. As the controversy was not solved, however, Russia finally refused to accede to the Budapest Convention[180].

3.5. Protection of the Public Order

In 2016, the State Duma of the Russian Federation adopted a package of antiterrorist amendments[181] to the legislation, designed by the deputy of the State Duma Irina Yarovaya and a member of the Federation Council, Viktor Ozerov. After the first reading, some of the most resonant norms of the bill were relaxed or deleted. But some of the provisions, criticized by the IT industry, remained in the document[182].

Irina Yarovaya argued that the Internet destroys the concept of the border and endangers the concept of sovereignty[183]. In her opinion, modern Information and Communications Technologies (ICTs) can jeopardize sovereign domestic interests and violate the principles of national security. According to Irina Yarovaya, the additional powers that the amendments attributes to the Federal Security Service of the Russian Federation are instrumental to allow the secret services to more effectively solve their tasks.

According to the amendments, Internet service providers are obliged to store on the territory of the Russian Federation for three years information on the reception, transmission, delivery and processing

[180] Order of the President of the Russian Federation of March 22, 2008 No. 144-rp "On invalidation of the decree of the President of the Russian Federation of November 15, 2005 No. 557-rp "On Signing the Convention on Cybercrime". ConsultantPlus Legal Reference System.

[181] See Federal Law of 06.07.2016 N 374-FZ "On Amendments to the Federal Law "On Countering Terrorism" and certain legislative acts of the Russian Federation regarding the establishment of additional counter-terrorism measures and ensuring public safety" // ConsultantPlus Legal Reference System.

[182] See ZNAK.COM (2018) <https://www.znak.com/2018-01-22/smi_pravitelstvo_smyagchilo_zakon_yarovoy_priznav_kritiku_konstruktivnoy>

[183] See RBC (2016) <https://www.rbc.ru/technology_and_media/24/06/2016/576c0a529a79471bc44d2b57>.

of voice information and text messages, including their content, as well as images, sounds or other messages of users of communication services[184].

Some recent judicial cases deserve attention to illustrate how the amendments have been concretely implemented. For example, Roskomnadzor filed a lawsuit against the restriction in the territory of the Russian Federation of access to information resources operated by Telegram Messenger Limited Liability Partnership (LLP). According to Roskomnadzor, Telegram Messenger LLP did not fulfil the obligation to provide the Federal Security Service of the Russian Federation with information necessary to decode received, transmitted, delivered and processed electronic messages, which is the basis for the application of Part 2, Art. 15.4 of the Federal Law of July 27, 2006 No. 149-FZ "On Information, Information Technologies and Information Protection".

This law provides the possibility of restricting access to information systems and programs for electronic computers that are designed and used to receive, transmit, deliver and process electronic messages through the Internet until the execution of such duties. The Tagansky District Court of Moscow satisfied the claim of Roskomnadzor and decided to limit the activities of Telegram in the Russian Federation[185].

In response, Telegram released a statement calling its users to come to the rally in its defence. The statement was distributed among Russian-speaking users, arguing that "For more than 10 months, Roskomnadzor has been blocking thousands of IP addresses daily, trying to prevent Telegram from operating in Russia. So far Telegram wins in this struggle, but on any given day everything can change – the state has enormous resources withdrawn from the population. The rally is held in response to the adopted law on the isolation of the Russian Internet, which aims to introduce total censorship in Russia. Having spent billions of roubles, the authorities plan to cut off Russia from the rest of the world, after which they will be able to block foreign social networks and instant messengers. Telegram supports the rally against the isolation of the Russian segment of the Internet and encourages its users to participate in it[186]".

In connection with the Telegram case, there was an attempt to appeal to the Constitutional Court of the Russian Federation. In his complaint to the Constitutional Court of the Russian Federation, Russian citizen V. Sedov disputed the constitutionality of clause 4.1 of Article 10.1 of Federal Law No. 149-FZ. This clause requires any entity that organizes the transmission, delivery, and processing of electronic messages on the Internet, to provide the information necessary for decoding all received,

---

[184] Draft Federal Law No. 1039149-6 "On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Establishment of Additional Measures to Counter Terrorism and Ensure Public Safety" (ed., Submitted to the State Duma of the Federal Assembly of the Russian Federation, text as of 07.04.2016) // ConsultantPlus Legal Reference System.

[185] The decision of the Tagansky District Court of Moscow dated April 13, 2018 in case No. 2-1779 / 2018. // ConsultantPlus Legal Reference System.

[186] See TJOURNAL (2019) <https://tjournal.ru/internet/89681-telegram-prizval-polzovateley-vyyti-na-miting-v-moskve-protiv-izolyacii- runeta>

transmitted, delivered and processed electronic messages to the federal executive body in the field of security.

According to the applicant, the contested statutory provision allows the possibility of a massive restriction of citizens' rights to confidentiality of correspondence, telephone conversations, postal, telegraph and other communications on the basis of a court decision that has not yet entered into legal force, which contradicts Article 23 of the Constitution of the Russian Federation.

The Constitutional Court of the Russian Federation, having examined the submitted materials, did not find grounds for accepting this complaint. In accordance with the Federal Constitutional Law on the Constitutional Court, only citizens whose rights and freedoms are violated by the law applied in a particular case have the right to appeal to the Constitutional Court of the Russian Federation with an individual or collective complaint about a violation of constitutional rights and freedoms[187]. Applicant V. Sedov did not prove before the Constitutional Court that the law under consideration had been applied in his case by the court in the civil or criminal case.

Thus, Mr Sedov's complaint was not accepted for consideration by the Constitutional Court of the Russian Federation, as it did not meet the criterion of admissibility, enshrined in the Federal Constitutional Law "On the Constitutional Court of the Russian Federation[188]".

3.6. Cyberdefence

A particularly interesting instance in the field of cyberdefence is the Law on the security of the critical information infrastructure of the Russian Federation[189]. The Law provides for measures to introduce a computer security incident management system or a "content management system" that is capable of ensuring the security of the critical information infrastructure of the Russian Federation.

This is a response to the widespread introduction of an ample range of information technologies into the production and process management systems of the critical infrastructure of the Russian Federation, together with the globalization of modern information and telecommunication networks. These phenomena foster the transformation of critical infrastructures and the ICTs utilized to manage them into a single global information and telecommunications network with blurred borders of

[187] Federal Constitutional Law of July 21, 1994 No. 1-FKZ (as amended on 07/29/2018) "On the Constitutional Court of the Russian Federation"// ConsultantPlus Legal Reference System.

[188] Determination of the Constitutional Court of the Russian Federation of 29.05.2018 No. 1153-O "On refusal to accept complaints of citizen Sedov Vladimir Sergeyevich for violation of his constitutional rights by clause 4.1 of Article 10.1 of the Federal Law" On Information, Information Technologies and Protection of Information " // ConsultantPlus Legal Reference System.

[189] See Federal Law of 26.07.2017 No. 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation" // ConsultantPlus Legal Reference System.

national segments, and the increasing use of information and telecommunication networks and common use networks for their information exchange[190].

Besides constitutional and legislative provisions governing national security as a whole, it must be noted that cyberdefence is framed by a variety of strategic and doctrinal documents approved by the President of the Russian Federation, acting in his constitutional role of Supreme Commander of the Armed Forces. Among such documents are the Military Doctrine of the Russian Federation and the Doctrine of Information Security. Thus, despite the recent legislative production in regard to cyberdefence , defence and security measures in the field of ICTs are not regulated by legislation, but only by official doctrines.

In Russia, there are officially approved doctrines, including the Doctrine of Information Security of the Russian Federation. Such doctrines are a system of official views in a certain sphere and, despite their official nature, they can hardly be regarded as a source of law, since they are more likely programmatic documents. They may contain definitions, but they lack legal regulations. Even though the law enforcer can use the provisions developed by the doctrine, and it can occupy an important place in ensuring the uniform regulation of social relations, it seems that the legal doctrine can hardly be considered as a source of law[191].

In particular, the Military Doctrine of the Russian Federation notes the "trend of shifting military dangers and military threats into the information space" and refers to the tasks of equipping the Armed Forces, other troops and bodies with weapons, military and special equipment of information confrontation[192].

Importantly, approval of the Military Doctrine of the Russian Federation under Clause "z" Art. 83 of the Constitution of the Russian Federation and sub. 2 p. 2 Art. 4 of the Federal Law "On Defence" is included in the powers of the President of the Russian Federation[193].

3.7. Conclusion: CheburashkaNet and the Sovereign Internet Law

In April 2014, Maxim Kavzdradze, member of the Council of the Federation, the upper chamber of the Russian parliament, proposed the creation of a Russian national intranet, a totally domestic network, unavailable from abroad. This network was nicknamed "CheburashkaNet" after the Russian cartoon character Cheburashka, a character from Gena the Crocodile, a 1969 Soviet stop-motion

[190] The main directions of state policy in the field of security of automated control systems for production and technological processes of critical infrastructure facilities of the Russian Federation (approved by the President of the Russian Federation on 03.02.2012 No. 803) // ConsultantPlus Legal Reference System.

[191] See Zlobin A.V. Forms of law in modern Russia // Lex russica, 2018, number 4. Pp . 23 – 36.

[192] Military doctrine of the Russian Federation (approved by the President of the Russian Federation No. Pr-2976 of December 25, 2014) // ConsultantPlus Legal Reference System.

[193] Decree of the President on 05 December 2016 number 646 "On approval of the Information Security Doctrine of the Russian Federation"// ConsultantPlus Legal Reference System.

animated film. Recently, Kavzdradze explained that his proposal should be limited to the creation of a national network for the secure circulation of "scientific information[194]."

In a similar spirit, on May 1, 2019, the President of the Russian Federation signed the Law "On Amendments to Certain Legislative Acts of the Russian Federation", better known as the "Sovereign Internet Law". The sovereign Internet legislation prescribes the establishment of an alternative DNS system, the purpose of which is to ensure the functioning of the Internet in Russia in case of its disconnection from the global network. The law will partially come into force on 1st November 2019 and will be in full capacity from 2021 onward.

According to the developers of the law, under these conditions, protective measures are necessary to ensure the long-term and stable operation of the Internet in Russia and to increase the reliability of the Russian Internet resources. The law establishes the necessary rules for traffic routing and for the control of their compliance, and promotes a system aimed at minimizing the transfer abroad of the data exchanged between Russian users.

Adoption and implementation of the "Sovereign Internet Law" may be seen with suspicion as it is likely to expand the powers of Roskomnadzor without appropriate checks and balances and will require significant expenditures to be implemented. When the Sovereign Internet Law was still a bill, these latter points of concern have been raised vocally by the Expert Council under the Government of the Russian Federation[195].

3.8. References

Criminal law of Russia. General and Special parts: textbook / A.A. Aryamov, TB Basova, E.V. Blagov et al.; rep. ed. Yu.V. Gracheva, A.I. Chuchaev. M.: Contract, 2017. 384 p.

Digital Index. Consumers International. Available at <https://digitalindex.consumersinternational.org/>. Accessed October 12, 2019.

Filimonov A. "It is necessary to share!" Or Protection of personal data of Russians from foreign special services // GARANT.RU information legal portal. Available at <http://www.garant.ru/article/559071/>. Accessed October 12, 2019.

Ivanov A. Storage of personal data abroad from the point of view of Russian law // The Law. 2015. No. 1. P. 134–143.

Kanev S. Cheburashka, or you cannot become famous for good deeds // Novaya Gazeta, No. 52 of May 16, 2014. Available at <https://www.novayagazeta.ru/articles/2014/05/05/59473-cheburashka-ili-horoshimi-delami-proslavitsya-nelzya>. Accessed October 12, 2019.

Media: the government softened the "Yarovaya Law", recognizing constructive criticism (ZNAK.COM, January 22, 2018) Available at <https://www.znak.com/2018-01-22/smi_pravitelstvo_smyagchilo_zakon_yarovoy_priznav_kritiku_konstruktivnoy>. Accessed October 12, 2019.

[194] See Kanev S. Cheburashka, or you cannot become famous for good deeds // Novaya Gazeta, No. 52 of May 16, 2014, <https://www.novayagazeta.ru/articles/2014/05/05/59473-cheburashka-ili-horoshimi-delami-proslavitsya-nelzya>.

[195] With sovereignty in tomorrow. Experts at the government estimated the cost of the autonomous Internet (Commersant Newspaper, No. 238 of December 25, 2018). <https://www.kommersant.ru/doc/3842329>. Accessed October 12, 2019.

OECD Guidelines for consumer protection in the context of electronic commerce. Available at <https://www.oecd.org/ict/econsumerconference/44047583.pdf>. Accessed October 12, 2019.

On crimes committed using modern information and communication technologies. Office of the Prosecutor General of the Russian Federation. August 14, 2018. Available at <https://genproc.gov.ru/smi/news/genproc/news-1431104/>. Accessed October 12, 2019.

Personal unprofitable. How much will Russia lose due to personal data law. RBC News Agency. Available at <https://www.rbc.ru/newspaper/2015/06/16/56bcc9349a7947299f72bef0>. Accessed October 12, 2019.

Saveliev A.I. Commentary to the Federal Law of July 27, 2006, No. 149-FZ "On Information, Information Technologies and Protection of Information" (itemized). Moscow, Statute, 2015. 320 p.

Telegram statement distributed among Russian-speaking users via messenger channels on March 6, 2019. Available at <https://tjournal.ru/internet/89681-telegram-prizval-polzovateley-vyyti-na-miting-v-moskve-protiv-izolyacii-runeta>. Accessed October 12, 2019.

The EU warned about problems with issuing visas due to the law on personal data. Interfax News Agency. Available at <http://www.interfax.ru/russia/402035>. Accessed October 12, 2019.

The Yarovaya Code: What Threats Antiterrorism Law implies to Internet Users // RBC Available at <https://www.rbc.ru/technology_and_media/24/06/2016/576c0a529a79471bc44d2b57>. Accessed October 12, 2019.

Transcript of the State Duma plenary of February 12, 2019. Available at <http://transcript.duma.gov.ru/node/5115/>. Accessed October 12, 2019.

With sovereignty in tomorrow. Experts at the government estimated the cost of the autonomous Internet (Commersant Newspaper, No. 238 of December 25, 2018). Available at <https://www.kommersant.ru/doc/3842329>. Accessed October 12, 2019.

Zlobin A.V. Forms of law in modern Russia // Lex russica, 2018, number 4. Pp. 23 – 36.

3.9. Legal Sources

Convention on the protection of individuals in the automated processing of personal data. Concluded in the city of Strasbourg on 28 January 1981. // ConsultantPlus Legal Reference System.

Agreement on the main areas of cooperation of the States members of the Commonwealth of Independent States in the field of consumer protection (concluded in Moscow on 25.01.2000). // ConsultantPlus Legal Reference System.

United Nations Guidelines for Consumer Protection adopted by the United Nations General Assembly on December 22, 2015, by resolution N 70 / 186. // ConsultantPlus Legal Reference System.

Convention on Computer Crime (ETS No. 185). It was concluded in the city of Budapest on November 23, 2001 (as amended on January 28, 2003) // ConsultantPlus Legal Reference System.

Constitution of the Russian Federation (adopted by popular vote on 12.12.1993, with the amendments made by the Laws of the Russian Federation on amendments to the Constitution of the Russian Federation of 30.12.2008 No. 6-FKZ, of 30.12.2008 No. 7-FKZ, of 02.05.2014 N 2-FKZ, of 21.07.2014 N 11-FKZ). // ConsultantPlus Legal Reference System.

Federal Constitutional Law of July 21, 1994 No. 1-FKZ (as amended on 07/29/2018) "On the Constitutional Court of the Russian Federation"// ConsultantPlus Legal Reference System.

Federal Law of 26.07.2017 No. 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation" // ConsultantPlus Legal Reference System.

Federal Law of December 28, 2013 N 398-FZ "On Amendments to the Federal Law "On Information, Information Technologies and the Protection of Information" entered into force on February 1, 2014. // ConsultantPlus Legal Reference System.

Federal Law of July 21, 2014 No. 242-FZ "On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Clarification of the Procedure for Processing Personal Data in Information and Telecommunication Networks" (as amended on 31.12.2014) // ConsultantPlus Legal Reference System.

Federal Law of 06.07.2016 N 374-FZ "On Amendments to the Federal Law "On Countering Terrorism" and certain legislative acts of the Russian Federation regarding the establishment of additional counter-terrorism measures and ensuring public safety" // ConsultantPlus Legal Reference System.

Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) "On Protection of Consumer Rights". // ConsultantPlus Legal Reference System.

Criminal Code of the Russian Federation dated 13.06.1996 No. 63-FZ (as amended on 23.04.2019) // ConsultantPlus Legal Reference System.

Decree of the Government of the Russian Federation of 27.09. 2007 No. 612 (as amended on 04.10.2012) "On the approval of the Rules for the sale of goods by remote means". // ConsultantPlus Legal Reference System.

Decree of the Government of the Russian Federation of 27.09. 2007 No. 612 (as amended on 04.10.2012) "On the approval of the Rules for the sale of goods by remote means". // ConsultantPlus Legal Reference System.

Order of the President of the Russian Federation of 15.11.2005 N 557-rp "On the signing of the Convention on Cybercrime"// ConsultantPlus Legal Reference System.

Order of the President of the Russian Federation of March 22, 2008 No. 144-rp "On invalidation of the decree of the President of the Russian Federation of November 15, 2005 No. 557-rp "On Signing the Convention on Cybercrime". ConsultantPlus Legal Reference System.

Military doctrine of the Russian Federation (approved by the President of the Russian Federation No. Pr-2976 of December 25, 2014) // ConsultantPlus Legal Reference System.

Decree of the President on 05 December 2016 number 646 "On approval of the Information Security Doctrine of the Russian Federation"// ConsultantPlus Legal Reference System.

Rules for the creation, formation and maintenance of the automated information system "Register of violators of the rights of personal data subjects". Approved by Decree of the Government of the Russian Federation of August 19, 2015 N 857// ConsultantPlus Legal Reference System.

The main directions of state policy in the field of security of automated control systems for production and technological processes of critical infrastructure facilities of the Russian Federation (approved by the President of the Russian Federation on 03.02.2012 No. 803) // ConsultantPlus Legal Reference System.

Draft Federal Law No. 1039149-6 "On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Establishment of Additional Measures to Counter Terrorism and Ensure Public Safety" (ed., Submitted to the State Duma of the Federal Assembly of the Russian Federation, text as of 07.04.2016) // ConsultantPlus Legal Reference System.

The decision of the Tagansky District Court of Moscow dated April 13, 2018 in case No. 2-1779 / 2018. // ConsultantPlus Legal Reference System.

The decision of the Tagansky District Court of Moscow dated 04.08.2016 in case No. 2-3491/2016 // ConsultantPlus Legal Reference System.

Determination of the Constitutional Court of the Russian Federation of 29.05.2018 No. 1153-O "On refusal to accept complaints of citizen Sedov Vladimir Sergeyevich for violation of his constitutional rights by clause 4.1 of Article 10.1 of the Federal Law" On Information, Information Technologies and Protection of Information " // ConsultantPlus Legal Reference System.

Annex

Country Report: Russia

1. Data Protection

▪ Scope

1. What national laws (or other types of normative acts) regulate the collection and use of personal data?

Most rules are found in specific legislation, particularly the Data Protection Act No. 152 FZ dated 27 July 2006 (DPA) and various regulatory acts adopted to implement the DPA as well as other laws, including the Information, Information Technologies and Information Protection Act No. 149 FZ dated 27 July 2006 establishing basic rules as to the information in general and its protection. In addition, the Russian Labour Code contains provisions on the protection of employees' personal data (Part XIV). Other laws may also contain data protection provisions, which implement the data protection rules in relation to specific areas of state services or industries.

Russia // Data protection laws of the world. DLA Piper Intelligence.
URL: <https://www.dlapiperdataprotection.com/?t=law&c=RU>.

2. Is the country a part of any international data protection agreement?

Convention on the protection of individuals in the automated processing of personal data. Concluded in the city of Strasbourg on January 28, 1981 (together with the Amendments to the Convention on the Protection of Individuals with the Automated Processing of Personal Data (CETS No. 108), allowing the accession of the European Communities adopted by the Committee of Ministers in Strasbourg on 15.06.1999). This document entered into force on October 1, 1985. For the Russian Federation, this document entered into force on September 1, 2013.

Source: "Consultant Plus" Legal Reference System.

3. What data is regulated?

Personal data is information, i.e. messages or data regardless of the form of their representation". The form of displaying information does not matter: it can be information in text, graphic, sound form, perceived by a person or device. The carrier of such data is also irrelevant: they can be recorded on paper, in another analogue form (for example, on videotape) or exist in electronic form. The information must have a certain relationship with an individual. Such an attitude may occur in cases where such information:

1) by virtue of its content, concerns a certain person;

2) has as its purpose an assessment of a person's activities or may affect the status of such a person, including by making any decisions in this regard;

3) is of a technical nature (for example, data of devices used by an individual) and is used for technical purposes, but can, if desired, be used by the operator for purposes that have an impact on the rights and obligations of the individual.

Information relates directly or indirectly to a particular or designated person, i.e. possesses certain identifying potential.

If the data makes it possible to single out an individual from a variety of persons and use his particular interaction model with respect to him, then that person is definable, and the corresponding information is his personal data.

Saveliev A.I. Scientific and practical article by article commentary to the Federal Law "On Personal Data". M.: Statute, 2017. 320 p.

4. Are there any exemptions?

The Federal Law on Personal Data does not apply to relations arising from:

1) the processing of personal data by individuals solely for personal and family needs, if this does not violate the rights of the subjects of personal data;

2) the organisation of storage, acquisition, accounting and use of documents containing the personal data of the Archival Fund of the Russian Federation and other archival documents in accordance with the legislation on archives in the Russian Federation;

3) the processing of personal data assigned in the prescribed manner to information constituting state secrets.

The Law on Personal Data does not apply to storage and other types of processing of unsystematised personal data, even if subsequent access by third parties is possible.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data"; Saveliev A.I. Scientific and practical article by article commentary to the Federal Law "On Personal Data". M.: Statute, 2017. 320 p.

5. To whom do the laws apply?

The legislation on personal data applies to all entities that process personal data. Federal government bodies, as well as government bodies of constituent entities of the Russian Federation can process personal data. Local governments and municipal bodies that are not part of the system of local governments carry out the processing of personal data.

If legal entities process personal data, they are also subject to the law on personal data.

Under the individuals processing in the framework of the legislation on personal data, are citizens who carry out business activities without forming a legal entity, from the moment of state registration as an individual entrepreneur. Individuals engaged in the processing of personal data may also include attorneys, notaries, heads of farms.

Kukharenko, T.A. Commentary to the Federal Law of July 27, 2006 No. 152-ФЗ "On Personal Data" (itemised) "Consultant Plus" Legal Reference System, 2011.

6. Do the laws apply to foreign entities that do not have physical presence in the country?

Even if a foreign company conducts its business through the Internet without a physical presence in Russia, data protection requirements may apply to such a company. The main criterion is that activity of such a foreign company is directed to the territory of the Russian Federation.

According to the Ministry of Communications and Mass Media, the use of a domain name associated with the Russian Federation (.ru, .рф., .su, .москва., .moscow и т.п.) may indicate the focus of activity on the territory of Russia; as well as the presence of the Russian-language version of the Internet site, created by the owner of such a site or on his behalf by another person, except for the function of an automated translation.

Additional criteria are the ability to make payments in Russian roubles, the ability to deliver goods, provide services or use digital content in Russia, as well as other cases of contract execution in the Russian Federation, the use of advertising in Russian, referring to the corresponding Internet site, and other circumstances that clearly indicate the intention of the owner of the website to include the Russian market in their business strategy.

Zherdina S. Localisation of personal data of Russians for foreign companies // EZh-Yurist. 2017. N 45. p. 5.

▪ Definitions

7. How are personal data defined?

Personal data – any information related to directly or indirectly determined or determining individual (subject of personal data).

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data".

8. Are there special categories of personal data (e.g. sensitive data)?

Article 10 of the Federal Law "On Personal Data" defines that special categories of personal data include data relating to race, nationality, political opinion, religious or philosophical beliefs, health, and intimate life. Giving special categories of personal data a special status is due to the possibility of the occurrence of particularly negative consequences for the subject upon their disclosure or other unauthorised use. Such consequences can be expressed not only in risks to the life and health of a person but also in discrimination, the impossibility of exercising basic constitutional rights to work, education, freedom of conscience, holding assemblies, etc.

According to ***Article 11*** of the Federal Law **"On Personal Data",** biometric personal data includes information that characterizes the physiological and biological characteristics of a person, on the basis of which his identity can be established and which are used by the operator to identify the subject of personal data. The sensitive nature of biometric data, the impossibility of their "replacement" in the event of a compromise due to their inseparable connection with the person, determine the special order of their processing.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data". Saveliev A.I. Scientific and practical article by article commentary to the Federal Law "On Personal Data". M.: Statute, 2017. 320 p.

9. How is the data controller and the data processor/operator defined?

Operator is a state body, municipal body, legal or natural person, independently or jointly with other persons organising and (or) processing personal data, as well as determining the purposes of personal data processing, the composition of personal data to be processed, actions (operations) performed with personal data.

This definition is in fact a borrowing of the provisions of Directive 95/46 / EC of the European Parliament and of the Council of the European Union on the protection of individuals in the processing of personal data and on the free circulation of such data, which became invalid due to the adoption of the GDPR.

It differs from the definition contained in the 1981 Convention, which uses the concept of the controller of the file, defined as "an individual or legal entity, state authority, institution or any other body competent in accordance with domestic law decide what should be the purpose of an automated data file, which categories of personal data should be stored or which operations should be performed with them".

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data". Saveliev A.I. Scientific and practical article by article commentary to the Federal Law "On Personal Data". M.: Statute, 2017. 320 p.

10. What are the data protection principles and how are they defined?

1. The processing of personal data must be carried out in a lawful and fair manner.

2. The processing of personal data should be limited to the achievement of specific, predetermined and legitimate goals. It is not allowed to process personal data incompatible with the purposes of collecting personal data.

3. It is not allowed to merge databases containing personal data that are processed for purposes that are incompatible with each other.

4. Only personal data is processed that meets the purposes of processing it.

5. The content and volume of processed personal data must comply with the stated processing objectives. The processed personal data should not be redundant in relation to the stated purposes of their processing.

6. When processing personal data, the accuracy of personal data must be ensured, its sufficiency and, if necessary, its relevance to the purposes of personal data processing. The operator must take the necessary measures or ensure that they are taken to remove or clarify incomplete or inaccurate data.

7. The storage of personal data should be carried out in a form that allows determining the subject of personal data not longer than the purpose of processing personal data unless the period for storing personal data is established by federal law, an agreement to which the subject of personal data is a

beneficiary. The personal data to be processed shall be destroyed or depersonalised upon the achievement of the processing objectives or in case of the loss of the need to achieve these objectives unless otherwise provided by federal law.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data".

11. Does the law provide any specific definitions with regards to data protection in the digital sphere?

Automated processing of personal data – processing of personal data using computer technology.

Personal Data Information System – a set of personal data contained in databases and information technologies and technical means ensuring their processing.

The user of an information system of personal data is a person participating in the operation of an information system of personal data or using the results of its operation.

Under the technical means that allow for the processing of personal data, refers to computer equipment, information and computer systems, and networks, means, and systems for transmitting, receiving and processing personal data, information protection tools used in information systems.

The system for the protection of personal data includes organisational and (or) technical measures determined to take into account the current threats to the security of personal data and information technologies used in information systems.

Actual threats to the security of personal data are understood as a set of conditions and factors that create an actual risk of unauthorised, including accidental, access to personal data when they are processed in an information system, which can result in the destruction, alteration, blocking, copying, provision, dissemination of personal data, as well as other illegal actions.

Federal law of 27.07.2006 N 152-FZ (as amended on 12/31/2017) "On personal data"; Government Decree of 01.11.2012 N 1119 *"On approval of requirements for the protection of personal data when processing them in personal data information systems"; "The basic model of threats to the security of personal data when they are processed in personal data information systems" (Extract)* (approved by the Federal Service for Technical and Export Control on February 15, 2008).

▪ Rights

12. Is the data protection law based on fundamental rights (defined in Constitutional law or International binding documents)?

Initially, provisions relating to the protection of the rights of citizens in the field of personal data were reflected in the Universal Declaration of Human Rights adopted by the UN General Assembly on December 10, 1948. Later they were developed and reflected in the 1981 Convention ratified by the Russian Federation in 2013. The legislation of the Russian Federation in the field of personal data generally repeats the main provisions of the above international acts.

In ***Art. 23*** of the Constitution of the Russian Federation, it is established that everyone has the right to privacy, personal and family secrets, protection of their honour and good name, the right to privacy of correspondence, telephone conversations, postal, telegraph and other messages. Restriction of this right is allowed only in exceptional cases provided by law.

Federal Law "On Personal Data": scientific and practical commentary (article by article) / A.Kh. Gafurova, E.V. Dorotenko, Yu.E. Kontemirov and others; by ed. A.A. Priezhzheva. M.: The editors of "Rossiyskaya Gazeta", 2015. Vol. 11. 176 s.

13. What are the rights of the data subjects according to the law?

- The right to receive information on the processing of his personal data.
- The right to clarify the personal data processed by the operator.
- The right to block personal data.
- The right to demand the destruction of data.
- The right to take measures prescribed by law to protect their rights.
- The right to appeal the actions of the operator to the authorised body.
- The right to the processing of personal data in order to promote goods, works, services on the market by making direct contacts with a potential consumer using means of communication, as well as for the purposes of political agitation only with the prior consent of the subject of personal data.
- The prohibition to make decisions on the basis of automated processing of personal data, generating legal consequences in relation to the subject of personal data or otherwise affecting his rights and legitimate interests.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data".

▪ Obligations and Sanctions

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

Obligation to ensure the confidentiality of personal data – the prohibition to disclose personal data to third parties without the consent of the subject.

Obtaining the consent of the subject of personal data (when there are no other conditions for their processing) in a form that provides the opportunity to prove the fact of obtaining consent, or in written cases in certain cases provided by law

Publication of the privacy policy or other document defining its policy in relation to the processing of personal data, and information about the implemented requirements for the protection of personal data, as well as providing access to the specified document using the appropriate information and telecommunication network.

Publication of local acts establishing procedures aimed at preventing and detecting violations of the legislation of the Russian Federation, elimination of the consequences of such violations.

Notification of Roskomnadzor prior to the processing of personal data.

Ensuring the security of information systems and the necessary level of personal data security.

Appointment of the person responsible for the processing of personal data (for operators who are legal entities).

Ensuring the impossibility of unauthorised access to the material carrier (except for paper media and carriers within the operator's information system) of biometric personal data.

Ensuring the preservation of personal data of citizens of the Russian Federation in Russia.

Ali M. Personal data: duties and responsibilities of the operator //
EZh-Lawyer. 2017. N 12. P. 5.

15. Is notification to a national regulator or registration required before processing data?

The operator, prior to the processing of personal data, is obliged to notify the authorised body for the protection of the rights of personal data subjects about their intention to process personal data, except in the special cases.

The operator has the right to carry out the processing of personal data without notifying the authorised body for the protection of the rights of personal data subjects:

1) processed in accordance with labor laws;

2) received by the operator in connection with the conclusion of the contract to which the subject of personal data is a party,

3) relating to members (participants) of a public association or religious organisation and processed by the relevant public association or religious organisation,

4) made by the subject of personal data publicly available;

5) including only surnames, names and patronymic of personal data subjects;

6) necessary for the purpose of a single pass of the subject of personal data to the territory in which the operator is located, or for other similar purposes;

7) included in the information systems of personal data, which in accordance with federal laws have the status of state automated information systems, as well as state information systems of personal data created to protect the security of the state and public order;

8) processed without the use of automated means;

9) processed in cases stipulated by the legislation of the Russian Federation on transport security.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017)
"On personal data".

16. Does the law require privacy impact assessment to process any category of personal data?

The operator is obliged to take measures necessary and sufficient to ensure the performance of their duties. Such measures include an assessment of the harm that may be caused to personal data subjects in the event of a violation of the Federal Law "On Personal Data", the ratio of the said

harm and the measures taken by the operator to ensure the fulfilment of duties provided for by the Federal Law "On Personal Data".

The main goal of such an audit is to analyse the effectiveness of organisational and technical measures taken to protect the processed personal data in order to minimize possible harm. The order and frequency of such an audit is determined by the local act of the operator.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data". Saveliev A.I. Scientific and practical article by article commentary to the Federal Law "On Personal Data". M.: Statute, 2017. 320 p.

17. What conditions must be met to ensure that personal data are processed lawfully?

The processing of personal data is permitted under the following conditions:

1) processing of personal data is carried out with the consent of the subject of personal data to the processing of his personal data;

2) processing of personal data is necessary to achieve the goals stipulated by an international treaty of the Russian Federation or the law for the implementation and fulfilment of the functions, powers and duties assigned by the legislation of the Russian Federation to the operator;

3) processing of personal data is carried out in connection with the participation of a person in constitutional, civil, administrative, criminal proceedings, proceedings in arbitration courts;

3.1) processing of personal data is necessary for the execution of a judicial act, an act of another body or official, subject to execution in accordance with the legislation of the Russian Federation on enforcement proceedings;

4) processing of personal data is necessary to fulfil the powers of federal executive bodies, state extra-budgetary funds, executive bodies of state power of the constituent entities of the Russian Federation, local governments and the functions of organisations involved in the provision of state and municipal services, respectively, including the registration of a personal data subject portal of state and municipal services and (or) regional portals of state and municipalities mortgage services;

5) processing of personal data is necessary for the execution of the contract, to which either the subject of personal data is a party or beneficiary, and also to enter into an agreement on the initiative of a personal data subject or a contract for which the subject of personal data will be a beneficiary or surety;

6) processing of personal data is necessary to protect the life, health or other vital interests of the subject of personal data, if the consent of the subject of personal data is impossible;

7) processing of personal data is necessary to exercise the rights and legitimate interests of the operator or third parties, or to achieve socially significant goals, provided that this does not violate the rights and freedoms of the subject of personal data;

8) processing of personal data is necessary for the professional activities of a journalist and (or) the legal activities of the media or scientific, literary or other creative activities, provided that it does not violate the rights and legitimate interests of the subject of personal data;

9) processing of personal data is carried out for statistical or other research purposes, subject to the mandatory depersonalisation of personal data;

10) processing of personal data is carried out, access of an unlimited number of persons to which is provided by the subject of personal data or at his request (hereinafter – personal data made publicly available by the subject of personal data);

11) processing of personal data to be published or mandatory disclosure in accordance with federal law.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017)
"On personal data".

18. What are the conditions for the expression of consent?

The subject of personal data decides on the provision of his personal data and agrees to their processing freely, by his own will and in his interest. Consent to the processing of personal data must be specific, informed and conscious. The subject of personal data or his representative in any form allowing confirming the fact of his receipt, unless otherwise established by federal law, may give consent to the processing of personal data. In the case of obtaining consent for the processing of personal data from a representative of the subject of personal data, the authority of the representative to give consent on behalf of the subject of personal data is checked by the operator.

The subject of personal data may withdraw consent to the processing of personal data.

In cases stipulated by federal law, the processing of personal data is carried out only with the consent in writing of the subject of personal data. The written consent on paper is recognised as equivalent to a consent in the form of an electronic document signed in accordance with federal law with an electronic signature.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017)
"On personal data".

19. If the law foresees special categories of data, what are the conditions to ensure the lawfulness of processing of such data?

The processing of special categories of personal data is considered legal if it is carried out for the following reasons.

The second reason is the processing of publicly available personal data, if the subject of personal data makes them publicly available.

The third reason is the need to process personal data in connection with the implementation of international readmission agreements of the Russian Federation.

The fourth reason is the processing of personal data in accordance with Federal Law No. 8-FZ dated January 25, 2002 "On the All-Russian Population Census".

The fifth reason is the processing of personal data in accordance with the legislation governing the citizenship of the Russian Federation, insurance legislation, legislation on defence, security, countering terrorism, transport security, countering corruption, criminal investigation executive legislation, as well as legislation on state social assistance, labor and pension legislation.

The sixth reason is that the operator carries out personal data activities in the field of the exercise of prosecutorial oversight by prosecution authorities, as well as the administration of justice.

The seventh basis is the processing of special categories of data by certain categories of personal data operators and the purpose of such processing. The following categories of operators were assigned:

- state bodies, municipal bodies or organisations for the purpose of arranging children left without parental care for upbringing in families of citizens;
- public associations or religious organisations to achieve the legitimate goals provided for by their constituent documents, which are only entitled to process the data of their members;
- persons who are professionally engaged in medical activities for medical and preventive purposes, in order to establish a medical diagnosis, the provision of medical and medical-social services.

The eighth reason is the need to process personal data in order to protect the life, health or other vital interests of the subject of personal data or the life, health or other vital interests of others.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data". Saveliev A.I. Scientific and practical article by article commentary to the Federal Law "On Personal Data". M.: Statute, 2017. 320 p.

20. What are the security requirements for collecting and processing personal data?

Ensuring the security of personal data is achieved, in particular, by:

1) identification of threats to the security of personal data when they are processed in personal data information systems;

2) the use of organisational and technical measures to ensure the security of personal data when processing them in personal data information systems necessary to meet the requirements for the protection of personal data, the performance of which ensures the levels of personal data protection established by the Government of the Russian Federation;

3) the use of the information security measures passed in the prescribed manner;

4) an assessment of the effectiveness of measures taken to ensure the security of personal data prior to the commissioning of the personal data information system;

5) registration of the machine carriers of personal data;

6) detection of facts of unauthorised access to personal data and taking measures;

7) recovery of personal data modified or destroyed due to unauthorised access to it;

8) the establishment of rules for access to personal data processed in the personal data information system, as well as ensuring the registration and accounting of all actions performed with personal data in the personal data information system;

9) control over measures taken to ensure the security of personal data and the level of security of personal data information systems.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data".

21. Is there a requirement to store (certain types of) personal data inside the jurisdiction?

There is no such requirement. When collecting personal data, including through the Internet information and telecommunications network, the operator is obliged to ensure the recording, systematisation, accumulation, storage, refinement (update, change), extraction of personal data of citizens of the Russian Federation using databases located in Federation.

Part 5 of Article 18 of the Federal Law "On Personal Data" enshrines the obligation of the operator to ensure the localisation of individual processes for the processing of personal data collected from Russian citizens. The provisions of this part came into

force on September 1, 2015 and have no analogues in foreign legal orders, in connection with which the issues of their interpretation and correlation with the provisions on cross-border data transfer are of particular relevance. The important role in this is also played by the possibility of blocking the operator's online resource, which processes personal data of citizens of the Russian Federation in violation of localisation requirements.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data". Saveliev A.I. Scientific and practical article by article commentary to the Federal Law "On Personal Data". M.: Statute, 2017. 320 p.

22. What are the requirements for transferring data outside the national jurisdiction?

According to the Council of Europe Convention on the Protection of Individuals in the automated processing of personal data, a party should not prohibit or condition cross-border personal data flows to the territory of the other Party with a special permit, for the sole purpose of protecting privacy.

Nevertheless, each Party has the right to deviate from this principle,

a) to the extent that its domestic law includes special rules for certain categories of personal data or automated personal data files because of the nature of the data or these files, unless the rules of the other Party provide for the same protection;

b) when a transfer is made from its territory to the territory of a state that is not a Party to this Convention, through the territory of the other Party, in order to prevent such a transfer, which would bypass the legislation of the Party mentioned at the beginning of this paragraph.

Cross-border transfer of personal data to the territory of foreign states that are parties to the Council of Europe Convention on the Protection of Individuals in the automated processing of personal data,

as well as other foreign states that provide adequate protection of the rights of personal data subjects, may be prohibited or restricted in order to protect the foundations of the constitutional system of the Russian Federation, morality, health, rights and legitimate interests of citizens, ensuring the defence of the country and the security of the state.

Roskomnadzor, as an authorised body for the protection of the rights of personal data subjects, approves the list of foreign states that are not parties to the Council of Europe Convention on the Protection of Individuals in the automated processing of personal data and ensure adequate protection of the rights of personal data subjects.

Cross-border transfer of personal data on the territory of foreign states that do not provide adequate protection of the rights of personal data subjects may be carried out in the following cases:

1) the existence of a written consent of the subject of personal data on the cross-border transfer of his personal data;

2) stipulated by international treaties of the Russian Federation;

3) provided for by federal laws, if it is necessary in order to protect the foundations of the constitutional system of the Russian Federation, to ensure the defence of the country and the security of the state, as well as to ensure the safety of a sustainable and safe operation of the transport complex, to protect the interests of the individual, society and the state in the sphere of the transport complex from acts of unlawful interventions;

4) the execution of the contract to which the subject of personal data is party;

5) protection of life, health, other vital interests of the subject of personal data or other persons when it is impossible to obtain written consent of the subject of personal data.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data"; Convention on the protection of individuals in the automated processing of personal data. Concluded in Strasbourg on January 28, 1981 (together with the Amendments to the Convention on the Protection of Individuals with the Automated Processing of Personal Data (CETS No. 108), allowing the accession of the European Communities adopted by the Committee of Ministers in Strasbourg on 15.06.1999).

23. Are data transfer agreements foreseen by the law?

Cross-border transfer of personal data on the territory of foreign states that do not provide adequate protection of the rights of personal data subjects may be carried out in cases provided for by international treaties of the Russian Federation.

At the same time, not only intergovernmental agreements, but also intergovernmental agreements and agreements of an interdepartmental nature, both bilateral and multilateral, are considered as international treaties of the Russian Federation.

The above international agreements may not contain the terms "cross-border transmission", "personal data", however the content of specific norms of such agreements or agreements as a whole should be directed specifically to actions that are classified by personal data legislation as cross-border data transmission.

The law does not require the preparation of an agreement on the transfer of personal data and their approval by an authorised body.

The authorised body for the protection of the rights of personal data subjects approves the list of foreign states that are not parties to the Council of Europe Convention on the Protection of Individuals in the automated processing of personal data and ensure adequate protection of the rights of personal data subjects.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12. 2017) "On personal data"; "Federal Law" On Personal Data ": Scientific and practical commentary" (article by article). Issue 11. Ed. A.A. Priezhzheva. "The Editors of the" Rossiyskaya Gazeta ", 2015.

24. Does the relevant national regulator need to approve the data transfer agreements?

The law does not require the preparation of an agreement on the transfer of personal data and their approval by an authorised body.

The authorised body for the protection of the rights of personal data subjects approves the list of foreign states that are not parties to the Council of Europe Convention on the Protection of Individuals in the automated processing of personal data and ensure adequate protection of the rights of personal data subjects.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017)
"On personal data"

25. What are the sanctions and remedies foreseen by the law for not complying with the obligations?

unlawful refusal of an official to present to a citizen documents and materials collected in accordance with the established procedure and directly affecting his rights and freedoms of a citizen (**Article 140** of the Criminal Code of the Russian Federation).

Source: Who and what is responsible for violation of the law on personal data. Prepared by the experts of the JSC "Consultant Plus" // "Consultant Plus" Legal Reference System, 2019.

▪ Actors

26. What actors are responsible for the implementation of the data protection law?

Administrative responsibility is established for:

- violation of the rules for processing personal data;
- failure to perform duties when interacting with a citizen – the subject of personal data;
- non-compliance with personal data protection requirements;
- failure to perform duties when interacting with Roskomnadzor.

Violation of legislation in the field of personal data may entail civil liability in the form of compensation for moral damage, compensation for damages, and recovery of a penalty, if it was provided by the contract.

The employee and the employer are liable for violations of personal data laws.

In this case, the employer may be materially liable to their employees.

An employee can be brought both to disciplinary and to material liability if it is his fault in the processing of personal data that violates the legislation in the field of personal data.

There is no special rule on liability for violation of the Personal Data Law in the Criminal Code of the Russian Federation. However, the actions of a person who has violated the rules for working with personal data may form a corpus delict from among those provided for by the Criminal Code of the Russian Federation.

In particular, criminal liability is established for:

- unlawful collecting or disseminating information about the private life of a person constituting his personal and family secrets, without his consent (Part 1 of Art. 137 of the Criminal Code of the Russian Federation);
- unauthorised access to computer information, which resulted in the destruction, blocking, modification (modification) or copying of information (part 1 of Art. 272 of the Criminal Code of the Russian Federation);

The Federal Service for Supervision in the Field of Communications, Information Technologies and Mass Communications (Roskomnadzor) is a federal executive body responsible for monitoring and supervising the compliance of personal data processing with the requirements of the legislation of the Russian Federation in the field of personal data. The Federal Service for Supervision of Communications, Information Technology and Mass Communications is an authorised federal executive body for the protection of the rights of personal data subjects.

Resolution of the Government of the Russian Federation of 16.03.2009 N 228 (Ed. 02/28/2019) "On the Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies and Mass Communications" (along with the "Regulations on the Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies and Mass Communications").

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

The Federal Service for Supervision in the Sphere of Communications, Information Technologies and Mass Communications (Roskomnadzor) is under the jurisdiction of the Ministry of Digital Development, Communications and Mass Communications of the Russian Federation. As part of it, the Office for the Protection of Rights of Subjects of Personal Data of the Federal Service for Supervision in the Sphere of Communications, Information Technology and Mass Communications is formed. It is a structural unit of the Federal Service for Supervision of Communications, Information Technologies and Mass Communications. The department of keeping the register of operators engaged in the processing of personal data, the Department for control and supervision of the processing of personal data, and the Department of the Legal and methodological support. The relevant departments are formed in the 71 territorial body of Roskomnadzor.

Resolution of the Government of the Russian Federation of 16.03.2009 N 228 (Ed. 28.02.2019) "On the Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies and Mass Communications" (along with the "Regulations on the Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies and Mass Communications") Official Website of Roskomnadzor. URL: <https://pd.rkn.gov.ru/authority/authority-structure/>.

28. What are the powers of the actors responsible for the implementation of the data protection law?

The activity of the control and supervision body aimed at preventing, detecting and stopping the violation by operators of personal data of the requirements of the Federal Law "On Personal Data" and the regulatory legal acts adopted in accordance with it by:

a) the organisation and conduct of scheduled and unscheduled inspections;

b) taking measures to suppress and (or) eliminate the consequences of the violations found;

c) control measures without interaction with operators;

d) measures for the prevention of violations.

Within these powers, Roskomnadzor:

- keeps a register of operators engaged in the processing of personal data;
- considers appeals of the subject of personal data about the compliance of the content of personal data and methods of their processing with the purposes of their processing and makes the appropriate decision;
- cooperates with the authorities authorised to protect the rights of personal data subjects in foreign countries, in particular the international exchange of information on the protection of the rights of personal data subjects;
- annually sends a report on its activities to the President of the Russian Federation, the Government of the Russian Federation and the Federal Assembly of the Russian Federation.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data". Resolution of the Government of the Russian Federation of 16.03.2009 N 228 (Ed. 28.02.2019) "On the Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies and Mass Communications" (along with the "Regulations on the Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies and Mass Communications").

2. Consumer Protection

▪ Scope

29. What national laws (or other types of normative acts) regulate consumer protection?

Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) "On Protection of Consumer Rights"

Civil Code of the Russian Federation (Part One) of 30.11.1994 N 51-FZ (as amended on 08/03/2018, entered into force on 01.01.2019).

Civil Code of the Russian Federation (Part Two) dated January 26, 1996 N 14-FZ (as amended on 29.07.2018, entered into force on 30.12.2018).

Civil Code of the Russian Federation (part three) dated 26.11.2001 N 146-FZ (as amended on 08/03/2018, entered into force on 01.09.2018).

Civil Code of the Russian Federation (Part Four) dated December 18, 2006 N 230-FZ (as amended on 23.05.2018).

"Consultant Plus" Legal Reference System.

30. Is the country a party of any international consumer protection agreement?

Agreement on the main areas of cooperation of the States members of the Commonwealth of Independent States in the field of consumer protection (concluded in Moscow on 25.01.2000).

Protocol on Amendments to the Agreement on the Main Directions of Cooperation of the States Parties of the Commonwealth of Independent States in the Field of Consumer Protection of January 25, 2000 (Together with the Regulations on the Consultative Council on Consumer Rights Protection of the CIS Member States). Signed in Minsk on 19.05.2011.

"Consultant Plus" Legal Reference System.

31. To whom do consumer protection laws apply?

The subjects of legal relations in the field of consumer protection are citizens who have the intention to order or purchase or ordering, purchasing or using goods (works, services) solely for personal, family, household and other needs not related to entrepreneurial activities, and business entities (organisations regardless of their organisational and legal form, as well as individual entrepreneurs), acting as sellers, manufacturers, performers or importers on consumer market.

Review of the practice of courts hearing cases on consumer protection disputes related to the sale of goods and services (approved by the Presidium of the Supreme Court of the Russian Federation on 17.10.2017).

32. Do the laws apply to foreign entities that do not have physical presence in the country?

The parties to the contract may, at the conclusion of the contract or subsequently select, by agreement among themselves, the law to be applied to their rights and obligations under the contract.

The choice of the applicable law to the contract to which the consumer is a party cannot entail depriving an individual (consumer) of his rights protection provided by the mandatory rules of the law of the consumer's country of residence if the consumer's counterparty (professional party) operates in the country of place residence of the consumer or by any means directs its activities to the territory of this country or the territory of several countries, including the territory of the country of residence will consume ate, provided that the contract is related to such activity of the professional party.

In the absence of agreement of the parties on the applicable law and in the circumstances specified above, the law of the country of residence of the consumer shall apply to the contract with the participation of the consumer.

The choice of the applicable law to the contract with the participation of the consumer cannot entail depriving the consumer of the protection of his rights provided by the mandatory rules of the country whose law would apply to this contract without the parties' agreement on the choice of law.

Civil Code of the Russian Federation (part three) dated 26.11.2001 N 146-FZ (as amended on 08/03/2018, entered into force on 01.09.2018).

▪ Definitions

33. How is consumer protection defined?

Consumer protection refers to the relationship between consumers and manufacturers, performers, importers, sellers, owners of aggregators of information about goods (services) in the sale of goods (performance of works, rendering services). The law establishes the rights of consumers to purchase goods (works, services) of adequate quality and safe for life, health, property of consumers and the environment, obtaining information about goods (works, services) and their manufacturers (performers, sellers), owners of information aggregators about goods (services), education, state and public protection of their interests, and also determines the mechanism for the realisation of these rights.

Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) "On Protection of Consumer Rights".

34. How are consumers defined?

Consumer – a citizen who has the intention to order or purchase or ordering, purchasing or using goods (works, services) solely for personal, family, household and other needs not related to the business.

Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) "On Protection of Consumer Rights".

35. How are providers and producers defined?

Manufacturer – an organisation regardless of its organisational and legal form, as well as an individual entrepreneur, producing goods for sale to consumers; contractor – an organisation, regardless of its organisational and legal form, as well as an individual entrepreneur performing work or providing services to consumers under a paid agreement; the seller is an organisation regardless of its organisational and legal form, as well as an individual entrepreneur who sells goods to consumers under a purchase and sale agreement.

Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) "On Protection of Consumer Rights".

36. Does the law provide any specific definitions with regards to consumer protection in the digital sphere?

Selling goods remotely – selling goods under a retail sale contract concluded on the basis of the buyer's familiarisation with the description of the goods offered by the seller, contained in catalogues, brochures, booklets or presented on photographs or using postal networks,

telecommunications networks, including information and telecommunications network "Internet", as well as communication networks for broadcasting TV channels and (or) radio channels, or in other ways, excluding the possibility of direct familiarisation of the buyer with the goods or sample of goods at the conclusion of such a contract.

Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) "On Protection of Consumer Rights". Decree of the Government of the Russian Federation of 27.09. 2007 No. 612 (as amended on 04.10.2012) "On the approval of the Rules for the sale of goods by remote means".

Rights

37. Is the consumer protection law based on fundamental rights (defined in Constitutional law or International binding documents)?

The legal basis for consumer protection is the Constitution of the Russian Federation, Federal laws, regulations of the President of the Russian Federation and the Government of the Russian Federation, as well as the United Nations Guidelines for Consumer Protection adopted by the United Nations General Assembly on December 22, 2015, by resolution N 70/186.

According to the Constitution of the Russian Federation, the state protection of the rights and freedoms of man and citizen in the Russian Federation is guaranteed. Everyone has the right to protect their rights and freedoms by all means not prohibited by law. In addition, everyone is guaranteed judicial protection of his rights and freedoms. Decisions and actions (or inaction) of state authorities, local governments, public associations and officials may be appealed in court.

Everyone has the right, in accordance with the international treaties of the Russian Federation, to apply to interstate bodies for the protection of human rights and freedoms if all available domestic remedies have been exhausted.

The Constitution of the Russian Federation (adopted by popular vote on 12/12/1993, as amended by the laws of the Russian Federation on amendments to the Constitution of the Russian Federation of 12/30/2008 N 6-FKZ, of 12/30/2008 N 7-FKZ, of 05.02.2014 N 2-FKZ, dated 07.21.2014 N 11-FKZ). Order of the Government of the Russian Federation of 28.08.2017 N 1837-p on approval of the Strategy of the state policy of the Russian Federation in the field of consumer protection for the period until 2030.

38. What are the rights of the consumer defined by the law with reference to digital good and services?

The consumer has the right to refuse to pay for such works (services), and if they are paid for, the consumer has the right to demand the seller to return the amount paid.

The consumer has the right to refuse the goods at any time before its transfer, and after the transfer of the goods – within 7 days.

If information on the procedure and deadlines for returning goods of good quality was not provided in writing at the time of delivery of the goods, the consumer has the right to refuse the goods within 3 months from the moment of transfer of the goods.

If there are defects in the goods for which no warranty or expiration dates have been established, the consumer has the right to make demands regarding the defects of the goods within a reasonable time, but within 2 years from the date of transfer to the buyer, if law or contract does not establish longer periods.

The consumer also has the right to make claims to the seller regarding the defects of the goods, if they are found during the warranty period or shelf life.

The consumer to whom the product of inadequate quality is sold, if this has not been stipulated by the seller, has the right to demand at its choice:

a) free elimination of defects in the goods or reimbursement of the costs of their correction by the buyer or a third party;

b) a commensurate reduction in the purchase price;

c) replacement for a product of a similar brand (model, article) or for the same product of another brand (model, article) with a corresponding recalculation of the purchase price. At the same time with respect to technically complex and expensive goods, these requirements of the buyer are subject to satisfaction in case of detection of significant shortcomings.

The consumer has the right to refuse to perform the contract and to demand the return of the amount paid for the goods. At the request of the seller and at his expense, the consumer must return the goods with defects.

The consumer also has the right to demand full compensation for damages caused to him because of the sale of goods of inadequate quality. Losses are reimbursed in the terms established by law to meet the relevant requirements of the buyer.

If the seller refuses to transfer the goods, the consumer has the right to refuse to perform the contract and demand compensation for the losses caused.

The consumer is not entitled to refuse the goods of good quality, which has individually defined properties, if exclusively the consumer acquiring it can use the specified goods.

Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) “On Protection of Consumer Rights”. Decree of the Government of the Russian Federation of September 27, 2007 No. 612 (as amended on 04.10.2012) “On the approval of the Rules for the sale of goods by remote means”.

39. Is consumer protection law applicable to users of zero price service i.e. free of charges?

In the case of a consumer acquiring digital content within the framework of free online services, the Law on Consumer Protection does not apply, which follows from the definition of “performer” – an organisation regardless of its organisational and legal form, as well as an individual entrepreneur performing work or providing services to consumers on paid agreement.

Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) “On Protection of Consumer Rights”. Saveliev A.I. Electronic commerce in Russia and abroad: legal regulation. Second ed. M.: Statute, 2016. 640 p.

▪ Obligations and Sanctions

40. Does the law establish specific security requirements to provide digital services or goods?

The consumer has the right to ensure that the product (work, service) under normal conditions of its use, storage, transportation and disposal is safe for the life, health of the consumer, the environment, and does not harm the property of the consumer. Requirements that must ensure the safety of a product (work, service) for the life and health of the consumer, the environment, and the prevention of harm to the property of the consumer are mandatory and are established by law or in the manner prescribed by it.

The manufacturer (performer) is obliged to ensure the safety of the goods (work) during the established service life or shelf life of the goods (work).

If the manufacturer (performer) has not established a service life for the goods (work), he is obliged to ensure the safety of the goods (work) within ten years from the day the goods (work) are transferred to the consumer.

Harm caused to the life, health or property of the consumer due to failure to ensure the safety of the goods (work) is refundable.

If for the safety of using a product (work, service), its storage, transportation and disposal it is necessary to observe special rules, the manufacturer (contractor) is obliged to indicate these rules in the accompanying documentation for the goods (work, service), on the label, marking or otherwise, and the seller (performer) is obliged to bring these rules to the attention of the consumer.

If, for goods (works, services), the law or in the procedure established by it establishes mandatory requirements ensuring their safety for the life, health of the consumer, the environment and preventing harm to the consumer's property, the conformity of goods (works, services) with these requirements is subject to mandatory confirmation stipulated by law and other legal acts.

Sale of goods (performance of work, provision of services), including imported goods (work, services), without information about the mandatory confirmation of its compliance with safety requirements is not allowed.

If it is established that if the consumer complies with the established rules for using, storing or transporting the goods (work), he causes or may harm the life, health and property of the consumer, the environment, the manufacturer (performer, seller) is obliged to immediately suspend its production (sale) until it is eliminated causes of harm, and, if necessary, take measures to remove it from circulation and recall it from the consumer(s).

If the causes of harm cannot be eliminated, the manufacturer (performer) is obliged to remove such goods (work, service) from production. If the manufacturer (executor) fails to fulfil this obligation, the authorised federal executive body takes measures to recall such goods (work, services) from the domestic market and (or) from consumers or consumers in the manner prescribed by the legislation of the Russian Federation.

Losses caused to the consumer in connection with the recall of the goods (work, services) are subject to compensation by the manufacturer (performer) in full.

The following goods shall be recognised as not meeting the requirements of safety of life and health of consumers: a) for which a refusal to issue a certificate of conformity to the safety requirements specified in the standards was received; b) certification for compliance with the established safety requirements for such goods that has not passed; c) with an unspecified expiration date and with unspecified special rules for safe use, storage, transportation and disposal.

Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) "On Protection of Consumer Rights". Commentary to the Criminal Code of the Russian Federation: in 4 tons (itemised) / A.V. Brilliantov, A.V. Galakhov, V.A. Davydov et al.; rep. ed. V.M. Lebedev. M.: Yurayt, 2017. V. 3: The special part. Section IX. 298 p.

41. What are the sanctions and remedies foreseen by the law for now complying with the obligations?

For violation of consumer rights established by laws and other regulatory legal acts of the Russian Federation, the seller (performer, manufacturer, authorised organisation or authorised individual entrepreneur, importer) bears administrative, criminal or civil liability in accordance with the legislation of the Russian Federation.

Administrative responsibility is provided for the sale of goods, the performance of work or the provision of services to the population of inadequate quality or in violation of the requirements established by the legislation of the Russian Federation, as well as in the absence of established information. It also provides for administrative liability for consumer fraud, violation of other consumer rights and violation of the rules for the sale of certain types of goods.

Criminal liability is provided for violation of sanitary and epidemiological rules, production, storage, transportation or sale of goods and products, performance of work or provision of services that do not meet safety requirements, as well as for the circulation of counterfeit, substandard and unregistered medicines, medical products and trafficking in biologically active additives.

Civil liability for violation of consumer protection laws is established in the form of compensation for damages, compensation for harm caused by deficiencies in goods, works or services, as well as in the form of compensation for moral harm.

Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) "On Protection of Consumer Rights". Code of the Russian Federation on Administrative Offenses dated December 30, 2001 No. 195-FZ (as amended on May 01, 2019). Criminal Code of the Russian Federation of 13.06.1996 N 63-FZ (as amended on 04.23.2019). Civil Code of the Russian Federation (Part One) of 30.11.1994 N 51-FZ (as amended on 03.08.2018, as amended and added, took effect from 01.01.2019). The Civil Code of the Russian Federation (Part Two) dated January 26, 1996 N 14-FZ (as amended on 07/29/2018, as amended and added, entered into force on December 30, 2018).

▪ Actors

42. What bodies are responsible for the implementation of the consumer protection law?

Federal state supervision in the field of consumer rights protection is carried out by an authorised federal executive body in this area.

The highest executive body of state power of the relevant subject of the Russian Federation takes measures to implement, ensure and protect the rights of consumers and within its authority.

Consumer protection on the territory of the municipal entity is carried out by local authorities.

Citizens have the right to unite on a voluntary basis into public associations of consumers (their associations, unions), which carry out their activities in accordance with the charters of these associations (their associations, unions) and the legislation of the Russian Federation.

Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) "On Protection of Consumer Rights".

43. Is there a specific consumer protection body? If so, what is its administrative structure?

Federal state supervision in the field of consumer protection is carried out by the Federal Service for Supervision of Consumer Rights Protection and Human Welfare

The Federal Service for Supervision of Consumer Rights Protection and Human Welfare is headed by a leader appointed to office and dismissed by the Government of the Russian Federation.

The head of the Federal Service for Supervision of Consumer Rights Protection and Human Welfare is the chief state sanitary doctor of the Russian Federation.

The Head of the Federal Service for Supervision of Consumer Rights Protection and Human Welfare is personally responsible for the implementation of the functions assigned to the Service.

The head of the Federal Service for Supervision of Consumer Rights Protection and Human Welfare has deputies appointed to office and dismissed from office by the Government of the Russian Federation on the proposal of the head of the Service.

The deputy heads of the Federal Service for Supervision of Consumer Rights Protection and Human Welfare, performing the functions of organizing and implementing federal state sanitary and epidemiological supervision, are deputy chief state sanitary doctor of the Russian Federation.

The number of deputy heads of the Federal Service for Supervision of Consumer Rights Protection and Human Welfare is established by the Government of the Russian Federation.

Decree of the Government of the Russian Federation of 02.05.2012 N 412 (ed. of 14.12.2018) "On approval of the Regulation on federal state supervision in the field of consumer rights protection".

Decree of the Government of the Russian Federation of 30.06.2004, N 322 (as amended on 26.03.2019) "On the approval of the Regulations on the Federal Service for Supervision of Consumer Rights Protection and Human Welfare".

44. What are the powers of the bodies responsible for the implementation of the consumer protection law?

1) organizing and conducting inspections of compliance by manufacturers (performers, sellers, authorised organisations or authorised individual entrepreneurs, importers, owners of aggregators) with the requirements established by international treaties of the Russian Federation, the Law on Consumer Protection, other federal laws and other regulatory legal acts of the Russian Federation, regulating relations in the field of consumer rights protection, regulations of officials of the state supervision body but;

2) organizing and conducting inspections of the conformity of goods (works, services) to mandatory requirements ensuring the safety of goods (works, services) for the life and health of consumers, the environment, preventing actions that mislead consumers, and preventing harm to consumers' property set forth in compliance with international treaties of the Russian Federation, federal laws and other regulatory legal acts of the Russian Federation;

3) applying, in accordance with the procedure established by the legislation of the Russian Federation, preventive measures for violating mandatory requirements, issuing orders to terminate violations of consumer rights, to terminate violations of mandatory requirements, to eliminate identified violations of mandatory requirements, to bring to justice the persons who committed such violations;

4) systematic observation of the fulfilment of mandatory requirements, analysis and forecasting of the state of fulfilment of mandatory requirements when manufacturers (performers, sellers, authorised organisations or authorised individual entrepreneurs, importers, owners of aggregators) carry out their activities;

5) statistical observation in the field of consumer protection, accounting and analysis of cases of harm to life and health of consumers, the environment and property of consumers associated with the acquisition and use of goods (works, services) with disabilities, hazardous goods (works, services) or with providing consumers with untimely, incomplete, unreliable and misleading information about goods (works, services);

6) the annual analysis and evaluation of the effectiveness of federal state supervision in the field of consumer protection;

7) annual preparation of state reports on the protection of consumer rights in the Russian Federation in the manner established by the Government of the Russian Federation.

Law of the Russian Federation of 07.02.1992 N 2300-1 (as amended on 18.03.2019) "On Protection of Consumer Rights".

3. Cybercrime

▪ Scope

45. What national laws (or other types of normative acts) regulate cybercrime?

Chapter 28 "Crimes in the field of computer information" of the Criminal Code of the Russian Federation.

Criminal legislation of the Russian Federation consists of only the Criminal Code of the Russian Federation. New laws providing for criminal liability are subject to inclusion in this Code.

Criminal Code of the Russian Federation of 13.06.1996 N 63-FZ (as amended on 23.04.2019).

46. Is the country a part of any international cybercrime agreement?

The Russian Federation is a party to the Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Computer Information Offenses (concluded in Minsk on 06/06/2001). The Russian Federation ratified the Agreement with the following reservation: "The Russian Federation reserves the right to refuse execution of the request, in whole or in part, if the execution of the request is likely to prejudice its sovereignty or security."

Federal law of 01.10.2008 N 164-ФЗ "On ratification of the Agreement on cooperation of the States members of the Commonwealth of Independent States in the fight against crimes in the field of computer information".Order of the President of the Russian Federation of 15.11.2005 N 557-rp "On the signing of the Convention on Cybercrime". Order of the President of the Russian Federation of March 22, 2008 No. 144-rp "On declaring the decree of the President of the Russian Federation of November 15, 2005 No. 557-rp" On Signing the Convention on Cybercrime "invalid.

47. What cybercrimes are regulated?

a) implementation of unauthorised access to computer-protected information by law, if this act resulted in the destruction, blocking, modification or copying of information, disruption of the operation of a computer, computer system or their network;

b) the creation, use or distribution of malicious programs;

c) violation of the rules of operation of a computer, computer system or their network by a person having access to a computer, computer system or their network, resulting in the destruction, blocking or modification of information protected by law of a computer, if this act caused significant harm or serious consequences;

d) illegal use of computer programs and databases that are objects of copyright, as well as the assignment of authorship, if this act has caused significant damage;

Agreement on cooperation of the States members of the Commonwealth of Independent States in the fight against crimes in the field of computer information (concluded in Minsk 01.06.2001).

48. To whom do the laws apply?

An individual may be subject to a crime and criminal liability, if he has the minimum necessary set of features: has reached the legal age and is sane. These signs are mandatory to establish the responsibility of all persons involved in the crime – the performers, organizers, instigators and collaborators. Criminal liability comes as a rule from the age of 16.

Commentary to the Criminal Code of the Russian Federation: in 4 volumes (itemised) / A.V. Brilliantov, A.V. Galakhova, V.A. Davydov et al.; ed. by V.M. Lebedev. M.: Yurayt, 2017. T. 1: General part. 316 p.

▪ Definitions

49. Do the laws apply to foreign entities that do not have physical presence in the country?

Foreign citizens and stateless persons who are not permanently residing in the Russian Federation who have committed a crime outside the Russian Federation are subject to criminal liability under this Code in cases where the crime is directed against the interests of the Russian Federation or a citizen of the Russian Federation or a stateless person residing in the Russian Federation as well as in cases stipulated by an international treaty of the Russian Federation or another document of an international character, containing liabilities recognised by the Russian Federation.

Criminal Code of the Russian Federation of 13.06.1996 N 63-FZ
(as amended on 23.04.2019).

50. How is cybercrime generally defined by the national law?

In the legislation there is no definition of a group of crimes, only individual crimes are defined. Computer-related crimes are defined as socially dangerous acts under criminal law that cause harm or create a danger of harm to the safety of the production, storage, use or dissemination of information or information resources.

Criminal Code of the Russian Federation of 13.06.1996 N 63-FZ
(as amended on 23.04.2019).

51. What are the cybercrimes provided for by the law and how are they defined?

Unauthorised access to the protected by the law computer information is unlawful or unauthorised use of the possibility of obtaining computer information by the owner or another of its legal owners.

Creation, distribution or use of computer programs or other computer information, which are intended for unauthorised destruction, blocking, modification, copying of computer information or neutralisation of computer information protection tools.

Violation of the rules for the use of storage, processing or transmission of protected computer information or information and telecommunication networks and terminal equipment, as well as rules for access to information and telecommunication networks, resulting in the destruction, blocking, modification or copying of computer information, which caused major damage.

Creation, distribution and (or) use of computer programs or other computer information, which are intended to improperly influence the critical information infrastructure of the Russian Federation, including for destroying, blocking, modifying, copying the information contained in it, or neutralizing the means of protecting this information .

Unauthorised access to protected computer information contained in the critical information infrastructure of the Russian Federation, including using computer programs or other computer information that are deliberately intended to improperly affect the critical information infrastructure of the Russian Federation, or other malicious computer programs, if it entailed causing damage to the critical information infrastructure of the Russian Federation.

Violation of the rules for the operation of the storage, processing or transmission of protected computer information contained in the critical information infrastructure of the Russian Federation, or information systems, information and telecommunication networks, automated control systems, telecommunication networks relating to the critical information infrastructure of the Russian Federation, or the rules for access to these information, information systems, information and telecommunication networks, automated systems management, telecommunication networks, if it resulted in damage to the critical information infrastructure of the Russian Federation.

Criminal law of Russia. General and Special parts: textbook / A.A. Aryamov, TB Basova, E.V. Blagov et al.; ed by Yu.V. Gracheva, A.I. Chuchaev. M.: CONTRACT, 2017. 384 p.

52. How is a computer system defined?

Information system is a set of information contained in databases and information technologies and technical means ensuring its processing.

Federal Law of 27.07.2006 N 149-ФЗ (as amended on 18.03.2019) "On Information, Information Technologies and on Information Protection".

54. How are computer data defined?

Computer information refers to information (messages, data) presented in the form of electrical signals, regardless of their means of storage, processing, and transmission.

Criminal Code of the Russian Federation of 13.06.1996 N 63-FZ (as amended on 23.04.2019).

55. How are forensic data defined?

Judicial computer-technical expertise is an independent type of forensic examinations conducted to determine the status of an object as a computer tool, determine its role in an investigated crime, and access information on electronic media with its subsequent comprehensive investigation.

Letter of the Federal Bailiff Service of Russia dated September 18, 2014 No. 00043/14/56151-BB "On Methodological Recommendations" (together with the "Methodological Recommendations on the Order of Appointment and Proceeding of Legal Expertise in Pre-Investigation and Investigation of Crimes Subject to the Federal Bailiff Service" approved by the FBS of Russia 15.09.2014 N 0004/22).

56. How are service providers defined?

Hosting provider – a person providing services for the provision of computing power for placing information in an information system that is constantly connected to the Internet.

Federal Law of 27.07.2006 N 149-ФЗ (as amended on 18.03.2019) "On Information, Information Technologies and on Information Protection".

57. Does the national law provide any other definitions instrumental to the application of cybercrime legislation?

The destruction of information is the reduction of information or its part into an unusable state, regardless of the possibility of its recovery. The destruction of information is not the renaming of

the file where it is contained, as well as the automatic "wipe out" of the old versions of the files by the latest;

Blocking information is the result of exposure to computer information or equipment, the consequence of which is the impossibility for some time or to constantly perform the required operations on computer information completely or in the required mode, that is, performing actions that lead to restriction or closure of access to computer equipment and resources, the obstruction of the access of legitimate users to computer information not related to its destruction;

Information modification – making changes to computer information (or its parameters);

Copying information – creating a copy of existing information on another medium, that is, transferring information to a separate carrier while maintaining the original information unchanged, reproducing information in any material form – by hand, photographing text from the display screen, as well as reading the information by any interception of information, etc.

A computer program is an objective form of representing a set of data and commands intended for the functioning of a computer device in order to obtain a certain result.

Creation of programs is an activity aimed at developing, preparing programs that are capable of unauthorised destruction, blocking, modifying, copying of computer information or neutralizing computer information protection tools.

The distribution of such programs means the provision of access to any unauthorised person in any of the possible ways, including selling, renting, sending free of charge via the electronic network, that is, any actions to provide access to the program via network or other means.

Using the program is working with the program, applying it for its intended purpose and other actions to introduce it into economic circulation in its original or modified form. Under the use of malicious programs refers to their use (by any person), in which their harmful properties are activated.

Guidelines for the implementation of prosecutorial supervision over the implementation of laws in the investigation of crimes in the field of computer information (approved by the Prosecutor General's Office of Russia).

- **Rights**

58. Is the cybercrime law based on fundamental rights (defined in Constitutional law or International binding documents)?

The provision on its highest legal force enshrined in the Constitution of the Russian Federation means that all constitutional norms have the supremacy over laws and other regulatory legal acts.

In accordance with **Art. 18** of the Constitution of the Russian Federation, the rights and freedoms of a person and a citizen are directly applicable. They determine the meaning, content and application of laws, the activities of the legislative and executive authorities, local self-government and are ensured by justice.

Generally recognised principles and norms of international law enshrined in international covenants, conventions and other documents (in particular, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights), and international treaties of the Russian Federation are in accordance with **Part 4 of Art. 15** of the Constitution of the Russian Federation an integral part of its legal system. The same constitutional norm determines that if an international treaty of the Russian Federation establishes other rules than those provided by law, then the rules of the international treaty apply.

Taking this into account, the court does not have the right to apply the norms of the law regulating the legal relations that arose, if an international agreement entered into force for the Russian Federation, the decision on consent to which the Russian Federation was made in the form of federal law, establishes other rules than those provided by law . In these cases, the rules of the international treaty of the Russian Federation.

Constitution of the Russian Federation (adopted by popular vote on 12.12.1993, with the amendments made by the Laws of the Russian Federation on amendments to the Constitution of the Russian Federation of 30.12.2008 No. 6-FKZ, of 30.12.2008 No. 7-FKZ, of 02.05.2014 N 2-FKZ, of 21.07.2014 N 11-FKZ). Resolution of the Plenum of the Supreme Court of the Russian Federation of October 31, 1995 N 8 (ed. 03/03/2015) "On some issues of the application by courts of the Constitution of the Russian Federation in the administration of justice".

59. What are the rights of the victim and the accused?

The most significant rights granted to a victim are the following:

1) to know about the accusation against the accused.

2) to testify.

3) to get acquainted with the decision on the appointment of a forensic examination and with the expert opinion.

4) the special right of victims is the receipt of copies of the procedural and judicial acts of the criminal case.

5) to know about complaints and representations brought in a criminal case and to file objections to them.

6) the victim's special right is his participation in the court hearing.

Everyone charged with a criminal offence is presumed innocent until his guilt is established by law.

Everyone charged with a criminal offence has at least the following rights:

a) to be immediately and in detail notified in a language understandable to him of the nature and cause of the accusation against him;

b) to have adequate time and facilities for the preparation of his defence;

c) to defend himself personally or through a defender chosen by him or, with a lack of funds to pay for counsel, to use the services of his appointed defender for free when the interests of justice so require;

d) Interrogate witnesses who testify against him or have the right to be interrogated by these witnesses, and have the right to call and interrogate witnesses in his favour under the same conditions as for witnesses against him;

e) use the free help of a translator if he does not understand the language used in court or does not speak that language.

The Criminal Procedure Code of the Russian Federation has significantly expanded the rights of the victim of a crime, making it a more active participant in the criminal process. However, analysis of legislation and law enforcement practice shows that in Russia, victims both legally and in fact are in a disadvantaged position, the level of legal protection of the victim is significantly lower than the suspect and the accused. The constitutional principle of legal proceedings on the basis of adversarial and equal rights of the parties implies parity of the rights of the victim and the accused (suspect) as parties to the criminal dispute.

G.I. Zagorsky. M .: Prospect, 2016. 1216 p. "Convention for the Protection of Human Rights and Fundamental Freedoms" (concluded in the city of Rome on November 4, 1950, as amended on May 13, 2004). Smirnova I.S. Asymmetry of the rights of the victim and the accused (suspect) // Bulletin of the Omsk Law Academy. 2016. N 2. P. 59 – 62.

▪ Procedures

60. Is there a specific procedure to identify, analyse, relate, categorize, assess and establish causes associated with forensic data regarding cybercrimes?

The objects of the study of forensic computer technical expertise are computing equipment, software products, and information objects. In this regard, within the framework of this forensic examination, hardware-computer, software-computer, information-computer research can be conducted.

The purpose of software and computer research is to study the functional purpose, characteristics, structural features, and the current state of the computer system software presented for the study.

Information-computer research is key in the production of forensic computer-technical expertise, as it allows you to complete the holistic construction of the evidence base by final resolution of most issues related to computer information.

The main objectives of this study are the search, detection, analysis and evaluation of information prepared by the user or created by programs for organizing information processes in a computer system.

In the production of information and computer research in the framework of computer-technical expertise can distinguish the following tasks:

- establishing the properties and type of information presented in a computer system when it is used directly;
- determination of the actual state of information;

- establishing the initial state of information on the data carrier;
- determination of time, chronological sequence of impact on information;
- determination of conditions for changing the properties of the studied information.

00043/14/56151-BB "On Methodological Recommendations" (together with the "Methodological Recommendations on the Order of Appointment and Proceeding of Legal Expertise in Pre-Investigation and Investigation of Crimes Subject to the Federal Bailiff Service" approved by the FBS of Russia 15.09.2014 N 0004/22). Order of the FSS of Russia of 23.06.2011 N 277 (ed. 04.12.2017) "On the organisation of the production of forensic examinations in expert divisions of the federal security service" (together with the "Instructions on the organisation of the production of forensic examinations in expert divisions of the federal security service").

61. In case of transnational crimes, how is cooperation between the national law enforcement agency and the foreign agents regulated?

The parties within the framework of this Agreement on cooperation of the States members of the Commonwealth of Independent States in the fight against crimes in the field of computer information shall cooperate in the following forms:

a) the exchange of information, including:

on upcoming or committed crimes in the field of computer information and individuals and legal entities involved in them; on the forms and methods of prevention, detection, suppression, detection and investigation of crimes in this area; methods of committing crimes in the field of computer information; on national legislation and international treaties governing the prevention, detection, suppression, disclosure and investigation of crimes in the field of computer information;

b) the execution of requests for operational investigations, as well as legal proceedings in accordance with international treaties on legal assistance;

c) planning and conducting coordinated activities and operations for the prevention, detection, suppression, disclosure and investigation of crimes in the field of computer information;

d) assisting in the training and professional development of personnel, including through the training of specialists, the organisation of conferences, seminars and training courses;

e) creation of information systems ensuring the fulfilment of tasks for the prevention, detection, suppression, disclosure and investigation of crimes in the sphere of computer information;

f) conducting joint scientific research on issues of mutual interest in combating computer-related crime;

g) the exchange of regulatory legal acts, scientific and technical literature on the fight against crimes in the field of computer information;

h) in other mutually acceptable forms.

In accordance with a number of agreements on legal assistance in criminal matters, in cases that are not delayed, requests may be sent directly by the competent authorities of the requesting state to the

competent authorities of the Russian Federation, including through Interpol. In this case, a copy of the order is simultaneously transmitted to the relevant central competent authority.

Agreement on cooperation of the States members of the Commonwealth of Independent States in the fight against crimes in the field of computer information (Concluded in Minsk 01.06.2001). UNODC Cybercrime Repository. URL: <https://sherloc.unodc.org/cld/lessons-learned/rus/specific_channels_for_urgent_requests_for_mla_in_cybercrime_cases.html?&tmpl=cyb

62. Are there any exceptions to the use of mutual legal assistance procedure to investigate the crime?

The law does not address this question. According to the European Convention on Mutual Legal Assistance in Criminal Matters, assistance may be refused:

a) if the request concerns an offence which the requested Party considers a political offence, an offence connected with a political offence or a financial offence;

b) if the requested Party considers that the execution of the request may prejudice sovereignty, security, public order or other essential interests of its country.

The execution of a request under the Agreement on Cooperation of the States Parties of the Commonwealth of Independent States in the Fight against Computer Crime Offenses can be denied in full or in part if the requested Party believes that its execution is contrary to its national law.

The requesting Party shall be notified in writing of the complete or partial refusal to execute the request, indicating the reasons for refusal.

European Convention on Mutual Legal Assistance in Criminal Matters (ETS N 30) Concluded in the city of Strasbourg 04/20/1959, as amended on 08.11.2001). Agreement on cooperation of the States members of the Commonwealth of Independent States in the fight against crimes in the field of computer information (concluded in Minsk 01.06.2001

63. Does the national law require the use of measures to prevent cybercrimes? If so, what are they?

The organizer of information dissemination in the Internet is obliged to store in the territory of the Russian Federation:

1) information on the facts of reception, transmission, delivery and (or) processing of voice information, written text, images, sounds, video or other electronic messages of Internet users, and information about these users within one year from the end of the implementation of such action;

2) text messages of Internet users, voice information, images, sounds, video, other electronic messages of Internet users up to six months from the moment they have finished receiving, transmitting, delivering and (or) processing.

The organizer of the dissemination of information on the Internet is obliged to provide relevant information to authorised state bodies carrying out operational investigative activities or ensuring the security of the Russian Federation in cases established by federal laws.

The organizer of the dissemination of information on the Internet is obliged to ensure the implementation of the requirements for equipment and software and hardware used by the specified organizer in the field

of communication established by the federal executive body in the field of communications in coordination with the authorised state bodies carrying out operational and investigative activities information systems operated by him, for these bodies to conduct in cases established by the federal bubbled laws and measures in order to implement the tasks assigned to them, and to take measures to prevent the disclosure of organisational and tactical methods of carrying out these activities.

In order to counteract the use in the Russian Federation of software and hardware access to information resources, information and telecommunication networks, access to which is restricted, the federal executive body that performs the functions of control and supervision in the field of media, mass communications, information technology and communication:

1) carries out the creation and operation of a federal state information system containing a list of information resources, information and telecommunication networks, access to which is restricted in the territory of the Russian Federation;

2) in accordance with the procedure established by the Government of the Russian Federation, interacts with federal executive bodies carrying out operational investigative activities or ensuring the security of the Russian Federation in order to obtain information about software and hardware access to information resources, information and telecommunication networks, access to which limited;

3) on the basis of a request from the federal executive body carrying out operational investigative activities or ensuring the security of the Russian Federation, determines the hosting provider or other person who provides the placement on the Internet of software and hardware access to information resources, information and telecommunication networks, access to which is limited.

4) sends a notification to the hosting provider in electronic form in Russian and English about the need to provide data to identify the owner of the corresponding software and hardware;

5) fixes the date and time of sending the notification in the federal state information system of information resources, information and telecommunication networks, access to which is restricted.

Federal Law of 27.07.2006 N 149-ФЗ (as amended on 18.03.2019) "On Information, Information Technologies and on Information Protection".

▪ Obligations and Sanctions

64. What obligations do law enforcement agencies have to protect the data of the suspect, the accused and the victim?

In exceptional cases related to the proceedings in another criminal, civil or administrative case, information about the protected person may be submitted to the preliminary investigation authorities, the prosecutor's office or the court based on the written request of the prosecutor or the court (judge) with the permission of the authority that made the decision protection.

The procedure for implementing security measures in the form of ensuring the confidentiality of information about a protected person is established by the Government of the Russian Federation.

65. What are the duties and obligations of the National Prosecuting Authorities in cases of cybercrime?

The prosecution authorities carry out prosecutorial supervision at the stage of initiating criminal proceedings for crimes in the sphere of computer information, as well as for investigating crimes in the sphere of computer information.

The prosecutor must carefully check the legality of the initiation of criminal cases and evaluate the submitted materials.

Studying the submitted materials, the prosecutor must make sure that the facts stated in statements, materials of the departmental and other verification of the violation of the integrity (confidentiality) of information in the computer system, network are objectively confirmed; about the presence of a causal link between the illegal actions and the consequences provided for by the disposition of ***Art. 272*** and ***274*** of the Criminal Code of the Russian Federation, in the form of copying, destruction, modification, blocking of information (to initiate a criminal case under ***Article 273*** of the Criminal Code of the Russian Federation, the onset of such consequences is not necessary); about the preliminary amount of damage caused by criminal acts.

The supervising prosecutor needs to verify the completeness of the materials, the legitimacy of their receipt and subsequent submission to the investigating authority.

Given the complexity of investigating computer-related crimes, the low qualifications of investigators, the need to use special knowledge in investigations, prosecutorial oversight of investigating these crimes should be carried out throughout the entire period of investigation.

Given the characteristics of the category of crimes under consideration, the prosecutor should carefully examine the evidence gathered during the preliminary investigation, which should be fully established by all the circumstances provided for in ***Art. 73*** Code of Criminal Procedure. At the same time, as noted earlier, the composition of the crimes provided for by Chapter 28 of the Criminal Code of the Russian Federation, in addition to the main features of a crime, determines the causal link between the act and the consequences.

Studying a criminal case during the investigation, the prosecutor must establish whether these expert opinions fully answer the questions put by the investigator, whether all the necessary questions are put to the expert and whether the information contained in the expert's opinion is enough to confirm the circumstances of the crime. Undoubtedly, the supervising prosecutor should have special knowledge of the types of forensic examinations conducted in criminal cases of this category, and give appropriate recommendations to the head of the investigative body.

If the prosecutor reveals a violation that has already been committed during the preliminary investigation, he must use the powers granted to him by the Criminal Procedure Code of the Russian

Federation and make a request to eliminate the violations committed during the preliminary investigation.

In accordance with ***Art. 221*** of the Criminal Procedural Code of the Russian Federation, the prosecutor or his deputy must consider the received criminal case within a period not exceeding ten days and take one of the following decisions:

- on the approval of the indictment and the direction of the criminal case to the court;
- on the return of the criminal case to the investigator for additional investigation, changing the scope of the prosecution or qualifying the actions of the accused or re-drafting the indictment and eliminating the identified deficiencies with their written instructions;
- on the direction of the criminal case to a higher prosecutor for the approval of the indictment, if it is subject to the jurisdiction of the higher court.

The prosecutor in accordance with paragraph. 2 h. 1 ***Article 221*** of the Code of Criminal Procedure has the right to return the criminal case to the investigator for additional investigation, changing the scope of the prosecution or qualifying the actions of the accused or reconsidering the indictment and eliminating the identified deficiencies with their written instructions. Currently, the court does not have such a right, but it can return the criminal case to the prosecutor, if there are grounds provided for by ***Art. 237*** Code of Criminal Procedure, which, as a rule, testifies to inadequate prosecutor's supervision over the course of the preliminary investigation.

The hosting provider is obliged to provide data that allows identifying the owner of the news aggregator or audio-visual service.

The hosting provider is obliged to notify the site owner serviced by him on the Internet about the need to remove a web page containing information whose distribution in the Russian Federation is prohibited.

If information is found in information and telecommunication networks, including the Internet, expressing in an indecent form that offends human dignity and public morality, obvious disrespect for society, the state, official state symbols of the Russian Federation, the Constitution of the Russian Federation or to the authorities exercising state power in the Russian Federation, the hosting provider is obliged to inform the information resource owner that they serve ask him to immediately remove such information.

In case of failure or inaction of the owner of an information resource, the hosting provider is obliged to limit access to the relevant information resource immediately after the expiration of the day from the date of receipt of the notification about it.

The hosting provider is obliged to limit access to the information resource that disseminates information that violates copyright and related rights no later than the expiration of three working days from the date of receipt of the relevant notice.

Within one working day from the date of receipt from Roskomnadzor of a notice of cancellation of measures to restrict access to an information resource, the hosting provider is obliged to inform the owner of the information resource and notify about the possibility of lifting the access restriction.

In the case of detection in information and telecommunication networks, including the Internet, the information disseminated in violation of the law, i.e. containing calls for mass riots, extremist activities, participation in mass (public) events held in violation of the established procedure, inaccurate socially important information distributed under the guise of reliable messages, which creates a threat of harm to life and / or citizens' health, property, the threat of mass violation of public order and (or) public safety or the threat of interfering with the functioning or termination of the functioning of life transport or social infrastructure, credit organisations, energy facilities, industry or communications, information materials of a foreign or international non-governmental organisation whose activity is considered undesirable in the territory of the Russian Federation, the hosting provider is obliged to inform the hosting provider about the information owner of the information resource served by them and notify him of the need to immediately remove unlawfully distributed information.

The hosting provider is obliged to notify the owner of the information resource serviced by him about the need to immediately take measures to eliminate violations of the legislation of the Russian Federation in the field of personal data, or take measures to restrict access to information processed in violation of the legislation of the Russian Federation in the field of personal data.

At the request of Roskomnadzor, the hosting provider is obliged to provide data allowing identification of the owner of software and hardware access to information resources, information and telecommunication networks, access to which is restricted.

Federal Law of 27.07.2006 N 149-ФЗ (as amended on 18.03.2019) "On Information, Information Technologies and on Information Protection".

66. Does the law impose any obligations on service providers in connection with cybercrime?

The hosting provider is obliged to provide data that allows identifying the owner of the news aggregator or audio-visual service.

The hosting provider is obliged to notify the site owner serviced by him on the Internet about the need to remove a web page containing information whose distribution in the Russian Federation is prohibited.

If information is found in information and telecommunication networks, including the Internet, expressing in an indecent form that offends human dignity and public morality, obvious disrespect for society, the state, official state symbols of the Russian Federation, the Constitution of the Russian Federation or to the authorities exercising state power in the Russian Federation, the hosting provider is obliged to inform the information resource owner that they serve ask him to immediately remove such information.

In case of failure or inaction of the owner of an information resource, the hosting provider is obliged to limit access to the relevant information resource immediately after the expiration of the day from the date of receipt of the notification about it.

The hosting provider is obliged to limit access to the information resource that disseminates information that violates copyright and related rights no later than the expiration of three working days from the date of receipt of the relevant notice.

Within one working day from the date of receipt from Roskomnadzor of a notice of cancellation of measures to restrict access to an information resource, the hosting provider is obliged to inform the owner of the information resource and notify about the possibility of lifting the access restriction.

In the case of detection in information and telecommunication networks, including the Internet, the information disseminated in violation of the law, i.e. containing calls for mass riots, extremist activities, participation in mass (public) events held in violation of the established procedure, inaccurate socially important information distributed under the guise of reliable messages, which creates a threat of harm to life and / or citizens' health, property, the threat of mass violation of public order and (or) public safety or the threat of interfering with the functioning or termination of the functioning of life transport or social infrastructure, credit organisations, energy facilities, industry or communications, information materials of a foreign or international non-governmental organisation whose activity is considered undesirable in the territory of the Russian Federation, the hosting provider is obliged to inform the hosting provider about the information owner of the information resource served by them and notify him of the need to immediately remove unlawfully distributed information.

The hosting provider is obliged to notify the owner of the information resource serviced by him about the need to immediately take measures to eliminate violations of the legislation of the Russian Federation in the field of personal data, or take measures to restrict access to information processed in violation of the legislation of the Russian Federation in the field of personal data.

At the request of Roskomnadzor, the hosting provider is obliged to provide data allowing identification of the owner of software and hardware access to information resources, information and telecommunication networks, access to which is restricted.

Federal Law of 27.07.2006 N 149-ФЗ (as amended on 18.03.2019) "On Information, Information Technologies and on Information Protection".

67. To which extent can a legal person be held liable for actions in connection with cybercrimes?

The provisions of the current law exclude the possibility of criminal liability of legal entities. For damage caused as a result of the activities of legal entities, only the administrative responsibility of this legal entity and the administrative or criminal liability of a specific individual who acted in the interests and on behalf of this legal entity is possible.

Commentary to the Criminal Code of the Russian Federation: in 4 volumes (itemised) / A.V. Brilliantov, A.V. Galakhova, V.A. Davydov et al.; ed. by V.M. Lebedev. M.: Yurayt, 2017. T. 1: General part. 316 p.

▪ Actors

68. What bodies implement the cybercrime legislation?

Brazil has established a number of cybercrime police agencies as defined in law 12735/2012.

Bodies of the Federal Security Service, being authorised bodies, interact with the organizers of information dissemination during operational investigative activities carried out as part of operational investigative activities related to the use of software and hardware (including in the interests of other authorised bodies).

The Ministry of Digital Development, Communications and Mass Communications of the Russian Federation is a federal executive body that is authorised, in coordination with the authorised state bodies carrying out operational investigative activities or ensuring the security of the Russian Federation, to establish requirements for equipment and software and hardware used by the dissemination organizer. Information in the information and telecommunication network "Internet" in the information it uses Discount systems.

In accordance with the Note of the Ministry of Foreign Affairs of Russia of 03.08.2015 N 6839 / 1dsng and the Note of the CIS Executive Committee of 10.08.2015 N 3-1 / 919, the Investigative Committee of the Russian Federation is the competent authority under the Cooperation Agreement of the Member States of the Commonwealth of Independent States in Combating computer crimes.

"Agreement on cooperation of the states – participants of the Commonwealth of Independent States in the fight against crimes in the field of computer information" (concluded in Minsk on 01.06.2001). Decree of the Government of the Russian Federation of July 31, 2014 N 743 (ed. November 20, 2017) "On approval of the Rules for interaction of information dissemination organizers in the Internet information and telecommunications network with authorised state bodies carrying out operational investigative activities or ensuring the security of the Russian Federation". Decree of the Government of the Russian Federation of July 31, 2014 N 741 (ed. September 25, 2018) "On the definition of a federal executive body authorised to establish requirements for equipment and software and hardware used by the information dissemination organizer in the Internet information and telecommunications network information systems operated in it."

69. Is there a special public prosecutor office for cybercrime? If so, how is it organised?

There is no special prosecutorial supervision authority on cybercrime, but given the complexity of investigating computer information crimes and the low qualification of investigators, the need to use special knowledge in investigating, the supervising prosecutor should have special knowledge about the types of forensic examinations conducted in criminal cases of this category make recommendations to the head of the investigative body.

Guidelines for the implementation of prosecutorial supervision over the execution of laws in the investigation of crimes in the field of computer information (approved by the Prosecutor General's Office of Russia).

70. Does the cybercrime legislation create any specific body?

To identify crimes in the field of so-called high technologies (which include crimes in the field of computer information), as well as to identify persons and criminal groups engaged in criminal activities in this area, the "K" Department of the Ministry of Internal Affairs of Russia was created.

The "K" Department of the Ministry of Internal Affairs of Russia, within its competence, carries out the detection, prevention, suppression and disclosure of

1) crimes in the field of computer information:

- unlawful access to legally protected computer information;
- the creation, use and distribution of malicious computer programs;
- violation of the rules of operation of the means of storing, processing or transmitting computer information or information and telecommunication networks;
- fraud in the field of computer information.

2) crimes committed with the use of information and telecommunication networks (including the Internet) against minors' health and public morality:

- production and distribution of materials or items with pornographic images of minors;
- the use of a minor in the manufacture of pornographic materials or objects.

3) crimes related to the illicit trafficking of special technical equipment intended for secretly obtaining information.

4) crimes related to the illegal use of objects of copyright or related rights.

Official website of the Ministry of Internal Affairs of Russia. URL: <https://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii>.

"Guidelines for the implementation of prosecutorial supervision over the execution of laws in the investigation of crimes in the field of computer information" (approved by the Prosecutor General's Office of Russia).

4. Public Order

▪ Definitions

71. How are public order, threats to public order and the protection of public order defined?

Public order is a system, a set of relations between people, rules of conduct, dormitory, established by normative acts, morality, customs, traditions, providing an atmosphere of public peace, personal security in various spheres of life, personal integrity, integrity of property, normal functioning of state and public institutions.

Violation of public order (i.e. hooliganism) – an act of obvious disrespect for society involving the use of weapons or objects used as weapons, as a specific mode of action of the perpetrator, either based on political, ideological, racial, national or religious hatred or hostility towards any social group, either by rail, sea, inland waterway or air transport, as well as by any other public transport.

Federal law of 02.04.2014 N 44-FZ (as amended on 12/31/2017) "On the participation of citizens in the protection of public order"

Commentary to the Criminal Code of the Russian Federation: in 4 tons (itemised) / A.V. Brilliantov, A.V. Galakhov, V.A. Davydov et al.; rep. ed. V.M. Lebedev. M.: Yurayt, 2017. T. 3: The special part. Section IX. 298 p.

72. Is the protection of public order grounded in constitutional norms?

According to the Constitution of the Russian Federation, the protection of the rights and freedoms of a person and a citizen, the ensuring of legality, the rule of law (including the rule of law in public places), public safety are under the joint jurisdiction of the Russian Federation and the subjects of the Russian Federation (Article 72). The implementation of measures to ensure the rule of law, the rights and freedoms of citizens, the protection of property, public order, and the fight against crime are assigned to the authority of the Government of the Russian Federation (clause "e" of Part 1 of Article 114 of the Constitution of the Russian Federation).

At the same time, art. 132 of the Constitution of the Russian Federation determines that local governments independently carry out the protection of public order. In addition, local governments may be vested by law with separate state powers with the transfer of material and financial resources necessary for their implementation. The implementation of the transferred powers is controlled by the state. These provisions are specified in the Law on General Principles of the Organisation of Local Self-Government in the Russian Federation. In particular, it has been established that the organisation of the protection of public order in the territory of the municipal district by the municipal police is among the local issues of the municipal district. This power is also enshrined in relation to issues of local importance of the urban district.

These rules are subject to application in the manner and on the conditions provided for by a special federal law defining the organisation and activities of the municipal police. However, these standards are not implemented. Municipal police are not created.

The Constitution of the Russian Federation (adopted by popular vote on 12.12.1993, as amended by the Laws of the Russian Federation on amendments to the Constitution of the Russian Federation of 12/30/2008 N 6-FKZ, of 12/30/2008 N 7-FKZ, of 02.02.2014 N 2- FKZ, dated 07.21.2014 N 11-FKZ). Federal law of 06.10.2003 N 131-FZ (as amended on 01.05.2019) "On the general principles of the organisation of local self-government in the Russian Federation". Belikov P.P., Vedyaeva E.S., Grebennikova A.A., Zhukovskaya L.P., Zakharova N.A., Zyuzin S.Yu., Mokeev M.M., Naumov S.Yu., Svishcheva V. .A., Shishelova SA Commentary to the Federal Law of October 6, 2003 N 131-FZ "On the General Principles of the Organisation of Local Self-Government in the Russian Federation" (article by article) / ed. L.P. Zhukovskaya // Consultant Plus Legal Reference System. 2016.

▪ Measures

73. What cyber measures address threats to public order?

The law does not address this question. These measures could include introduction computer security incident management system or the "content management system" are possible to ensure the security of the critical information infrastructure of the Russian Federation. Relations in this area are regulated in accordance with the Constitution of the Russian Federation, generally accepted

principles and norms of international law, the Federal Law on the Security of the Critical Information Infrastructure of the Russian Federation, other federal laws and other regulatory legal acts adopted in accordance with them.

Ensuring the security of automated control systems for critical infrastructure facilities of the Russian Federation is impossible without ensuring the security of automated control systems for critical infrastructure facilities of the Russian Federation and critical information infrastructure in general. This situation is due to the widespread introduction of a wide range of information technologies into the production and technological process management systems of the critical infrastructure of the Russian Federation, the globalisation of modern information and telecommunication networks, their transformation into a single global information and telecommunications network with blurred boundaries of national segments, a significant increase in the share of distributed automated Critical Object Management Systems infrastructure of the Russian Federation and the increasing use of information and telecommunication networks and common use networks for their information exchange.

Federal law of 26.07.2017 N 187-FZ "On the security of the critical information infrastructure of the Russian Federation". The main directions of the state policy in the field of security of automated control systems for production and technological processes of critical infrastructure facilities of the Russian Federation (approved by the President of the Russian Federation 03.02.2012 N 803).

▪ Actors

74. What public authorities are responsible for the implementation of surveillance techniques?

On the territory of the Russian Federation, the right to carry out operational investigative activities, including the use of information systems, video and audio recordings, film and photography, as well as other technical and other means that do not damage the life and health of people and do not harm the environment, is granted to the operational units of:

- the internal affairs bodies of the Russian Federation;
- federal security agencies;
- federal executive body in the field of state protection;
- customs authorities of the Russian Federation;
- foreign intelligence services of the Russian Federation;
- Federal Penitentiary Service.

Federal law of 12.08.1995 N 144-FZ (as amended on 07.06.2016) "On operational investigative activities".

75. What are obligations of these public authorities?

When solving the tasks of the operational investigative activities, the bodies authorised to carry it out must:

1. Take, within the limits of their authority, all necessary measures to protect the constitutional rights and freedoms of a person and citizen, property, as well as to ensure the security of society and the state.

2. Perform, within their powers, instructions in writing to the inquiry officer, inquiry body, investigator, head of the investigative body on conducting operational search measures in criminal cases and materials verifying reports of a crime they have taken to production, as well as a court decision in criminal cases.

3. To carry out, on the basis of and in the manner prescribed by international treaties of the Russian Federation, requests from relevant international law enforcement organisations, law enforcement agencies and special services of foreign states.

4. Inform other bodies that carry out operational investigative activity on the territory of the Russian Federation about facts of unlawful activity that are within the competence of these bodies that became known to them, and provide these bodies with the necessary assistance.

5. Follow the rules of conspiracy in the implementation of operational investigative activities.

Federal law of 12.08.1995 N 144-FZ (as amended on 07.06.2016) "On operational investigative activities".

76. Can private actors be involved in the implementation of cyber measures to address threats to public order?

The activities of private entities in participating in the implementation of the cyber measures to address threats to public order are regulated by the National Standard, which is intended for use by organisations of any form of ownership (for example, commercial, state and non-profit organisations). This standard establishes the requirements for the development, implementation, operation, monitoring, analysis, support and improvement of the documented information security management system among the overall business risks of the organisation. In addition, the standard establishes requirements for the implementation of information security management and control measures that can be used by organisations or their units in accordance with the established goals and objectives of information security.

5. Cyberdefence

▪ Scope

77. Is there a national cyberdefence strategy or is cyberdefence mentioned in the national defence strategy?

The information security doctrine of the Russian Federation is a system of official views on ensuring the national security of the Russian Federation in the information sphere. Approved by the Decree of the President of the Russian Federation dated 05.12.2016 N 646.

Presidential Decree of 05.12.2016 N 646 "On the approval of the Doctrine of Information Security of the Russian Federation".

78. What is the legal status of the national defence or cyberdefence strategy?

Traditionally, legal doctrine in Russian jurisprudence is not recognised as a source of law by most scholars. This is explained by the fact that in the Soviet state only acts emanating from the state had legal force, and the fact that until recently due attention was not paid to the nature of legal doctrine. In a democratic Russia, more and more lawyers are in favour of considering the doctrine as an official source of law and insist on it.

In Russia, there are officially approved doctrines, including the Doctrine of Information Security of the Russian Federation. Such doctrines are a system of official views in a certain sphere and, despite their official nature, they can hardly be regarded as a source of law, since they are more likely programmatic documents, they may contain definitions, but they lack legal regulations.

Despite the fact that the law enforcer can use the provisions elaborated by the doctrine, and it can occupy an important place in ensuring uniform regulation of social relations, it seems that legal doctrine can hardly be considered as a form of law.

Zlobin A.V. Forms of law in modern Russia // Lex russica. 2018. N 4. P. 23 – 36.

79. What national laws or other normative acts regulate cyberdefence in the country?

Federal Law of 27.07.2006 N 149-FZ (as amended on 18.03.2019) “On Information, Information Technologies and Information Protection”.

Federal Law of 07.07.2003 N 126-FZ (as amended on 27.12.2018) “On Communications”.

Federal law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) “On personal data”.

Federal Law of 31.05.1996 N 61-FZ (as amended on 03.08.2018) “On Defence”.

Federal Law of 28.12.2010 N 390-ФЗ (as amended on 05.10.2015) “On Security”.

Federal law of 26.07.2017 N 187-FZ “On the security of the critical information infrastructure of the Russian Federation”.

Law of the Russian Federation of 21.07.1993 N 5485-1 (as amended on 29.07.2018) “On State Secrets”.

Federal Constitutional Law of January 30, 2002, No. 1-FKZ (as amended on July 01, 2017) “On Martial Law”.

Federal constitutional law of 30.05.2001 N 3-FKZ (as amended on 03.07.2016) “On the state of emergency”.

Presidential Decree of 05.12.2016 N 646 “On the approval of the Doctrine of Information Security of the Russian Federation”.

Military Doctrine of the Russian Federation (approved by the President of the Russian Federation on 25.12.2014 N Pr-2976)

Presidential Decree of December 31, 2015 N 683 “On the National Security Strategy of the Russian Federation”.

“Consultant Plus” Legal Reference System.

80. Is the country party of any international cooperation agreement in the sphere of cyberdefence ?

The Russian Federation is a party to the cooperation agreement of the member states of the Collective Security Treaty Organisation in the field of information security. It was concluded in Minsk on November 30, 2017.

Agreement between the Governments of the Shanghai Cooperation Organisation member states on cooperation in the field of ensuring international information security (Together with <Lists of basic concepts and types of threats, their sources and signs>). (Concluded in Yekaterinburg 16.06.2009).

"Consultant Plus" Legal Reference System.

81. Does the national cyberdefence strategy provide for retaliation?

The military doctrine of the Russian Federation, which notes the "trend of shifting military dangers and military threats into the information space," refers to the tasks of equipping the Armed Forces, other troops and bodies with armaments, military and special equipment, in particular, the development of information confrontation forces and means.

Military Doctrine of the Russian Federation (approved by the President of the Russian Federation on 25.12.2014 N Pr-2976.

▪ Definitions

82. How are national security and national defence defined?

The national security of the Russian Federation is the state of protection of an individual, society and the state from internal and external threats, which ensures the realisation of constitutional rights and freedoms of citizens of the Russian Federation, decent quality and standard of living, sovereignty, independence, state and territorial integrity, sustainable socio-economic development of the Russian Federation. National security includes the defence of the country and all types of security provided for by the Constitution of the Russian Federation and the legislation of the Russian Federation, primarily state, public, information, environmental, economic, transport, energy security, personal security.

Defence refers to a system of political, economic, military, social, legal, and other measures to prepare for armed defence and the armed defence of the Russian Federation, the integrity and inviolability of its territory.

Presidential Decree of 31.12.2015 N 683 "On the Strategy of the National Security of the Russian Federation". Federal Law of 31.05.1996 N 61-FZ (as amended on 08.03.2018) "On Defence".

83. How are cybersecurity and cyberdefence defined?

Information security of the Russian Federation – the state of protection of individuals, society and the state from internal and external information threats, which ensures the realisation of constitutional rights and freedoms of man and citizen, decent quality and standard of living of

citizens, sovereignty, territorial integrity and sustainable socio-economic development of the Russian Federation , defence and security of the state.

In the legislation of the Russian Federation, cyber defence is defined by the term "protection of information". Information protection is the adoption of legal, organisational and technical measures aimed at ensuring the protection of information from unauthorised access, destruction, modification, blocking, copying, provision, dissemination, as well as from other illegal actions regarding such information, as well as respect for confidentiality of information restricted access and the exercise of the right of access to information.

Presidential Decree of 05.12.2016 N 646 "On the approval of the Doctrine of Information Security of the Russian Federation". Federal Law of 27.07.2006 N 149-ФЗ (as amended on 18.03.2019) "On Information, Information Technologies and on Information Protection".

84. How are threats to national security and cyberthreats defined?

The threat to national security is a set of conditions and factors that create a direct or indirect possibility of damaging national interests, that is, objectively significant needs of the individual, society and the state in ensuring their security and sustainable development.

The threat to the information security of the Russian Federation is a set of actions and factors that create the danger of harming national interests in the information sphere.

Presidential Decree of 31.12.2015 N 683 "On the Strategy of the National Security of the Russian Federation". Presidential Decree of 05.12.2016 N 646 "On the approval of the Doctrine of Information Security of the Russian Federation".

85. How is a cyberattack defined?

Computer attack – targeted effect of software and (or) software and hardware on objects of critical information infrastructure, telecommunication networks used to organize the interaction of such objects in order to violate and (or) terminate their operation and (or) create a security threat processed by such information objects.

Federal law of 26.07.2017 N 187-FZ "On the security of the critical information infrastructure of the Russian Federation".

86. Does the national law provide any other definitions instrumental to the application of cyberdefence legislation?

Computer incident – the fact of violation and (or) termination of the operation of the critical information infrastructure object, the telecommunication network used to organize the interaction of such objects, and (or) the security breach of the information processed by such an object, including the result of a computer attack.

Critical information infrastructure – objects of critical information infrastructure, as well as telecommunication networks used to organize the interaction of such objects.

Objects of critical information infrastructure – information systems, information and telecommunication networks, automated control systems of subjects of critical information infrastructure.

Federal law of 26.07.2017 N 187-FZ "On the security of the critical information infrastructure of the Russian Federation".

▪ National Framework

87. Is cyberdefence grounded on the constitutional provisions and/or international law?

The legal basis of the Information Security Doctrine is the Constitution of the Russian Federation, generally accepted principles and norms of international law, international treaties of the Russian Federation, federal constitutional laws, federal laws, and regulatory acts of the President of the Russian Federation and the Government of the Russian Federation.

Presidential Decree of 05.12.2016 N 646 "On the approval of the Doctrine of Information Security of the Russian **Federation".**

88. Which specific national defence measures are related to cybersecurity?

The main measures of the Russian Federation in the field of cyber security, defined by the Military Doctrine of the Russian Federation, include:

- assessment and forecasting of the development of the military-political situation at the global and regional level, as well as the state of interstate relations in the military-political sphere using modern technical means and information technologies;
- creating conditions that reduce the risk of using information and communication technologies for military-political purposes to carry out actions contrary to international law, against sovereignty, political independence, territorial integrity of states and posing a threat to international peace, security, global and regional stability;
- provision of informational interaction between federal executive authorities, executive authorities of the constituent entities of the Russian Federation, other state bodies in solving tasks in the field of defence and security;
- improving the information security system of the Armed Forces, other troops and agencies;
- development of forces and means of information confrontation;
- qualitative improvement of information exchange tools based on the use of modern technologies and international standards, as well as a single information space of the Armed Forces, other troops and agencies as part of the information space of the Russian Federation;
- creation of basic information management systems and their integration with weapons control systems and complexes of automation equipment for management bodies of strategic, operational-strategic, operational, operational-tactical and tactical scale;

- development of a dialogue with interested states on national approaches to countering military dangers and military threats arising from the large-scale use of information and communication technologies for military-political purposes.

Military Doctrine of the Russian Federation (approved by the President of the Russian Federation on 12/25/2014 N Pr-2976).

89. Is there a national defence doctrine and does the law or strategy refer to it?

Approval of the Military Doctrine of the Russian Federation in accordance with Clause "Z" Art. 83 of the Constitution of the Russian Federation and sub. 2 p. 2 Art. 4 of the Federal Law "On Defence" is included in the powers of the President of the Russian Federation. The President of the Russian Federation approved the military doctrine of the Russian Federation on December 25, 2014. The military doctrine of the Russian Federation is one of the main strategic planning documents in the Russian Federation and is a system of formally adopted views in the state on preparations for armed defence and armed defence of the Russian Federation.

The Constitution of the Russian Federation (adopted by popular vote on 12.12.1993, as amended by the laws on amendments to the Constitution of the Russian Federation of 30.12.2008 N 6-FKZ, of 30.12.2008 N 7-FKZ, from 05.02.2014 N 2-FKZ, dated 07.21.2014 N 11-FKZ). Federal Law of 31.05.1996 N 61-FZ (as amended on 03.08.2018) "On Defence". Military Doctrine of the Russian Federation (approved by the President of the Russian Federation on 12/25/2014 N Pr-2976).

90. What measures are mentioned in the national law and strategy in order to implement cyberdefence ?

The main areas of information security in the field of national defence are:

a) strategic deterrence and prevention of military conflicts that may arise as a result of the use of information technology;

b) improving the information security system of the Armed Forces of the Russian Federation, other troops, military formations and bodies, including the forces and means of information confrontation;

c) forecasting, detection and assessment of information threats, including threats to the Armed Forces of the Russian Federation in the information sphere;

d) assistance in ensuring the protection of the interests of the allies of the Russian Federation in the information sphere;

e) neutralisation of information and psychological impact, including aimed at undermining the historical foundations and patriotic traditions associated with the defence of the Fatherland.

Presidential Decree of 05.12.2016 N 646 "On the approval of the Doctrine of Information Security of the Russian Federation".

91. How can Internet users' online activities be limited for the reasons of protection of national security and cyberdefence ?

Federal laws in order to protect the foundations of the constitutional order, morality, health, rights and legitimate interests of others, ensure the defence of the country and the security of the state establish restrictions on access to information.

By virtue of the provisions of part 3 of article 55 of the Constitution of the Russian Federation, restrictions on the rights and freedoms of a person and a citizen (including freedom of speech), established not by federal law, but by other regulatory legal acts, cannot be recognised as legal.

During the period of martial law and the state of emergency, the rights and freedoms of citizens of the Russian Federation, foreign citizens, and stateless persons may be limited to the extent necessary to ensure the defence of the country and the security of the state.

According to the Federal Constitutional Law "On the State of Emergency", freedom of the press and other mass media is allowed by introducing preliminary censorship specifying the conditions and procedure for its implementation, as well as temporary seizure or arrest of printed materials, radio transmitters, sound-amplifying technical means, copying equipment, the establishment of special accreditation procedures for journalists;

According to the Federal Constitutional Law "On Martial Law", military censorship of mailings and messages transmitted via telecommunication systems, as well as control over telephone conversations, and the creation of censorship bodies directly involved in these issues are allowed.

Federal Law of 27.07.2006 N 149-FZ (as amended on 18.03.2019) "On Information, Information Technologies and Information Protection". Federal Constitutional Law of January 30, 2002, No. 1-FKZ (as amended on July 01, 2017) "On Martial Law". Federal constitutional law of 30.05.2001 N 3-FKZ (as amended on 03.07.2016) "On the state of emergency". Resolution of the Plenum of the Supreme Court of the Russian Federation dated 15.06.2010 N 16 (as amended on 09.02.2012) "On the practice of the application by the courts of the Law of the Russian Federation "On the Mass Media".

92. Does the national law or strategy foresee any special regime to be implemented in case of emergency in the context of cyberdefence ?

In the event of threats to the stability, security and integrity of the information and telecommunications network Internet and public communication network in the Russian Federation, the public communication network of the general use authority may be centrally controlled by the federal executive body responsible for monitoring and supervising the media, mass communications, information technology and communications (Roskomnadzor).

The Roskomnadzor provides, at no cost, to telecom operators, technical means of countering threats, and establishes technical conditions for installing technical means to counter threats, as well as requirements for communication networks when using technical means to counter threats.

Centralised management of a public telecommunications network is carried out by managing technical means of countering threats and (or) by transmitting binding instructions to telecom operators, owners or other owners of technological communication networks, owners or other owners of traffic exchange points, owners or other owners of communication lines crossing The

state border of the Russian Federation, other persons, if such persons have an autonomous system number.

The Government of the Russian Federation approves the procedure for centralised management of a public telecommunications network.

In the case of centralised management of a public telecommunications network, persons participating in centralised management are required to comply with the telecommunication message routing rules established by the federal executive body responsible for monitoring and supervising the media, mass communications, information technologies and communications. Telecommunication message routing rules apply to telecommunication messages if the recipient or sender of such messages is a user of communication services in the territory of the Russian Federation.

Roskomnadzor is obliged to inform the persons participating in the centralised management in the event of threats to the stability, security and integrity of the information and telecommunications network Internet and public communication networks in the territory of the Russian Federation.

The means of communication, with the use of which the persons participating in the centralised management carry out the instructions within the framework of the centralised management of the public communication network, shall be located on the territory of the Russian Federation. The Government of the Russian Federation approves the procedure for monitoring the fulfilment by the persons participating in the centralised management of the duties of locating the means of communication in the territory of the Russian Federation, with which the instructions are fulfilled within the framework of centralised management of the public telecommunications network.

Federal Law of 01.05.2019 N 90-ФЗ "On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection".

93. Is there any specific framework regulating threats to critical infrastructure?

The state system for detecting, preventing and eliminating the effects of computer attacks on information resources of the Russian Federation is a single geographically distributed complex, including forces and means designed to detect, prevent and eliminate the consequences of computer attacks and respond to computer incidents.

Federal law of 26.07.2017 N 187-FZ "On the security of the critical information infrastructure of the Russian Federation".

▪ Actors

94. What actors are explicitly mentioned as playing a role regarding cyberdefence in the law or national cyber defence strategy or defence strategy?

Council of Federation of the Federal Assembly of the Russian Federation, State Duma of the Federal Assembly of the Russian Federation, Government of the Russian Federation, Security Council of the Russian Federation, federal executive bodies, Central Bank of the Russian Federation, Military-Industrial Commission of the Russian Federation, interdepartmental bodies established by the

President of the Russian Federation and the Government of the Russian Federation, executive authorities of the constituent entities of the Russian Federation, local authorities legal authorities that, in accordance with the legislation of the Russian Federation, take part in solving problems of ensuring information security.

Presidential Decree of 05.12.2016 N 646 "On the approval of the Doctrine of Information Security of the Russian Federation.

95. Is there a specific cyber defence body?

The National Computer Incident Coordination Centre is an integral part of the forces designed to detect, prevent, and repair the effects of computer attacks and respond to computer incidents.

The task of the Centre is to ensure the coordination of the activities of the subjects of the critical information infrastructure of the Russian Federation on the issues of detecting, preventing and eliminating the consequences of computer attacks and responding to computer incidents.

Order of the Federal Security Service of Russia of 24.07.2018 N 366 "On the National Coordination Centre for Computer Incidents" (along with the "Regulations on the National Coordination Centre for Computer Incidents").

96. What are the tasks of aforementioned actors?

Ensuring the protection of the rights and legitimate interests of citizens and organisations in the information sphere; assessing the state of information security, forecasting and detecting information threats, identifying priority areas for their prevention and eliminating the consequences of their manifestation; planning, implementation and evaluation of the effectiveness of a set of information security measures; organisation of activities and coordination of information security forces interaction, improvement of their legal, organisational, operational-investigative, intelligence, counterintelligence, scientific, technical, informational, analytical, personnel and economic support; development and implementation of measures of state support for organisations engaged in the development, production and operation of information security tools, provision of information security services, as well as organisations carrying out educational activities in this field.

Strengthening the management vertical and centralisation of information security forces at the federal, interregional, regional, municipal levels, as well as at the level of information objects, information system operators and communication networks;

improvement of the forms and methods of interaction between information security forces in order to increase their readiness to counter information threats, including through regular training (exercises); improvement of information-analytical and scientific-technical aspects of the functioning of the information security system; increasing the efficiency of interaction between state bodies, local self-government bodies, organisations and citizens in solving problems of ensuring information security.

Presidential Decree of 05.12.2016 N 646 "On the approval of the Doctrine of Information Security of the Russian Federation".

4. Cybersecurity and Data Protection Regulation in India: An Uneven Patchwork

Anja Kovacs

Cybersecurity has been an important policy concern for the Indian government since at least the early 1990s. Until today, however, the landscape of its cybersecurity policies remains an uneven patchwork. In particular, as this essay will illustrate, where the concerns of technology users are at odds with the interests of law enforcement and intelligence agencies, the former tend to lose out. Thus, while India was one of the first countries, in 2000, to pass a law dealing with cybercrime and electronic commerce and has, in 2019, also approved law to strengthen consumer protection in the digital age, at the time of writing the country still does not have a horizontal personal data protection law. At the same time, law enforcement and intelligence agencies can legally access and retain user data under a wide range of loosely worded provisions[196].

The historical antecedents of this patchwork can to an important extent be traced to the early 1990s, a period of great political and economic change in India[197]. Following an economic crisis in 1991, a more liberal economic regime replaced the earlier model that was oriented towards more socialist forms of planning. While IT and IT-enabled services (ITeS) companies in India had benefited from sector-specific liberalisation measures since the late 1970s[198], this broader opening up of the Indian economy led to a boom in the sector that enabled India to redefine itself, by the early 2000s, as an emerging information technology superpower[199].

The policy changes of the early 1990s also paved the way for a gradual liberalisation of the telecom sector that would eventually result in the country having one of the highest Internet user bases in the world. As of March 2019, India was believed to have 451 million monthly active Internet users, second only to China's user base. Sixty five percent of these users are believed to access the Internet daily[200]. While this means the Internet penetration rate is still only at 36%, large numbers of these users have been added over the previous decade, under the impetus of both public sector, such as the digitisation of government services under the Digital India flag[201], and private sector initiatives, such as the

196 See sections 4.1, on data protection, and 4.4, on public order, of this chapter in particular for further details.

197 See Datta (2016).

198 See Gopalakrishnan (26 April 2016).

199 For critical accounts of these evolutions and the social, political and economic changes they brought with them, see Corbridge and Harriss (2003); Frankel (2005); and Upadhya (2011).

200 See IAMAI (2019).

201 See <https://www.digitalindia.gov.in/for further details>.

entrance of Reliance Jio into the telecom market, which has driven down 4G prices to unprecedented levels[202].

As the decade progressed, the wealth of data that this user base creates is playing an increasingly important role in India's vision for its growth and development trajectory, with data increasingly accorded pride of place as a "national asset" and efforts underway to ensure that control of that data comes at least to some extent in Indian hands – whether public or private – rather than being predominantly in the hands of foreign entities[203].

In 1990, around a year before the economic crisis brought India on the verge of an economic meltdown, however, another important event took place: a popular uprising against India's rule took place in the Muslim-majority Kashmir Valley, in the Indian state of Jammu and Kashmir, which led Pakistan to subsequently provide the militants in the state with diplomatic as well as material support. As the spread of Information and Communication Technologies (ICTs) in Indian society started to gather pace, so did, in other words, the country's challenges around how ICTs may impact national security in general, and be utilised for terrorist purposes in particular[204]. Thus, when India and the US established a Joint Working Group on Counter Terrorism in 2000, this was quickly followed by a subgroup on cybersecurity only a year later[205]. Challenges related to the use of communication technologies by terrorists became apparent even to non-specialists, however, when their use was revealed in the context of bomb blasts by an until then fairly unknown entity named Indian Mujahideen, which hit several major Indian cities in 2006, and by the Pakistan based terrorist group Laishkar-e-Taiba in terrorist attacks on Mumbai in 2008[206]. The latter left at least 166 people dead. Not surprisingly, then, as Saikat Datta has shown, concerns about the use of cyberspace by terrorists has been a driving force of India's cybersecurity policy throughout this period[207].

In order to understand the shape that India's cybersecurity policy has taken over the past twenty-five years, the context of these twin events is then crucial, as their impact on India's cybersecurity policies has been profound. In a nutshell, while certain protections for citizens are recognised as crucial to ensure trust in ICTs and the continued economic growth and development of the country in the digital age, in the final analysis these are generally made subservient to the interests of the state. At least until

---

202 See Jasrotia et al. (2019).

203 For examples of both, see the draft National e-Commerce Policy, 2019, available here: <https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf>.

204 See Datta (2016).

205 Ibid.

206 On the use of ICTs by the Indian Mujahideen, see Datta (2016). For the Laishkar-e-Taiba, see Glanz et al; (21 December 2014). And such challenges continue today, see Sagar (9 November 2019).

207 See Datta (2016).

the Supreme Court forces the government to pay attention, protections that do not immediately seem essential to ensure economic growth and development are largely ignored.

Somewhat surprisingly in this context, perhaps, India's military cyberdefence capabilities do not as yet match the centrality of cybersecurity in India's policy discourses, however: efforts at coordination and integration of the different services of the armed forces, while recognised as central to effectiveness in the cyberdomain, remain fledgling at best. Thus, as Abhijnan Rej and Shashank Joshi have noted, cybersecurity policy, including cyberdefence, for now remains focused predominantly on the civilian aspects of such threats[208].

4.1. Data Protection

In a landmark judgement in 2017, India's Supreme Court confirmed that the Indian people enjoy a fundamental right to privacy under the Indian constitution. With the Puttaswamy judgement[209], the learned judges went against the Government's argument in court that privacy in India is not a fundamental right. Moreover, informational privacy was explicitly acknowledged as an integral aspect of privacy in the judgement. Yet, as of November 2019, India still does not yet have a personal data protection act.

A draft has been under discussion. In late July 2018, almost a year after it was constituted by the Government of India to "identify key data protection issues in India and recommend methods of addressing them[210]", the Committee of Experts under the chairmanship of Justice BN Krishna released a draft Personal Data Protection Bill[211], as well as an accompanying report, titled "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians[212][213]".

The Srikrishna Committee's outputs are not the first attempt at improving protections for personal data in India. In 2006, Member of Parliament Vijay J. Darda introduced a first draft Personal Data Protection Bill in Parliament[214]; between 2009 and 2017, at least another five attempts to introduce related legislation were made in the form of private members' bills. None of these initiatives were passed[215]. Moreover, in 2012, a Group of Experts on Privacy under the chairmanship of Justice

[208] See Rej and Joshi (2018).

[209] *Justice K.S. Puttaswamy (Retd.) and Anr. Vs Union of India and Ors.*, writ petition (civil) no. 494 of 2012.

[210] See Ministry of Electronics and Information Technology (2017), p. 1.

[211] The draft Bill is available here: <https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf>.

[212] See Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018).

[213] A Personal Data Protection Bill was finally tabled in the Indian Parliament in December 2019. While the exact wording of this bill is different from the 2018 draft, and a few provisions have undergone fairly substantial changes, the overall trends identified in this chapter continue to hold.

[214] See Gupta (18 September 2007).

[215] See Dutta (24 August 2017).

AP Shah, constituted a year earlier by the Planning Commission of the Government of India[216], submitted a report of its own[217]. Surveying both international and national initiatives, the report outlined a number of privacy principles that any Indian data protection legislation should adhere to, as well as analysing existing legislation in India from this perspective. At the time, a draft Privacy Bill prepared by the Department of Personnel and Training, Government of India, was in circulation as well, but it was, however, never tabled in Parliament[218]. A redraft of this bill by the Committee of Secretaries (CoS), the heads of seven of India's most powerful Ministries and Departments, surfaced as the draft Right to Privacy Bill, 2014, but never found consensus within the government either[219].

With such a long history behind it, the current bill is a welcome initiative, and yet, despite these years of discussion, its shortcomings remain considerable[220].

First, so called next-generation rights, such as the right to explanation of automated decision-making or the right to object to decisions solely based on automated processing if such processing effects the data subject's rights, are completely absent from the draft bill[221].

Second, while consent is included as a ground for the processing of personal data, its effectiveness is undermined by provisions that allow data fiduciaries to exercise their own judgement as to what is "fair and reasonable" in relation to such processing, considerably expanding the scope for the processing of personal data without having to ask the data subject for their consent in practice[222]. In addition, employers are granted considerable powers to process personal data of their employees without having to obtain their consent first, including as they deem necessary for any activity relating to the assessment of the performance of the employee[223]. Moreover, for functions of the state,

---

[216] See Planning Commission (2011).

[217] See Group of Experts on Privacy Chaired by Justice A.P. Shah (2012).

[218] See Gandhi (27 March 2018). A first version of this draft Bill was leaked in April 2011, and can be found here: <https://bourgeoisinspirations.files.wordpress.com/2010/03/draft_right-to-privacy.pdf>. A later version of the draft Bill was discussed within the Government, as evidence by a leaked office memorandum from the Ministry of Home Affairs dated September 2011 (see Ministry of Home Affairs (2011)). This document also contains the version of the bill that was discussed by the Ministry at the time.

[219] See Greenleaf (1 June 2014).

[220] For detailed analyses, see Internet Democracy Project (2018) and Concerned Citizens (2018).

[221] See Ranganathan (9 August 2018).

[222] For example, section 5 of the draft Personal Data Protection Bill, 2018, on purpose limitation, while noting that data should be collected only for purposes that are clear, specific and lawful, does not require such purpose to be specified if it constitutes "any other incidental purpose [in addition to those purposes specified] that the data principal would *reasonably* expect the personal data to be used for" [emphasis the author's]. This completely ignores the fact that at present, there is little agreement among different stakeholders in India on what constitutes such a "reasonable" expectation. Section 4 of the draft Personal Data Protection Bill, 2018, on fair and reasonable processing, is plagued by similar problems.

[223] See section 16 of the draft Personal Data Protection Bill, 2018.

including the provision of benefits and the granting of licenses, permits and the like, consent is done away with altogether[224].

This is particularly important, as, finally, processing of personal data in the interests of the security of the state and for the prevention, detection, investigation and prosecution of law are exempted from multiple provisions of the Act, including those on consent[225]. The draft bill does require such surveillance to be authorised by law[226], but as we shall see in a later section, such laws are many in India. The draft bill also requires such surveillance to be necessary and proportionate to the interests being achieved[227]; however, those standards have not yet been laid down in any law. Until this has happened, or a court has come to a determination in this regard, the state thus has broad powers to collect data either in the course of providing benefits and services or for purposes of law and order. Moreover, restrictions on the sharing of data between different arms of the government, or on the use of data collected by the government for one purpose, such as service to the public, in the service of another purpose, such as to protect the interests of the state, are absent from the law as well. Finally, the draft Data Protection Bill additionally requires the storage of at least one copy of all data on a server or in a data centre located in India, thus further facilitating broad, and arguably unprecedented access by India's police forces and intelligence agencies to the data of the country's residents[228].

The draft bill's provisions on data localisation, in particular, have met with considerable protest, and there are indications that the government might be rethinking its stance on this issue[229]. Other changes might be included in the bill as well: in January 2019, intelligence agencies had indicated that they wanted stronger protections for their activities under the bill[230].

India's draft Personal Data Protection Bill, 2018, thus, emerges not so much as a tool to protect users' rights but as a framework to regulate the use of personal data by private and public actors, and to thus shield them from liability. Seeing the central role of new technology in India's understanding of terrorist threats and of data in its visions for growth and development, this should, however, not come as a surprise. While concerns such as the need for data protection may be acknowledged in policy

---

224 See sections 13 and 19 of the draft Personal Data Protection Bill, 2018.

225 As specified in sections 42(2) and 43(2) of the draft Personal Data Protection Bill, 2018, data processing for these purposes is exempted from all provisions in chapter II, of the Bill, on data protection obligations, except section 4, on fair and reasonable processing; chapter III of the Bill, on grounds for processing of personal data; chapter IV, on grounds for processing of sensitive personal data; chapter V, on personal and sensitive personal data of children; chapter VI, on data principal rights; chapter VII, on transparency and accountability measures, except section 31, on security safeguards; and chapter VIII, on transfer of personal data outside India.

226 See section 42(1) of the draft Personal Data Protection Bill, 2018.

227 Ibid.

228 For details on access to data by India's law enforcement and intelligence agencies provided by other Indian laws, see section 4.4, on public order, of this chapter.

229 See Mankotia (24 July 2019).

230 See Samanta (7 January 2019).

articulations by India's government, financial and economic considerations[231] as well as concerns about national security[232] ultimately prevail time and again.

4.2. Consumer Protection

While data protection might remain a fraught topic in India, the need to update consumer protection legislation to bring it in line with the requirements of the digital age has been less controversial. First introduced in a different version Parliament in 2015, the Consumer Protection Act 2019 was passed by the Indian Parliament in August 2019, and will, after its notification, repeal the earlier Consumer Protection Act 1986. Concerns that have been brought on by digitisation are widely seen as one of the driving forces for the changes made to the Act.

For example, the definition of "consumer" in the new Act has been expanded to include e-commerce transactions[233]. The definition of "unfair trade practices" has been expanded to include misleading electronic advertising[234]. The term "product seller" has been defined in such a way that e-commerce platforms are included as well, making such platforms, too, potentially liable where a product is found defective or a service deficient[235]. And as the definition of "goods" has been amended to include "food" as defined under the Food Safety and Standards Act, 2006, India's many food delivery platforms are arguably brought under the Act as well[236].

Moreover, changing realities have been taken into account in other ways also: whereas under the 1986 Act, complaints had to be filed where the opposite party resided or conducted its business, or where the cause of action arose, under the new Act, complaints can be made where the complainant resides or works[237]. Further, the new Act also allows for the e-filing of complaints.

Further changes have been proposed in the draft Consumer Protection (e-Commerce) Rules, 2019, that were opened to public consultation in November 2019[238]. These Rules cover a wide range of issues, from the different types of information that e-commerce entities need to display, over the precautions they need to take to ensure the protection of consumers' rights, to the grievance redress procedures they need to put in place.

---

231 See Kovacs and Ranganathan (2019).

232 See Datta (2016).

233 See Galiya (20 August 2019).

234 See Varma (2 September 2019).

235 See Galiya (20 August 2019).

236 See Varma (2 September 2019).

237 Ibid.

238 The draft e-Commerce Rules, 2019, are available here: <http://consumeraffairs.nic.in/DraftRule/Draft%20e-commerce%20Rules.docx>.

Moreover, the draft National e-Commerce Policy, 2019, which was released in February 2019, promises a move towards a system of electronic grievance redressal, including making compensation available to aggrieved consumers electronically, through e-consumer courts, as well as the development of a legal framework to regulate unsolicited commercial messages and calls.

But some provisions – both proposed and approved – are controversial. This includes a provision in the draft e-Commerce Rules that requires that every e-commerce entity carrying out e-commerce business in India be a registered legal entity under the laws of India and that its promotor or key management personnel should not have been found guilty of any criminal offence in the past five years[239]. Further requirements under this provision are that the entity adheres to the rules for intermediaries that have been issued under the IT (Amendment) Act, 2008, and that all payments facilitated by the e-commerce entity are conform with the guidelines of the Reserve Bank of India. Some of the latter include data localisation requirements for payment data[240].

In addition, the Act for the first time sets up a consumer protection body that has among its tasks not only awareness raising, research and advice, but that can also investigate complaints. The Act also provides for Consumer Protection Commissions at the district, state and national levels that can investigate and adjudicate on complaints as well. While the Commissions are, thus, quasi-judicial bodies, the Act does not, however, explicitly require the Commissions to have one or more judicial members. Concerns have also been raised about the independence of the Commissions, as the Act leaves the composition of the Commissions and the appointment and removal of members as well as the prescription of the conditions of service for members to the Central Government[241]. While Consumer Protection Councils filled with government officials are supposed to provide advice as per the Act, the Act does not specify who they will provide advice to.

---

239 See section 3 of the draft e-Commerce Rules, 2019.

240 See Reserve Bank of India (2018).

241 See e.g. Suhag and Sinha (2018) and Jain (29 August 2019). Such concerns seem to be slightly alleviated by the draft Consumer Protection (Qualification for Appointment, Method of Recruitment, Procedure of Appointment, Term of Office, Resignation and Removal of the President and Members of the State Commission and District Commission) Rules, 2019, released in November 2019. The draft Rules require the President of the State and District Commissions to be or have been a Judge of the High Court or a District Judge, respectively (see sections 3(1) and 4(1) of the draft Rules). Moreover, the draft Rules propose that the members of the State Commission and the President and members of the District Commission will be appointed by the State Government on the recommendation of a selection committee headed by a Judge of the High Court, to be nominated by the Chief Justice of the High Court. The other members of the committee will be the Secretary of the Ministry of Law of the State Government and the Secretary in charge of consumer affairs at the State Government (section 7(2) of the draft Rules). However, the selection committee merely has the power to recommend a panel of names of candidates for appointment as member in order of merit for the consideration of the State Government. The draft Rules do not explicitly require the State Government to accept the recommendations or to adhere to the order suggested by the selection committee in appointing members (sections 7(12) and 7(13) of the draft Rules). Moreover, the President of the State Commission, though a High Court judge, will be appointed merely after consultation with the Chief Justice of the High Court of the State (section 7(1) of the draft Rules). Finally, sections 12 and 13 of the draft Rules provide the Central Government with the power to relax any of the provisions of the Rules where it is of the opinion that it is necessary or expedient to do so and confirms that if any questions arise relating to the interpretation of the Rules, the decision of the Central Government shall be final. Where the National Commission is concerned, no procedures for appointment of the President or members have so far been laid down in these or any other draft rules. The draft Rules are available here: <http://consumeraffairs.nic.in/DraftRule/Draft%20State%20Commission%20and%20District%20Commission%20%20Rules.docx>.

4.3. Cybercrime

While cybercrime is addressed in a number of sectoral acts and even in the Criminal Procedure Code, such as for example to address the creation and publication of child sexual abuse images or to criminalise cyberstalking, the main Act governing cybercrime remains the Information Technology Act (IT Act).

When India passed the IT Act, a law dealing specifically with cybercrime and electronic commerce, in 2000, it was only the twelfth country in the world to do so[242]. The passing of the IT Act at that early point in time can be seen as the earliest acknowledgement of the economic value of data in India. By then, information technology enabled services had emerged not only as a crucial growth sector of the Indian economy, they had also become a symbol for India's new-found status as an emerging, modern global power[243]. Building on a UN model law put forward in the late 1990s, the passing of the IT Act aimed, among other things, to further promote the IT industry and e-commerce by providing legal sanctity to all electronic records and other activities carried out through electronic means[244] as well as to foster good security practices and prevent cybercrime.

When the Act was subsequently amended without much discussion in 2008, shortly after bomb attacks in Mumbai by Pakistan-based Islamist terror group Lashkar-e-Tayyiba claimed the lives of more than 160 people, a number of new offences were introduced that extended the scope of the Act considerably beyond these early, mostly economic concerns into more extensive content regulation[245]. This included provisions to provide punishment for the sending of offensive messages (section 66A); to criminalise the transmission and publication of sexually explicit material (section 67A) in addition to an existing provision already criminalising obscene content; and to criminalise a broad range of actions involved in the creation, publication and distribution of child sexual abuse images. It also included a section criminalising the capturing, publishing and transmitting of images of someone's private parts without their consent (section 66E), making India effectively one of the first countries to have a legal provision to combat the non-consensual sharing of sexual images. Important changes were also made at the time to strengthen the safe harbour provisions in section 79.

These amendments have not been without controversy. For example, if section 67A of the IT Act criminalises sexually explicit material, such material is not deemed illegal per se under any other Indian law[246]. Although international law requires the right to freedom of expression to be protected

[242] See Duggal (2005).

[243] See Corbridge and Harriss (2003); Frankel (2005); and Upadhya (2011).

[244] As explained in the preamble to the Act, which also makes references to the UN model law.

[245] See Tewari and Nayak (23 December 2008). Industry had been asking for a number of amendments for some years as well by then, however. See Napinnai (2010).

[246] See Kovacs and Ranganathan (2017).

irrespective of the medium, the medium at present thus determines whether the sharing of sexually explicit is an offence by definition in India or not[247].

Moreover, in a loss to women's rights, the existence of section 67A also undermines the recognition of the importance of consent that is highlighted in section 66E of the IT Act. Research has shown that the police tend to use sections 67 and 67A, criminalising obscenity and sexually explicit material, far more liberally than section 66E, criminalising the production and transmission of images of someone's private parts without the person's consent[248]. By doing so, police contribute to perpetuating a morality discourse around women's naked bodies, rather than a discourse of consent[249].

Controversy also emerged around sections 66A and 79, both of which ended up before the Supreme Court. Section 66A criminalised, among other things, messages that were grossly offensive or that the sender knew to be false but sends nevertheless in order to cause annoyance, inconvenience or insult. None of these terms have been defined under any Indian law. Reports of misuse of the section, including to silence political speech, were widespread before the Supreme Court, in *Shreya Singla v Union of India*[250], deemed the section overly broad and struck it down as unconstitutional in 2015.

Shreya Singhal v Union of India also saw a challenge to section 79, and in particular to the Rules that were framed under the section. This included a requirement for intermediaries to take down content following actual knowledge based on criteria that were as vague as those in section 66A, as well as a lack of clarity around what constitutes "actual knowledge" by an intermediary. The Court provided clarity on the interpretation of the Rules, narrowing down their reading and that of the section, but refused to strike down either.

Amendments to the Intermediary Rules, reportedly inspired by social media misinformation[251], are currently under discussion. These include, among other things, a requirement for intermediaries with more than 5 million users to incorporate in India. Other amendments demand all intermediaries put into place technology-enabled automated tools or other mechanisms, with relevant controls, to proactively identity and remove or disable public access to unlawful information or content, as well as enabling traceability of any unlawful content on their platforms[252].

---

[247] Article 19(2) of the International Covenant on Civil and Political Rights states: "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

[248] See Datta (2017).

[249] See Kovacs and Ranganathan (2017).

[250] AIR 2015 SC 1523.

[251] See Ministry of Electronics and Information Technology (2018).

[252] The draft Information Technology Intermediaries Guidelines (Amendment) Rules, 2018, can be found here: <https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf>. For analyses, see Krishnan & Sinha (2019); Pal (6 February 2019); and Sarkar (12 August 2019).

Among the bodies established by the IT Act to ensure its implementation is the Cyber Appellate Tribunal. The Controller of the Certifying Authorities for electronic signature certificates and adjudicating officers to be appointed by the government can investigate contraventions of the Act or specific sections of it. As per section 57(1) of the IT (Amendment) Act 2008, appeals to orders made by the Controller or an adjudicating officer can be made to the Cyber Appellate Tribunal. From 2011 until 2017, however, the Tribunal was barely functioning: as it remained without a Chairperson throughout this period, no orders were passed and no cases were heard[253]. In 2017, the Finance Act was amended to merge the Cyber Appellate Tribunal with the Telecom Disputes Settlement and Appellate Tribunal, supposedly in a cost minimising exercise. By mid-2018, it appeared that cases had started moving again[254].

The Indian Computer Emergency Response Team (CERT-IN), in contrast, designated the national nodal agency for incident response under section 70B of the IT (Amendment) Act, 2008, has functioned more effectively since its establishment in 2004, and has over time emerged as one of the central agencies in India's cybersecurity architecture.

4.4. Public Order

Public order is one important ground to justify surveillance efforts in the Indian context. While not defined in law as such, there has been considerable jurisprudence on the concept and its interpretation in the Supreme Court of India, that has narrowed its scope over the years. In particular, the courts have clarified that public order is a narrower concept than law and order, and restrictions placed on this ground therefore come with a higher burden of proof. This includes a test of proximity: any threat to public order should resemble "a spark in a powder keg[255]".

Despite these qualifications, the influence of the concern for public order in Indian legislation and jurisprudence runs deep. Thus, for example, in *State of U.P. v. Lalai Singh Yadav*[256], the Supreme Court ruled that "ordered security" is a constitutional value, and that where free speech and public order seem to clash, the latter is to prevail. Although there have been dissenting voices, this remains the dominant strand in free speech jurisprudence in India until today[257].

It is in in this light that the high number of "Internet shutdowns" in India, too, must be understood: according to a tracker of Internet shutdowns in India, their numbers rose from 3 in 2012 to 106 in 2019, with a peak of 134 in 2018[258]. In 2017, the Temporary Suspension of Telecom Services

[253] See Comptroller and Auditor General of India (2016), in particular chapter 4, and Srivas (12 December 2016).

[254] See Na (9 July 2018).

[255] See Bhatia (17 February 2016).

[256] AIR 1977 SC 202.

[257] See Law Commission of India (2017) and Narrain (2016).

[258] See <https://internetshutdowns.in/>, maintained by the Delhi-based Software Freedom Law Centre (SFLC). SFLC considers an Internet shutdown any state imposed blanket ban on access to Internet services, either mobile or fixed line or both. Instances where only access to some content or services is affected, while other content or services remain accessible, are not taken into account. In

(Public Emergency and Public Safety) Rules were notified under section 7 of the Indian Telegraph Act, which provides the Central Government with the power to make rules for the conduct of telegraphs. However, despite this detailed procedure now being available, section 144 of the Criminal Procedure Code continues to be used at times[259]. This section grants a District Magistrate, a Sub- divisional Magistrate or any other Executive Magistrate specially empowered by the State Government in this behalf, the power to issue orders in urgent cases of nuisance or apprehended danger. Although less common, section 5(2) of the Indian Telegraph Act, 1885 has also been used in the past to order Internet shutdowns. This section allows the government to stop the transmission, to intercept, to detain and to order the disclosure of any message or class of messages or relating to any particular subject on the occurrence of a public emergency or in the interest of public safety, if it is necessary or expedient to do so in the interests of, among other things, public order[260].

In 2015, after the government of Gujarat, following a series of public protests, had blocked mobile Internet access for a week using section 144, a public interest litigation in the Gujarat High Court challenged the authority of the state to do so, arguing that instead section 69A of the IT Act should have been used[261]. The High Court ruled that the invocation of section 144 was permissible: the public disturbances at the time were sufficient justification for the section's invocation, the Court argued, if the government deemed the section to be the most appropriate tool to maintain public order and prevent further rioting.

Surveillance provisions in India, too, are often justified, directly or indirectly, on the grounds of public order. The broad-sweep surveillance provisions that were included in the IT Act when it was amended in 2008 need to be understood in this light. Section 69 allows the government to intercept, monitor and decrypt any information through any computer resource, while section 69A allows the government to block for public access any information through any computer resource. In both cases, public order is among the grounds on which action can be taken.

However, it is important to understand that these and other provisions include a large number of other grounds on which the monitoring, intercepting and/or decrypting of data by law enforcement is allowed. Thus, for example, section 69 of the IT Act allows for the interception, monitoring and decryption of information for the investigation of any offence. Section 69B allows for the monitoring and collection of traffic data to enhance cyber security as well as to identify, analyse and prevent any intrusion or spread of a computer contaminant in the country.

---

practice, there have been no instances so far where only fixed line Internet access has been shut down. See <https://internetshutdowns.in/about>.

259 See e.g. Saikia (7 April 2018).

260 For a detailed analysis of the legal frameworks governing Internet shutdowns in India, see SFLC.in (2018).

261 *Gaurav Sureshbhai Vyas v State of Gujarat & 5*, writ petition (PIL) no. 191 of 2015 (Gujarat).

In addition, through their licence conditions, telecom operators are obliged to provide extensive assistance, including through the installation of surveillance equipment, to law enforcement in their surveillance efforts[262]. Moreover, where access to data stored on company servers is concerned, it seems police continue to rely on section 91 of the Criminal Procedure Code. This section allows them access to the data without requiring the prior approval of a government official, as is the case when accessing data under section 69[263].

A number of systems have also been put into place to automate access to data thus gathered (e.g. the so called "CMS" or "Central Monitoring System"), to enable real-time detection of key words and phrases deemed suspicious across the Indian Internet, from social media to voice channels (e.g. NETRA or Network Traffic Analysis), and to collate and analyse data contained in standalone databases (e.g. NATGRID or National Intelligence Grid)[264]. A large number of systems to conduct sentiment analysis and social network analysis of India's social media landscape have been deployed as well[265]. Although it is not clear whether the latter limit themselves to publicly available personal data, it is noteworthy in this light that the draft Personal Data Protection Bill, 2018, explicitly provides for the Authority to specify purposes that would be considered "fair and reasonable" for the processing of such publicly available personal data. This would effectively establish an explicit legal ground to facilitate the mass surveillance of such data.

For the moment, details about all of these initiatives available in the public domain remain, however, sketchy. What the legal basis is for these efforts, and who the actors are that are responsible for their execution, is frequently not clear. This is particularly worrying as intelligence agencies in India are mostly established through executive order and do not come under parliamentary oversight[266].

In light of these extensive surveillance efforts, public order might thus well be enforced on the basis of surveillance provisions that do not have public order as a ground.

4.5. Cyberdefence

India does not have a formal national security strategy or national defence policy that can guide its cyber defence. While the Integrated Defence Staff (IDS), the armed forces' main tri-service body (drawing resources from all three services, i.e. the army, navy and air force), forwarded a draft National Security Strategy to the National Security Adviser in 2008, it was never formally approved[267].

---

[262] See SFLC.in (2014).

[263] See Srikumar et al. (2019).

[264] See SFLC.in (2014).

[265] See Sinha (2017).

[266] Nor, in fact, are they subject to audits by the Comptroller and Auditor General of India or to the Right to Information Act 2005. For a short overview of the issues involved, see Guruswamy (2010). For examples of the repeated calls for intelligence reforms, see Institute for Defence Studies and Analyses (2012) and Joshi and Pushan (2015) – the former also contains a detailed analysis of the challenges.

[267] See Rej and Joshi (2018).

In 2017, the Ministry of Defence did, however, release the Joint Doctrine of the Indian Armed Forces, a rare document to address all three services of the armed forces, and intended as a foundation on the basis of which all three services operate "in synergy[268]." The defence of cyberspace is included explicitly among the national security objectives in the document, which recognises information warfare, including cyberspace, as having an overarching role in military operations today.

This is not to say that cyberdefence has not been on India's agenda before this articulation. However, with terrorism at the heart of the agenda, the approach has not been a purely military one. For example, when the US and India instituted in 2000 a Joint Working Group on Counter Terrorism, this was quickly followed by the establishment of a subgroup on cybersecurity, a year later, again confirming the close intertwining of cybersecurity policy and terrorist threats in India[269].

Two measures that find mention in the Joint Doctrine for the Armed Forces are of particular importance here. First, there is the launch, in 2016, of an integrated Defence Communication Network, which "will enable all the stakeholders to share situational awareness for a faster decision making process" and is intended to facilitate a "smooth flow of data and information, effective networking and inter-Service integration, automation and interoperability[270]", necessary to win network centric wars.

Second, to enhance capability, economise expenditure and ensure calibration and coordination of operations with regard to information warfare and cyberspace, the Joint Doctrine also recognises the need for integrated structures that span across the three arms of India's defence forces. This had also been one of the recommendations of the Naresh Chandra Task Force in 2012, tasked with comprehensively reviewing India's national security requirements[271]. The Joint Doctrine notes the establishment of a Defence Cyber Agency (DCA) as a first step to doing so.

In 2018, the creation of the Defence Cyber Agency (DCA), to function under the Integrated Defence Staff, was approved by Prime Minister Narendra Modi. But rather than a full-fledged tri-service military cyber command, as initially proposed, the DCA for now is a simpler tri-service agency[272]. Moreover, while the exact mandate of the DCA, and in particular whether it will only have a defensive role or an offensive one as well, remains unclear, some reports indicate that its contributions will remain limited to the former[273], even if its capabilities should allow for both[274].

---

[268] See Headquarters Integrated Defence Staff (2017). A similar document was earlier circulated in 2006, but was classified; see Rej and Joshi (2018), p. 32.

[269] See Datta (2016).

[270] See Headquarters Integrated Defence Staff (2017), p. 49.

[271] See Kanwal (2018).

[272] See Pandit (29 April 2019).

[273] Ibid.

[274] See Sagar (1 June 2019).

While the Joint Doctrine of the Armed Forces may thus pay lip service to the importance of not just coordination but integration of the capabilities of different services in the armed forces, now the standard in many Western forces, the current constitution of the DCA is another indication that effective jointness and integration remain far off in the Indian Armed Forces. Inter-service tension, in part driven by the Army's efforts to position itself as "first among equals" and consequent turf-wars, continue to prevent this[275]. Moreover, like the DCA, other tri-service bodies, too, continue to remain weak. Where the DCA is concerned in particular, the different arms of India's defence forces reportedly continue to be reluctant to share information and resources[276]. The Joint Doctrine, as well, has been criticised for ultimately taking an Army-centric view, thus missing another important opportunity to "inject a new spirit of jointness into Indian thinking and institutions[277]". In addition, it has been argued that it also does little to address concerns that India lacks an integrated approach to cyber warfare and electronic warfare, as for example China does[278].

Whether the recent creation of a new post of Chief of Defence Staff, in late 2019, will change this, remains to be seen. The Chief of Defence Staff will be the principal military adviser to the Defence Minister as well as heading a new Department of Military Affairs. The Defence Cyber Agency will come under his command[279].

Efforts to develop an infrastructure for the protection of critical information infrastructure seem to have been more successful. As early as 2003, in an address to the World Summit on the Information Society, Mr. Arun Shourie, then Minister for Information Technology, Communications and Privatisation of the Government of India, noted the importance of protecting such systems from disruptions by terrorists and other adversaries[280]. When the IT Act was amended in 2008, the changes included a provision mandating the designation of a national nodal agency to take care of this function[281]. The National Cyber Security Policy, released in 2013, too, emphasised the importance of the protection and resilience of critical information infrastructure. Nevertheless, it took until early 2014 for a Gazette Notification to designate the National Critical Information Infrastructure Protection Centre as the national nodal agency, almost six years after the amendment of the IT Act first made this possible.

---

275 See Rej and Joshi (2018).

276 See Hooda (26 June 2019).

277 See Rej and Joshi (2018), p. 15.

278 See Bommakanti (2019).

279 See Sawhney (17 August 2019) and Chawla (4 October 2019). It deserves to be noted that not all are adverse to greater integration among the services of the armed forces: Vivekananda International Foundation (2019), for example, contains a number recommendations for the future development of the DCA by a group of officers now retired from the Indian armed forces, including on how the DCA can move from an agency to a full-fledged command within three years' time.

280 See Shourie (2003).

281 See section 70A of the Information Technology (Amendment) Act, 2008.

In November 2019, after the administrative networks of the Kudankulam nuclear power plant in South India was revealed to have been successfully hacked[282], the effectiveness of these institutions was, however, questioned again as well. Experts criticised the official Indian response for its "complacency" and/or "ignorance", as it revealed that India's cyberdefence strategies are based on outdated principles such as the air-gap strategy[283]. Although progress seems to be made – with the first joint cyber exercises of the Indian Armed Forces, which included scenarios of cyber-attacks on critical information infrastructure, conducted in April 2019[284] – India's progress where matters of cyberdefence are concerned thus remains limited.

4.6. Conclusion

The idiosyncrasies of India's political and economic trajectories since the early 1990s have had a profound impact on its cybersecurity framework in general and data protection policies in particular. At the same time as ICTs started to profoundly transform the world, economic liberalisation in India helped foster a boom in India's IT and ITeS sectors that led to a repositioning of the country as a global information technology superpower by the early 2000s. Moreover, by 2019, India had the second highest Internet user base in the world. Parallel to these trends, however, following a popular uprising against India's rule in Kashmir in 1990 and evidence of subsequent support from Pakistan to militants fighting in the region, concerns about how ICTs may impact national security in general, and may be utilised for terrorist purposes in particular, emerged as important new challenges.

The development of India's cybersecurity and data protection policy landscape reflects these contradictory pulls. From the Information Technology Act in the 2000s to the draft Personal Data Protection Bill and the Consumer Protection Act more recently, India continues to put into place policies to promote and protect the further growth of its digital economy. At the same time, however, these and other laws are infused with provisions that ensure the transparency of communication flows to the state, allowing law enforcement agencies widespread access to Indians' data, as well as the state's ability to control such flows when these are believed to pose a potential security threat. With the focus so firmly on surveillance and control of digital spaces, other aspects of cybersecurity policy, such as cyberdefence, have taken a backseat.

The resulting tension certainly has an impact on industry, which is faced with ever greater demands on the part of law enforcement to assist in its surveillance activities, as evidenced for example by the proposed changes to the Intermediaries Guidelines Rules. But those paying the greatest price are, in the final analysis, the people of India: as more and more Indians find their lives intimately entwined with technology, they also find themselves pulled into a digital surveillance architecture that makes

[282] See Sircar and Sachdev (30 October 2019) and Datta and Venkatanarayan (30 October 2019).

[283] See Das (4 November 2019).

[284] See Pandit (29 April 2019).

them legible to the state in unprecedented ways. They may be accorded some of the protections crucial to ensure trust in ICTs and the continued growth and development of the country's digital economy. But where such protections contradict the interests of the state, it is the latter that invariably prevail. In the absence of additional checks and balances, the relationship between the citizens of India and the state is fundamentally reconfigured in the process.

4.7. References

Bhatia, Gautam (17 February 2016). Free Speech and Public Order. Centre for Internet and Society. <https://cis-india.org/internet-governance/blog/free-speech-and-public-order-1>.

Bommakanti, Kartik (2019). Electronic and Cyber Warfare: A Comparative Analysis of the PLA and the Indian Army. ORF Occasional Paper 203. New Delhi, July 2019. Observer Research Foundation. <https://www.orfonline.org/research/electronic-and-cyber-warfare-a-comparative-analysis-of-the-pla-and-the-indian-army-53098/>.

Chawla, Gunjan (4 October 2019). India's New Cyber Defence Agency – II: Balancing Constitutional Constraints and Covert Ops? Medianama. <https://www.medianama.com/2019/10/223-india-defence-cyber-agency-part-2/>.

Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018). A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. New Delhi, 27 July 2019. Ministry of Electronics and Information Technology, Government of India. <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf>.

Comptroller and Auditor General of India (2016). Report of the Comptroller and Auditor General of India for the Year Ended March 2015. Union Government (Communications and IT Sector). Report No. 29 of 2016. New Delhi, 2016. Comptroller and Auditor General of India. <https://cag.gov.in/content/report-no-29-2016-compliance-audit-communication-it-sector-union-government>.

Concerned People (2018). Solving for Data Justice: A Response to the Draft Personal Data Protection Bill. New Delhi, 18 October 2018. Internet Democracy Project. <https://internetdemocracy.in/reports/datajustice/>.

Corbridge, Stuart & Harriss, John (2003). Reinventing India: Liberalisation, Hindu Nationalism and Popular Democracy. Second edition. New Delhi, Oxford University Press.

Das, Debak (4 November 2019). An Indian Nuclear Power Plant Suffered a Cyberattack. Here's What You Need to Know. Washington Post. <https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/>.

Datta, Bishakha (2017). Guavas and Genitals: An Exploratory Study on Section 67 of the Information Technology Act, India. Mumbai: Point of View.

Datta, Saikat (2016). Cybersecurity, Internet Governance and India's Foreign Policy: Historical Antecedents. New Delhi, January 2016. Internet Democracy Project. <https://internetdemocracy.in/reports/cybersecurity-ig-ifp-saikat-datta/>.

Datta, Saikat & Venkatanarayan, Anand (30 October 2019). Cyberattack Scare Dogs India's Nuclear Plants. Asia Times. <https://www.asiatimes.com/2019/10/article/cyberattack-scare-dogs-indias-nuclear-plants/>.

Duggal, Pavan (2005). Cyber Law and Its Implementation in India. Bagga, R.K.; Keniston, Kenneth & Mathur, Rohit Raj (eds.), The State, IT and Development. New Delhi, Sage.

Dutta, Prabhash K (24 August 2017). Right to Privacy: 5 Bills Yet No Law, How Parliament Has Dealt With Personal Data Protection. India Today. <https://www.indiatoday.in/india/story/right-to-privacy-fundamental-right-parliament-1031136-2017-08-24>.

Frankel, Francine R. (2005). India's Political Economy 1947-2004: The Gradual Revolution. Second Edition. New Delhi, Oxford University Press.

Galiya, Stuti (20 August 2019). India: Consumer Protection Act, 2019 – Key Highlights. Mondaq. <http://www.mondaq.com/india/x/838108/Dodd-Frank+Wall+Street+Reform+Consumer+Protection+Act/CONSUMER+PROTECTION+ACT+2019+KEY+HIGHLIGHTS>.

Gandhi, Jatin (27 March 2018). Srikrishna Committee Report on Data Protection and Privacy by May-End. Hindustan Times. <https://www.hindustantimes.com/india-news/srikrishna-committee-report-on-data-protection-and-privacy-by-may-end/story-KYTHD6DxcgkA9VwtZ24OrN.html>.

Glanz, James; Rotella, Sebastian; & Sanger, David E. (21 December 2014). In 2008 Mumbai Attacks, Piles of Spy Data, But an Uncompleted Puzzle. New York Times. <https://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html>.

Gopalakrishnan, Kris S. (26 April 2016). Indian IT and ITeS Journey: Liberalisation and Beyond. Live Mint. <https://www.livemint.com/Opinion/fNjocJ9cwlGCDqLWt2OjXP/Indian-IT-and-ITeS-journey-Liberalization-and-beyond.html>.

Greenleaf, Graham (1 June 2014). India's Draft the Right to Privacy Bill 2014 – Will Modi's BJP Enact it? Privacy Laws & Business International Report. N°. 129. Pp. 21-24. Available at SSRN. <https://ssrn.com/abstract=2481796>.

Group of Experts on Privacy Chaired by Justice A.P. Shah (2012). Report of the Group of Experts on Privacy (Chaired by Justice A.P. Shah, Former Chief Justice, Delhi High Court). New Delhi, 16 October 2012. Planning Commission, Government of India. <planningcommission.nic.in/reports/genrep/rep_privacy.pdf>.

Gupta, Apar (18 September 2007). The Personal Data Protection Bill, 2006. India Law and Technology Blog. <https://iltb.net/the-personal-data-protection-bill-2006-7c66721ef8d>.

Guruswamy, Menaka (27 September 2010). Regulating the Gentleman's Game: Intelligence Reform in India. Centre for the Advanced Study of India, University of Pennsylvania. <https://casi.sas.upenn.edu/iit/guruswamy>.

Headquarters Integrated Defence Staff (2017). Joint Doctrine Indian Armed Forces. New Delhi, April 2017. Directorate of Doctrine, Headquarters Integrated Defence Staff, Ministry of Defence. <https://www.ids.nic.in/IDSAdmin/upload_images/doctrine/JointDoctrineIndianArmedForces2017.pdf>.

Hooda, DS (26 June 2019). India's New Defence Cyber Agency Will Have to Work around Stovepipes Built by Army, Navy & Air Force: Lt Gen DS Hooda. News18. <https://www.news18.com/news/opinion/new-defence-cyber-agency-will-have-to-work-around-stovepipes-built-by-army-navy-air-force-lt-gen-hooda-2204033.html>.

IAMAI (2019). India Internet 2019. New Delhi, 26 September 2019. IAMAI and Nielsen.

Institute for Defence Study and Analyses (2012). A Case for Intelligence Reforms in India. IDSA Task Force Report. New Delhi, 2012. Institute for Defence Study and Analyses. <https://idsa.in/system/files/book/book_IntellegenceReform.pdf.>.

Internet Democracy Project (2018). Is the Fourth Way Going Far Enough? Our Submission to Meity on Draft Personal Data Protection Bill 2018. New Delhi, 12 October 2018. Internet Democracy Project. <https://internetdemocracy.in/reports/pdpb/>.

Jain, Rohit (29 August 2019). Consumer Protection Act 2019 Ushers in More Benefits for Consumers. Bloomberg Quint. <https://www.bloombergquint.com/law-and-policy/will-the-new-consumer-protection-act-make-consumers-king>.

Jasrotia, Sahil Singh; Sharma, Roop Lal & Mishra, Hari Govind (2019). Disruptions in Indian Telecom Sector: A Qualitative Study on Reliance Jio. Indore Management Journal. Vol. 11, n°. 1. Pp. 37-45. <https://www.iimidr.ac.in/wp-content/uploads/Vol11-1-03.pdf>.

Joshi, Manoj & Das, Pushan (2015). India's Intelligence Agencies: In Need of Reform and Oversight. ORF Issue Brief No. 98. New Delhi, July 2015. Observer Research Foundation. <https://www.orfonline.org/wp-content/uploads/2015/07/IssueBrief_98.pdf>.

Kanwal, Gurmeet (2018). Introduction: The Need for Defence Reforms. Kanwal, Gurmeet & Kohli, Neha (eds.), Defence Reforms: A National Imperative. New Delhi, Pentagon Press and Institute for Defence Studies and Analyses. <https://idsa.in/system/files/book/book-defence-reform.pdf>.

Kovacs, Anja & Ranganathan, Nayantara (2017). India. Association for Progressive Communications (ed.), Unshackling Expression: A Study on Laws Criminalising Expression Online in Asia. South Africa, Association for Progressive Communications. <https://www.giswatch.org/sites/default/files/giswspecial2017_web.pdf>.

Kovacs, Anja & Ranganathan, Nayantara (2019). Data Sovereignty, of Whom? Limits and Suitability of Sovereignty Frameworks for Data in India. Data Governance Network Working Paper 03. Mumbai, November 2019. Data Governance Network. <http://datagovernance.org/report/data-sovereignty>.

Krishnan, Vinayak & Sinha, Roshni (2019). Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018. Rules & Regulation Review. New Delhi, 30 January 2019. PRS Legislative Research. <prsindia.org/sites/default/files/bill_files/IT%20Intermediary%20Guidelines%20Amendment%20Rules%20Brief-For%20Upload.pdf>.

Law Commission of India (2017). Hate Speech. Report 267. New Delhi, March 2017. Law Commission of India. <lawcommissionofindia.nic.in/reports/Report267.pdf>.

Mankotia, Anandita Singh (24 July2019). Data Protection Bill: Changes Likely in Proposed Data Privacy Rules: Only Critical Data May Need to Be Housed in India. Economic Times. <https://economictimes.indiatimes.com/tech/internet/changes-likely-in-proposed-data-privacy-rules-only-critical-data-may-need-to-be-housed-in-india/articleshow/70355298.cms?from=mdr>.

Ministry of Electronics and Information Technology (2017). Constitution of a Committee of Experts to Deliberate on a Data Protection Framework for India. Office Memorandum No. 3(6)/2017-CLES. New Delhi, 31 July 2017. Ministry of Electronics and Information Technology, Government of India. <https://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf>.

Ministry of Electronics and Information Technology (2018). Comments Invited on Draft Intermediary Guidelines 2018. New Delhi, 24 December 2018. Ministry of Electronics and Information Technology, Government of India. <https://meity.gov.in/comments-invited-draft-intermediary-rules>.

Ministry of Home Affairs (2011). Draft Bill on Right to Privacy. Office Memorandum No. II/20034/250/2011-IS-II. New Delhi, 29 September 2011. Ministry of Home Affairs, Government of India. <https://cis-india.org/internet-governance/draft-bill-on-right-to-privacy>.

Na, Vijayashankar (9 July 2018). Cyber Appellate Tribunal Back in Action through TDSAT. Naavi. <https://www.naavi.org/wp/cyber-appellate-tribunal-back-in-action-through-tdsat/>.

Nappinai, N.S. (2010). Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study. Journal of International Commercial Law and Technology. Vol. 5., n° 1. Pp. 22-28.

Narrain, Siddharth (2016). Hate Speech, Hurt Sentiment and the (Im)Possibility of Free Speech. Economic and Political Weekly. Vol. 51, n°. 17. <https://www.epw.in/journal/2016/17/special-articles/hate-speech-hurt-sentiment-and-impossibility-free-speech.html>.

Pal, Sherill (6 February 2019). Intermediary Liability: Un-safe Harbour? Fortune India. <https://www.fortuneindia.com/opinion/intermediary-liability-un-safe-harbour/102944>.

Pandit, Rajat (29 April 2019). Forces Prepare to Deal with Cyber-attacks on Key Infrastructure. Economic Times. <https://economictimes.indiatimes.com/news/defence/forces-prepare-to-deal-with-cyber-attacks-on-key-infrastructure/articleshow/69091292.cms>.

Planning Commission (2011). Constitution of Group of Experts to Deliberate on Privacy Issues. Office Memorandum No. 13040/47/2011-CIT&I. New Delhi, 26 December 2011. CIT & I Division, Planning Commission, Government of India. <https://cis-india.org/internet-governance/constitution-of-group-of-experts.pdf>.

Ranganathan, Nayantara (9 August 2018). India's Data Protection Draft Ignores Key Next-Generation Rights. Asia Times. <https://www.asiatimes.com/2018/08/opinion/indias-data-protection-draft-ignores-key-next-generation-rights/>

Rej, Abhijnan & Joshi, Shashank (2018). India's Joint Doctrine: A Lost Opportunity. ORF Occasional Paper 139. New Delhi, January 2018. Observer Research Foundation. <https://www.orfonline.org/research/india-joint-doctrine-lost-opportunity/>.

Reserve Bank of India (2018). Storage of Payment System Data. Circular DPSS.CO.OD.No 2785/06.08.005/2017-18. Mumbai, 6 April 2018. Reserve Bank of India. <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0>.

Saikia, Arunabh (7 April 2018). India's Internet Shutdown: Most States Block Services without Following Centre's Rules. Scroll. <https://scroll.in/article/874565/internet-shutdown-most-states-continue-to-block-services-without-adhering-to-the-centres-new-rules>.

Sagar, Pradip R. (1 June 2019). Three-pronged Plan. The Week. <https://www.theweek.in/theweek/current/2019/05/31/three-pronged-plan.html>.

Sagar, Pradip R. (9 November 2019). Tech, A Risk. The Week. <https://www.theweek.in/theweek/cover/2019/11/09/tech-a-risk.html>.

Samanta, Pranab Dhal (7 January 2019). Government Exploring Ways to Exempt Security Agencies from Data Protection Bill. Economic Times. <https://economictimes.indiatimes.com/news/politics-and-nation/government-exploring-ways-to-exempt-security-agencies-from-data-protection-bill/articleshow/67413173.cms?from=mdr>.

Sarkar, Torsha (12 August 2019). Rethinking the Intermediary Liability Regime in India. CyberBRICS. <https://cyberbrics.info/rethinking-the-intermediary-liability-regime-in-india/>.

Sawhney, Pravin (17 August 2019). Where Does CDS Fit In? The Tribune. <https://www.tribuneindia.com/news/archive/where-does-cds-fit-in-818565>.

Shourie, Arun (2003). Statement by H.E. Mr. Arun Shourie, Minister for Information Technology, Communications and Privatisation, Government of India, at the World Summit on Information Society. Geneva, 11 December 2003. Permanent Mission of India to the Offices of the United Nations, Its Specialised Agencies and Other International Organisations in Geneva. <http://www.itu.int/net/wsis/geneva/coverage/statements/india/in.html>.

Sinha, Amber (2017). Social Media Monitoring. Bangalore, 13 January 2017. Centre for Internet and Society. <https://cis-india.org/internet-governance/files/social-media-monitoring/at_download/file>.

Sircar, Sushovan & Sachdev, Vakasha (30 October 2019). Kudankulam Cyber Attack Did Happen, Says NPCIL a Day after Denial. Bloomberg Quint. <https://www.bloombergquint.com/politics/kudankulam-nuclear-power-plant-malware-attack-correct-confirms-npcil>.

SFLC.in (2014). India's Surveillance State. New Delhi, March 2014. SFLC.in. <https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf>.

SFLC.in (2018). Living in Digital Darkness: A Handbook on Internet Shutdowns in India. New Delhi, May 2018. SFLC.in. <https://sflc.in/sites/default/files/reports/Living%20in%20Digital%20Darkness%20-%20A%20Handbook%20on%20Internet%20Shutdowns%20in%20India%2c%20May%202018%20-%20by%20SFLCin.pdf>.

Srikumar, Madhulika; Srinivasan, Sreenidhi; Kennedy-Mayo, DeBrae & Swire, Peter (2019). India-US Data Sharing for Law Enforcement: Blueprint for Reforms. New Delhi, January 2019. Observer Research Foundation and Cross-Border Requests for Data Project of the Georgia Tech Institute for Information Security and Privacy. <https://www.orfonline.org/research/india-us-data-sharing-for-law-enforcement-blueprint-for-reforms-47425/>.

Srivas, Anuj (12 December 2016). The Tragic and Comedic Functioning of India's Cyber Appellate Tribunal. The Wire. <https://thewire.in/banking/tragic-comedic-functioning-indias-cyber-appellate-tribunal>.

Suhag, Roopal & Sinha, Roshni (2018). The Consumer Protection Bill 2018. Legislative Brief. New Delhi, 27 April 2018. PRS Legislative Research. <prsindia.org/sites/default/files/bill_files/Legislative%20Brief%20-%20Consumer%20Protection%20Bill%2C%202018_0.pdf>.

Tewari, Ruhi & Nayak, Malathi (23 December 2008). Govt Pushes Through IT Bill; Wins Digital Snooping Right. Live Mint. <https://www.livemint.com/Home-Page/wRQFhAdHHDhAHWBj6qEUBJ/Govt-pushes-through-IT-Bill-wins-digital-snooping-right.html>.

Upadhya, Carol (2011). Software and the 'New' Middle Class in the 'New India'. Baviskar, Amita & Ray, Raka (eds.), Elite and Everyman: The Cultural Politics of the Indian Middle Classes. New Delhi, Routledge.

Varma, Satvik (2 September 2019). Consumer Protection Act 2019: Enhancing Consumer Rights. Bar and Bench. <https://www.barandbench.com/columns/consumer-protection-act-2019-enhancing-consumer-rights>.

Vivekananda International Foundation (2019). Credible Cyber Deterrence in Armed Forces of India. VIF Taks Force Report. New Delhi, March 2019. Vivekananda International Foundation. <https://www.vifindia.org/sites/default/files/Credible-Cyber-Deterrence-in-Armed-Forces-of-India_0.pdf>.

Annex

Country Report: India

1. Data Protection

▪ Scope

1. What national laws (or other type of normative acts) regulate the collection and use of personal data?

A draft Personal Data Protection Bill was released in 2018 and is expected to be tabled in Parliament soon. Until then, the Information Technology (Amendment) Act, 2008, provides limited protection. In addition, the **Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act,** 2016, and the **Aadhaar and Other Laws (Amendment) Act**, 2019 address questions regarding personal data specifically in the context of Aadhaar, India's unique ID. Sectoral directions and regulations, such as those issued by the Reserve Bank of India, also impact personal data. Further draft policies and laws that address aspects of data protection include the draft National e-Commerce Policy, 2019, and the DNA Technology (Use and Application) Regulation Bill, 2019.

2. Is the country a part of any international data protection agreement?

India is not part of any international data protection agreements.

3. What data is regulated?

The draft **Personal Data Protection Bill** applies to the processing of personal data that has been collected, disclosed, shared or otherwise processed within India, as well as to personal data that is processed by the state, an Indian company or citizen, or any person or body of persons incorporated or created under Indian law.

Section 43A of the **IT (Amendment) Act** concerns sensitive personal data or information in a computer resource owned, controlled or operated by a body corporate. ***Section 72A*** of **the IT (Amendment) Act** concerns personal information about a person which any person, including an intermediary, may have access to while providing services under the terms of a lawful contract.

4. Are there any exemptions?

The draft **Personal Data Protection Bill** shall not apply to the processing of anonymised data. It also exempts from a number of provisions in the Act:

1) necessary and proportionate processing in the interests of the security of the State, authorised by law and in accordance with the procedure established by law;

2) necessary and proportionate processing in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of law, authorised by law;

3) processing for the purpose of legal proceedings, including any judicial function;

4) processing for research, archiving, or statistical purposes, where, among other things, the purpose of processing cannot be achieved if the personal data is anonymised;

5) processing by a natural person for purely personal or domestic purposes.

6) processing for journalistic purposes, provided the processing is in compliance with any code of ethics issued by the Press Council of India or any media self-regulatory organisation;

7) manual processing by small entities.

In addition, no data fiduciary shall process such biometric data as may be notified by the Central Government, unless such processing is permitted by law.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, issued under ***Section 87*** read with ***Section 43A*** of **the IT (Amendment),** do away with the requirement to obtain prior permission from the provider of sensitive personal data or information before disclosing such data or information to a third party where access to such sensitive personal data or information is sought by government agencies mandated to do so under the law.

5. To whom do the laws apply?

The draft **Personal Data Protection Bill** extends to the whole of India. It applies to the State, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law. It also applies to data fiduciaries and data processors not present within the territory of India who engage in processing of personal data in connection with any business carried on in India, or any systematic activity of offering goods or services to data subjects within the territory of India, or in connection with any activity which involves the profiling of data subjects within the territory of India.

The **IT (Amendment) Act** applies to the whole of India as well as to any offence or contravention under the Act committed outside India by any person, irrespective of their nationality, provided the suspected offence involves a computer, computer system or computer network located in India. ***Section 43A*** of the **IT (Amendment) Act** specifically applies to body corporates, i.e. any company, including a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities. ***Section 72*** of the **IT (Amendment) Act** applies to any person, including an intermediary, who has secured access to material containing personal information about a person while providing services under the terms of a lawful contract.

6. Do the laws apply to foreign entities that do not have physical presence in the country?

Yes. For details, see above.

- **Definitions**

7. How are personal data defined?

The draft **Personal Data Protection Bill** defines personal data as 'data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identify of such natural person, or any combination of such features, or any combination of such features with any other information'.

The **IT (Amendment) Act** does not provide a definition.

8. Are there special categories of personal data (e.g. sensitive data)?

The draft **Personal Data Protection Bill** distinguishes 'sensitive personal data' (including 'biometric data', 'financial data', 'genetic data', 'health data', 'intersex status', 'official identifier', and 'transgender status') from personal data. It further provides the Central Government with the power to notify categories of personal data as 'critical personal data' that shall only be processed in a server or data centre located in India.

Section 43A of the **IT (Amendment) Act** also specifies and defines 'sensitive personal data and information'; the Reasonable Security Practices and Procedures Rules, 2011, under that section provide further detail.

9. How is the data controller and the data processor/operator defined?

Rather than 'data controller', the draft **Personal Data Protection Bill** uses the term 'data fiduciary', which means 'any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data'. The draft Bill defines 'data processor' as 'any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary'.

The **IT (Amendment) Act** does not include these definitions.

10. What are the data protection principles and how are they defined?

The draft **Personal Data Protection Bill** lists the following:

1) fair and reasonable processing, that respects the privacy of the data subject;

2) purpose limitation, meaning that the purposes are clear, specific and lawful, although incidental purposes that the data subject would 'reasonably expect the data to be used for' are allowed as well;

3) collection limitation, meaning that only data that is necessary for the purpose of processing should be collected;

4) lawful processing, meaning that processing shall only be done on the grounds specified in the Bill for personal data and sensitive personal data respectively;

5) notice (with the draft Bill specifying fourteen elements of information which the notice needs to contain), to be provided at the time of collection of the personal data or, if the data is not collected from the data subject, as soon as is reasonably practicable, and to be provided in a clear and concise

manner that is easily comprehensible and in multiple languages 'where necessary and practicable' – exemption of the notice obligation is provided where processing is required for prompt action;

6) data quality, which means that the data fiduciary needs to take reasonable steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purposes for which it is processed;

7) data storage limitation, which means that the data fiduciary shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed, unless longer retention is mandated by law; and

8) accountability, which means that the data fiduciary will comply with all obligations set out in the Act in respect of any processing undertaken by it or on its behalf, and can demonstrate that any processing undertaken by it or on its behalf is in accordance with the Act.

The **IT (Amendment) Act** does not list data protection principles.

11. Does the law provide any specific definitions with regards to data protection in the digital sphere?

The draft **Personal Data Protection Bill** also defines 'automated means'. In addition, its preamble highlights that its formulation in general has to be seen in the context of the growth of the digital economy.

Relevant definitions in the **IT (Amendment) Act** include those for 'access, 'intermediary' and 'reasonable security practices and procedures'.

▪ Rights

12. Is the data protection law based on fundamental rights (defined in Constitutional law or International binding documents)?

The Preamble to the draft **Personal Data Protection Bill** specifically states that the right to privacy is a fundamental right and that it is necessary to protect personal data as an essential facet of informational privacy.

The **IT (Amendment) Act** does not explicitly address this question.

13. What are the rights of the data subjects according to the law?

The draft **Personal Data Protection Bill** lists the following data subject rights:

1) the right to confirmation whether the data fiduciary is processing or has processed personal data of the data subject and to access a brief summary of that data and of the processing activities undertaken by the data fiduciary in relation to that data;

2) the right to, where necessary, correct inaccurate or misleading personal data, to complete incomplete personal data, and to update personal data that is out of date – where the data fiduciary does not agree that there is a need, it has to provide its justification to the data subject in writing and indicate alongside the relevant personal data that it is disputed;

3) the right to data portability, which means that the data subject has the right to receive their personal data under control of a data fiduciary in a structured, commonly used and machine-readable format, and to have it transferred to another data fiduciary in that format, wherever the processing has been carried out through automated means, except where the processing is necessary for specific functions of the State outlined in the Act, is in compliance of law, or where compliance with this provision would reveal a trade secret of any data fiduciary or would not be technical feasible;

4) the right to be forgotten, which is defined as the right to restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal under certain conditions and after the Adjudicating Officer has determined that these conditions have been satisfied.

▪ Obligations and Sanctions

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

In addition to the obligations data fiduciaries and data processors/operators have with regard to the implementation of the general data protection principles and the rights of the data subjects under the draft **Personal Data Protection Bill** (see above), data fiduciaries have a number of obligations under the Bill that specifically relate to the personal and sensitive data of children. These include processing the personal data of children in a way that protects and advances their rights and interests and incorporating mechanisms for age verification and parental consent. Additional obligations adhere to those data fiduciaries who process large volumes of personal data of children or who operate websites or provide services targeted at children, so-called guardian data fiduciaries.

Data fiduciaries are also obliged to take a number of privacy and accountability measures, including

privacy by design;

transparency regarding their general practices relating to the processing of personal data as well as regarding important processes in the processing of personal data related specifically to the data subject;

appropriate security safeguards;

procedures and mechanisms to address grievances of data subjects in an efficient and timely manner; and

notification of the Authority of breaches of the personal data processed by the controller where such breach is likely to cause harm to a data subject.

Data fiduciaries need to further ensure the storage on a server or data centre located in India of at least one serving copy of personal data to which the law applies.

Those data fiduciaries classified as ‘significant’ data fiduciaries are also required to appoint a data protection officer; to conduct data protection impact assessments; to keep accurate and up-to-data records of the details of their operations; and to have their policies and the conduct of their

processing of personal data audited annually by an independent data auditor. Classification as a significant data fiduciary will depend on such factors as the volume of data processed, the sensitivity of the personal data processed, the turnover of the data fiduciary, the risk of harm resulting from the processing and the use of new technologies for processing.

Data processors can only be engaged or involved in any way by data fiduciaries through a valid contract. Unless permitted by this contract, data processors are not allowed to involve any other data processor in the processing without the authorisation of the data fiduciary. Data processors can further only process personal data in accordance with the instructions of the data fiduciary, unless required to do otherwise under law, and have to treat any personal data that comes within their knowledge as confidential.

The Reasonable Security Practices and Procedures Rules, 2011, under **section 43A** of the **IT (Amendment) Act** also briefly outline a number of obligations.

15. Is notification to a national regulator or registration required before processing data?

As per the draft **Personal Data Protection Bill**, those data fiduciaries or classes of data fiduciaries who have been classified by the Data Protection Authority as 'significant data fiduciaries' are required to register with the Authority. Classification as a significant data fiduciary will depend on such factors as the volume of data processed, the sensitivity of the personal data processed, the turnover of the data fiduciary, the risk of harm resulting from the processing and the use of new technologies for processing.

Further, although not required before processing the data, the transfer of sensitive personal data outside the territory of India to a person or entity engaged in the provision of health or emergency services where such transfer is strictly necessary for prompt action requires notification to the Authority within the time period that will be prescribed. Where a data fiduciary seeks to transfer personal data outside the territory of India subject to standard contractual clauses or intra-group schemes that have been approved by the Authority, it also needs to certify and periodically report to the Authority that the transfer is made under a contract that adheres to such standard contractual clauses or intra-group schemes and that it will bear liability for any harm caused in the case of non-compliance.

16. Does the law require privacy impact assessment to process any category of personal data?

As per the draft **Personal Data Protection Bill**, significant data fiduciaries are required to undertake a data protection impact assessment when they intend to undertake any processing involving new technologies, or large scale profiling, or the use of sensitive personal data such as genetic or biometric data, or any other processing which carries a risk of significant harm to data subjects. In addition, the Data Protection Authority may specify further circumstances or classes of data or processing operations for which a data protection impact assessment by significant data fiduciaries is mandatory. The Data Protection Authority can also specify instances in which

significant data fiduciaries need to engage a data auditor under the Act to carry out the data protection impact assessment. Where the Data Protection Authority is of the view that any processing activity undertaken by data fiduciaries other than significant data fiduciaries carries a risk of significant harm to data subjects, it can notify that data protection impact assessments are mandatory for them as well.

17. What conditions must be met to ensure that personal data are processed lawfully?

The draft **Personal Data Protection Bill** recognises the following grounds for the processing of personal data:

1) on the basis of consent;

2) for functions of the State, including the provision of any service or benefit to the data subject from the State and the issuance of any certification, licence or permit for any action or activity of the data subject by the state;

3) in compliance with law or any order of any court or tribunal;

4) when necessary for prompt action in medical emergencies and during epidemics, disasters and breakdowns of public order;

5) for purposes related to employment, where processing on the basis of consent is inappropriate or would involve a disproportionate effort, including recruitment, termination, provision of any benefit to the employee, verification of attendance of the employee and any other activity relating to the assessment of the employee's performance;

6) for reasonable purposes, including the prevention and detection of any unlawful activity, whistle blowing, mergers and acquisitions, network and information security, credit scoring, the recovery of debt and the processing of publicly available personal data.

18. What are the conditions for the expression of consent?

The draft **Personal Data Protection Bill** requires consent to be given no later than at the beginning of processing, with consent being valid when it is free, informed, specific, clear and capable of being withdrawn. Where explicit consent for sensitive personal data is concerned, the Bill sets additional, higher standards for the consent be considered informed, clear and specific.

19. If the law foresees special categories of data, what are the conditions to ensure the lawfulness of processing of such data?

The draft **Personal Data Protection Bill** recognises the following grounds for the processing of sensitive personal data:

1) explicit consent;

2) for certain functions of the State, including the exercise of any function of the State authorised by law for the provision of any service or benefit to the data principal;

3) in compliance with any law which explicitly mandates such processing or any order of any court or tribunal;

4) certain categories of sensitive personal data, including passwords, financial data, health data, official identifiers, genetic data and biometric data, may be processed when necessary for prompt action in medical emergencies are during epidemics, disasters and breakdowns of public order.

The Data Protection Authority may specify further categories of personal data as sensitive personal data and may also specify any further grounds on which such specified categories of sensitive personal data may be processed.

The Reasonable Security Practices and Procedures Rules, 2011, under the **IT (Amendment) Act** require the provider of sensitive personal data or information to provide consent for the purpose for which the data or information will be used before such data or information is collected. Such consent needs to be written and capable of being withdrawn. In the latter case, the body corporate shall have the option not to provide the goods or services for which the sensitive personal data or information was sought.

20. What are the security requirements for collecting and processing personal data?

The draft **Personal Data Protection Bill** requires the data fiduciary and data processor to implement security safeguards such as the use of de-identification and encryption, steps necessary to protect the integrity of personal data, and steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data, having regard to the nature, scope and purpose of the processing of the personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing.

Where a breach of personal data is likely to cause harm to any data subject, the draft **Personal Data Protection Bill** requires the data fiduciary to notify the Data Protection Authority of the breach, as well as of 1) the nature of the personal data that has been breached, 2) the number of data subjects affected by the breach, 3) possible consequences of the breach, and 4) measures taken to remedy the breach. The Authority will determine whether or not the breach should be reported to the data subject.

The Reasonable Security Practices and Procedures Rules, 2011, under the **IT (Amendment) Act** specify a number of security precautions to be taken as well, including the adoption of international standards for information security management or other codes of best practices that have been approved and notified by the Central Government.

21. Is there a requirement to store (certain types of) personal data inside the jurisdiction?

The draft **Personal Data Protection Bill** requires every data fiduciary to ensure that at least one serving copy of personal data to which the Act applies is stored on a service or in a data centre located in India. The Central Government may notify certain categories of personal data as exempt from this requirement on the grounds of necessity or strategic interests of the State, but sensitive personal data cannot be exempted. In addition, the draft **Personal Data Protection Bill** gives the Central Government the power to notify categories of personal data as critical personal data, which shall only be processed in a server or data centre located in India.

Sectoral localisation requirements already exist in India, including as required by the Reserve Bank of India Notification on Storage of Payments Systems Data of April 2018; the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017; the Companies Act, 2013, and the attendant rules and the Unified Access Licence for Telecom. Localisation requirements of various kinds have also been included in other draft policies and regulations, such as the draft E-Commerce Policy 2019 and the draft e-Pharmacy Rules 2018.

22. What are the requirements for transferring data outside the national jurisdiction?

As per the draft **Personal Data Protection Bill**, personal data other than those categories of sensitive personal data that have been notified as critical personal data may be transferred outside of India where:

1) the transfer is made subject to standard contractual clauses or intra-group schemes that have been approved by the Data Protection Authority after it has been satisfied that these effectively protect the rights of data subjects under the Act; or

2) the Central Government, after consultation with the Authority, has prescribed that transfers to a particular country, or to a sector within a country or to a particular international organisation is permissible as it believes that the relevant personal data shall be subject to an adequate level of protection.

3) the Authority approves a particular transfer or set of transfers as permissible due to a situation of necessity.

In addition, in the first two cases, the data subject needs to have consented to the transfer of personal data or explicitly consented in the case of sensitive personal data that has not been notified as critical personal data.

Sensitive personal data that has been notified as critical personal data can be transferred outside of India:

1) to a particular person or entity engaged in the provision of health services or emergency services where such transfer is strictly necessary for prompt action;

2) to a particular country, a prescribed sector within a country or to a particular international organisation that has been prescribed, where the Central Government is satisfied that such transfer or class of transfers is necessary for any class of data fiduciaries or data subjects and does not hamper the effective enforcement of the Act.

23. Are data transfer agreements foreseen by the law?

Yes, see above.

24. Does the relevant national regulator need to approve the data transfer agreements?

Yes, see above.

25. What are the sanctions and remedies foreseen by the law for not complying with the obligations?

The draft **Personal Data Protection Bill** provides for fines and, where a data subject who has suffered harm as a result of any violation files a complaint, compensation for the data subject. Where a violation is listed as an offence in the Bill, it can also attract a prison term, as well as a fine. In addition, the Data Protection Authority can issue warnings, reprimands, and orders to cease and desist from committing or causing any violation of the Act; require the data fiduciary or data processor to modify its business; temporarily suspend or discontinue the business or activity of the data fiduciary or data processor that is in contravention of the provisions of the Act; vary, suspend or cancel any registration granted by the Authority in the case of a significant data fiduciary; suspend or discontinue any cross-border flow of personal data; and require the data fiduciary or data processor to take any such action in regards to a matter that arose during an inquiry as the Authority may deem fit.

Section 43 of the **IT (Amendment) Act** provides for compensation to the victim, while section 72A of the Act attracts a prison term and/or a fine.

- **Actors**

26. What actors are responsible for the implementation of the data protection law?

The draft **Personal Data Protection Bill** provides for the establishment of a Data Protection Authority of India, which will be the main actor responsible for implementation. It also provides for the establishment of an Appellate Tribunal. Appeals to decisions or orders of the Appellate Tribunal are to be made to the Supreme Court of India.

An adjudicating officer appointed by the Central Government will adjudicate matters in which the claim for injury or damage under ***Section 43A*** of the **IT (Amendment) Act** does not exceed Rs. five crores (Rs. 50 million). The jurisdiction in respect of claims for injury or damage exceeding that amount vests with the competent court. Appeals to an order from an adjudicating officer can be made to the Cyber Appellate Tribunal. Appeals to decisions or orders from the Cyber Appellate Tribunal are to be made to the High Court.

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

The Data Protection Authority will be a body corporate, with the chairperson and members appointed by the Central Government on the recommendation of a selection committee. When the Authority calls for information from or conducts inspections and inquiries into the affairs of data fiduciaries in accordance with the provisions of the Act, it shall have the same powers in a number of respects as those vested in a civil court under the Code of Civil Procedure, 1908. For the purpose of imposing penalties and awarding compensation, the Authority will have a separate adjudication wing, with the number, qualification, jurisdiction and manner and terms of appointment of the adjudicating officers to be prescribed by the Central Government; the draft Bill requires this to be done in a manner that ensure the operational segregation, independence and neutrality of the adjudication wing.

The Appellate Tribunal, though it has the powers to regulate its own procedures, shall be deemed to be a civil court in a number of respects and every proceeding before the Appellate Tribunal shall be deemed to be a judicial proceeding.

Under the **IT (Amendment) Act**, the adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal, and all proceedings before it shall be deemed judicial proceedings. The Cyber Appellate Tribunal, though it has the powers to regulate its own procedures, too, shall be deemed to be a civil court in a number of respects, and every proceeding before it shall be deemed to be a judicial proceeding.

28. What are the powers of the actors responsible for the implementation of the data protection law?

The draft **Personal Data Protection Bill** requires the Authority is to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of the Act, and promote awareness of data protection. It contains a large number of powers and functions to help concretise that mandate, including the power to issue codes of practice, to issue directions to data fiduciaries and data processors, to call for information from data fiduciaries and data processors, to conduct an inquiry, to engage in search and seizure, and to take action pursuant to an inquiry.

When the Authority calls for information from or conducts inspections and inquiries into the affairs of data fiduciaries in accordance with the provisions of the Act, it shall have the same powers in a number of respects as those vested in a civil court under the Code of Civil Procedure, 1908, including the discovery and production of books of account and other documents at such time and place as may be specified; the inspection of any book, document, register or record of any data fiduciary; summoning and enforcing the attendance of any person and examining them under oath; and issuing commission for the examination of witnesses or documents.

The Appellate Tribunal is to hear appeals from orders of the Authority and of the adjudicating officers of the Authority's adjudication wing, as well as challenges to search and seizure orders by the Authority. It, too, has a number of powers as vested in a civil court under the Code of Civil Procedure, 1908, including those listed above for the Data Protection Authority as well as, among other things, receiving evidence on affidavits and dismissing an application for default or examining it, ex parte.

Under the **IT (Amendment) Act**, the adjudicating officer shall have the powers of a civil court, which are conferred on the Cyber Appellate Tribunal. The Cyber Appellate Tribunal has the powers of a civil court under the Code of Civil Procedure 1908, in a number of respects while trying a suit; these powers largely, though not completely, overlap with those of the Appellate Tribunal established under the draft Data Protection Bill.

2. Consumer Protection

▪ Scope

29. What national laws (or other type of normative acts) regulate consumer protection?

In August 2019, the **Consumer Protection Act**, 2019 was adopted, which will replace earlier legislation from 1986. Draft Consumer Protection (e-Commerce) Rules, 2019, made under section 101 of the Consumer Protection Act, were made available for public consultation in November 2019. The draft National E-Commerce Policy 2019, too, has sections that are of relevance. Existing sectoral regulation such as the Food Safety and Standards Act, 2006, continues to apply as well.

30. Is the country a party of any international consumer protection agreement?

Since 2009, India is a party to the Convention for the Unification of Certain Rules for International Carriage by Air (also known as the Montreal Convention).

31. To whom do consumer protection laws apply?

The 2019 Act extends to the whole of India, except Jammu and Kashmir. The draft e-Commerce Rules are intended to regulate every e-commerce entity carrying out or intending to carry out e-commerce business in India as well as sellers selling or advertising their products or services through an e-commerce platform. Entities or businesses notified otherwise by the government are excluded.

32. Do the laws apply to foreign entities that do not have physical presence in the country?

The draft **e-Commerce Rules** require all e-commerce entities that seek to carry out e-commerce business in India to register as a legal entity under the laws of India.

▪ Definitions

33. How is consumer protection defined?

Neither the **Consumer Protection Act** nor the draft **e-Commerce Rules** define consumer protection.

34. How are consumers defined?

The **Consumer Protection Act** defines a' consumer' as any person who buys any goods or hires or avails of any service for a consideration, including where this has been paid or promised only in part or where it is bought under a system of deferred payment. It includes any user of the good and any beneficiary of the service other than the person who buys the good or hires the service, where such use is made, or such service is availed of with the approval of the buyer. It does not include a person who buys such goods or avails of such service for resale or for any commercial purpose, except if the latter refers to the purpose of earning his livelihood, by means of self-employment.

35. How are providers and producers defined?

The **Consumer Protection Act** defines an 'electronic service provider' as 'a person who provides technologies or processes to enable a product seller to engage in advertising or selling goods or services to a consumer and includes any online marketplace or online auction sites'. A 'product service provider', in relation to a product, means 'a person who provides any service in respect of such product'.

The **Consumer Protection** does not define 'producer', but 'manufacturer' and 'product manufacturer'. A 'manufacturer' is 'a person who (i) makes any product or parts thereof; or (ii) assembles parts thereof made by others; or (iii) puts or causes to be put his own mark on any products made by any other person'. A 'product manufacturer' is defined as a person who does any of the above or '(iv) makes a product and sells, distributes, leases, installs, prepares, packages, labels, markets, repairs, maintains such product or is otherwise involved in placing such product for commercial purpose; (v) designs, produces, fabricates, constructs or re-manufactures any product before its sale; or (vi) being a product seller of a product, is also a manufacturer of such product'.

36. Does the law provide any specific definitions with regards to consumer protection in the digital sphere?

In the **Consumer Protection Act**, 2019, as compared to the 1986 Act, a number of definitions have been included or expanded to address consumer protection in the digital sphere. For example, the law states explicitly that where the expressions 'buys any goods' and 'hires or avails any services' is used in the definition of 'consumer', this includes offline or online transactions through electronic means. In addition, the definition of 'advertisement' includes any audio or visual publicity, representation, endorsement or pronouncement made by means of electronic media, Internet or website. The definition of 'unfair trade practices' includes permitting the publication of advertisements, whether in any newspaper or otherwise, including by way of electronic record, for the sale or supply at a bargain price of goods or services that are not intended to be offered for sale or supply at the bargain price, or not for a period and in quantities that can be considered reasonable seeing the nature of the market, business and advertisement. The law also defines 'e-commerce'.

The draft **e-Commerce Rules** further define 'e-commerce entity', 'inventory-based model of e-commerce' and 'market-based model of e-commerce'. Definitions of 'electronic record' and 'information' in the draft Rules have been replicated from the Information Technology Act.

- **Rights**

37. Is the consumer protection law based on fundamental rights (defined in Constitutional law or International binding documents)?

Neither the **Consumer Protection Act** nor the draft **e-Commerce Rules** explicitly address this question.

38. What are the rights of the consumer defined by the law with reference to digital good and services?

The **Consumer Protection Act** only defines consumer rights in a general manner, to include the following:

(i) the right to be protected against the marketing of goods, products or services which are hazardous to life and property;

(ii) the right to be informed about the quality, quantity, potency, purity, standard and price of goods, products or services, as the case may be, so as to protect the consumer against unfair trade practices;

(iii) the right to be assured, wherever possible, access to a variety of goods, products or services at competitive prices;

(iv) the right to be heard and to be assured that consumer's interests will receive due consideration at appropriate fora;

(v) the right to seek redressal against unfair trade practice or restrictive trade practices or unscrupulous exploitation of consumers; and

(vi) the right to consumer awareness.

The draft **e-Commerce Rules** do not explicitly address the rights of the consumer.

39. Is consumer protection law applicable to users of zero price service i.e. free of charges?

With the exception of specialised services (such as remote surgery), zero rating by Internet access providers is not allowed in India. The definition of 'service' in the **Consumer Protection Act** explicitly includes within its scope the provision of facilities in connection with telecom but does not include the rendering of any service free of charge.

▪ Obligations and Sanctions

40. Does the law establish specific security requirements to provide digital services or goods?

The **Consumer Protection Act** does not explicitly address this question.

The draft **e-Commerce Rules** require e-commerce entities to ensure that personally identifiable information of customers is protected and that such data collection, use and storage comply with provisions of the Information Technology (Amendment) Act, 2008, which includes, among others, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules. The draft e-Commerce Rules also require payments for sale to be facilitated in conformity with the guidelines of the Reserve Bank of India, which include security requirements as well.

41. What are the sanctions and remedies foreseen by the law for now complying with the obligations?

Where a violation is listed as an offence in the **Consumer Protection Act**, it can attract a prison term as well as a fine. The court can also suspend the licence of anyone found guilty for a period of up to two years or cancel the licence in case of second or subsequent conviction.

The Central Consumer Protection Authority (the Central Authority) can order the recalling of goods or withdrawing of services; the reimbursement of the prices of goods and services recalled to the purchasers; and the discontinuation of practices which are unfair and prejudicial to the consumers' interest. It can also issue directions to all relevant parties to discontinue or modify false or misleading advertisements, prohibit the endorser of a false or misleading advertisement from making further endorsements and impose penalties.

The Consumer Disputes Redressal Commissions at district, state and national level can order the opposite party to remove defects pointed out; to replace the goods with new goods; to reimburse the price or charge paid by the consumer with interest; to provide compensation to the consumer; to discontinue unfair or restrictive trade practices and not to repeat them; not to offer the hazardous or unsafe goods or services for sale or withdraw them from sale and to cease to manufacture them; to issue corrective advertisement; to provide for adequate costs to parties; and to cease and desist from issuing misleading advertisements. In addition, the State and National Commissions can declare any terms of contract, which is unfair to any consumer, null and void.

- **Actors**

42. What bodies are responsible for the implementation of the consumer protection law?

The principal actors provided for under the Act are the **Central Consumer Protection Authority** (the Central Authority), including its investigation wing, and Consumer Disputes Redressal Commissions at the district, state and national levels (the Commissions), each of which will have a Consumer Mediation Cell attached to them. The Act also provides specific powers to the district collectors. Appeals to orders of the National Consumer Disputes Redressal Commission are to be heard by the Supreme Court.

The Act also sets up Consumer Protection Councils at the national, state and district levels, to give advice on the promotion and protection of the consumers' rights under the Act. Its members include the minister in charge of consumer affairs at the state and national levels, and the district collector at the state level.

43. Is there a specific consumer protection body? If so, what is its administrative structure?

The objective of the **Central Consumer Protection Authority** is to regulate matters relating to the violation of rights of consumers, unfair trade practices and false or misleading advertisements which are prejudicial to the interests of the public and consumers, and to promote, protect and enforce the rights of consumers as a class.

The Central Authority, still to be set up at the time of writing, shall be headed by a Chief Commissioner, as well as having a number of other Commissioners as prescribed, all to be

appointed by the Central Government. Headquartered in Delhi, it may have regional and other offices in any other part of India, as per the Central Government's decision. The Central Government shall provide a number of officers and other employees to the Central Authority, as considered necessary for the Central Authority's efficient functioning. The Central Authority may further engage a number of experts and professionals of integrity and ability with relevant specialised knowledge and expertise. The Central Authority will have an investigation wing, to conduct inquiries or investigations under the Act, as directed by the Central Authority. The Director-General of the investigation wing, as well as other officials, may be appointed by the Central Government.

44. What are the powers of the bodies responsible for the implementation of the consumer protection law?

The **Consumer Protection Act** lists a large number of powers and functions of the Central Authority, including to inquire or cause an inquiry or investigation into violations of consumer rights or unfair trade practices; to file complaints before the District, State and National Commissions; to intervene in proceedings before the Commissions that concern allegations of violation of consumer rights or unfair trade practices; to review matters relating to, and factors inhibiting enjoyment of consumer rights and recommend appropriate remedial measures; to mandate the use of unique and universal goods identifiers and to issue guidelines to prevent unfair trade practices; and to issue safety notices. It can also recommend adoption of international covenants and best international practices on consumer rights, undertake research, raise awareness, and provide advice to Government Departments.

Where the investigation wing of the **Central Authority or the District Collector** engage in an inquiry or investigation, they will have powers of search and seizure. District Collectors may investigate complaints within their jurisdiction on a complaint or reference from the Central Authority or a Commissioner of a regional office.

The specific actions that the Central Authority can take, following an investigation, have been documented above, in the section on sanctions and remedies.

The District, State and National Commissions are quasi-judicial bodies that can entertain consumer complaints of different value and have the same powers in a number of respects as those vested in a civil court under the Code of Civil Procedure, 1908. Every proceeding before the Commissions shall be deemed a judicial proceeding. With the agreement of all parties involved, the Commissions can refer any complaint to the Consumer Meditation Cell attached to the relevant Commission. The Commissions can also review their own orders. The State and National Commissions will further hear appeals to decisions of the preceding level. In addition, they can, in particular circumstances, call for the records and pass appropriate orders in any consumer dispute pending before or decided by the preceding level and can transfer cases pending before the lower level(s). Where a person fails to comply with an order by a Commission, the Commission shall have the power of a Judicial

Magistrate of first class for the trial of that offence. The specific actions that a Commission can take following an investigation have been documented in the section on sanctions and remedies.

3. Cybercrime

▪ Scope

45. What national laws (or other type of normative acts) regulate cybercrime?

The main act in India to specifically regulate cybercrime is the **Information Technology (Amendment) Act**, 2008. Other laws include relevant sections as well, however, such as, for example, the Copyright Act, 1957, and the **Protection of Children from Sexual Offences (Amendment) Act,** 2019. In addition, the **Indian Penal Code** and the **Indian Evidence Act**, 1872 too, continue to apply.

46. Is the country a part of any international cybercrime agreement?

India has not signed any international cybercrime agreement.

47. What cybercrimes are regulated?

The **IT (Amendment) Act** addresses a wide range of cybercrimes, from hacking-related offences over crimes related to impersonation and fraud, and from violations of privacy concerning the private areas of any person to offences related to obscenity and sexually explicit material, including child sexual abuse images.

Other laws, such as the **Copyright (Amendment) Act**, 2012 and the **Protection of Children from Sexual Offences (Amendment) Act,** 2019, address crimes specific to the domain they cover (in the case of these examples, copyright violations and child sexual abuse images respectively).

While most provisions of the **Indian Penal Code** have general applicability, some recognise cyberspace related aspects of a crime specifically. For example, the offence of stalking is defined in the Indian Penal code to explicitly include monitoring 'the use by a woman of the internet, email or any other form of electronic communication'.

48. To whom do the laws apply?

The **IT (Amendment) Act** applies to the whole of India as well as to any offence or contravention under the Act committed outside India by any person, irrespective of their nationality, provided the suspected offence involves a computer, computer system or computer network located in India.

49. Do the laws apply to foreign entities that do not have physical presence in the country?

Yes, see above.

▪ Definitions

50. How is cybercrime generally defined by the national law?

The **IT (Amendment) Act** does not define cybercrime.

51. What are the cybercrimes provided for by the law and how are they defined?

The **IT (Amendment) Act** includes offences such as:

- tampering with computer source documents;
- computer related offences such as damaging computers and computer systems;
- dishonestly receiving stolen computer resources or communication;
- identity theft and cheating by personation; violating the privacy of the private area of any person;
- publishing or transmitting obscene or sexually explicit material, or material depicting children in a sexually explicit act;
- publishing an electronic signature certificate while knowing it to be false in certain particular or publishing it for a fraudulent or unlawful purpose.

While constituent elements of the crime are at times defined in detail, the crimes as such are not.

52. How is a computer system defined?

The **IT (Amendment) Act** defines a 'computer system' as 'a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions'.

53. How are computer data defined?

The **IT (Amendment) Act** defines data as 'a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer'.

54. How are forensic data defined?

The **IT (Amendment) Act** does not define forensic data, nor does the Indian Evidence Act. The **IT (Amendment) Act** does define 'electronic form evidence' as 'any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cellphones, digital fax machines'.

55. How are service providers defined?

The **IT (Amendment) Act** does not define the term 'service providers'. However, it defines 'intermediary', 'with respect to any particular electronic records', as 'any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes'.

56. Does the national law provide any other definitions instrumental to the application of cybercrime legislation?

The **IT (Amendment) Act** also defines 'access', 'addressee', 'affixing [electronic signature]', 'asymmetric crypto system', 'communication device', 'computer', 'computer network', 'computer resource', 'cybercafé', 'cyber security', 'digital signature', 'electronic form', 'electronic record', 'electronic signature', 'function' in relation to a computer, 'information', 'key pair', 'originator', 'private key', 'public key', 'secure system', 'security procedure', 'subscriber' and 'verify' as well as a number of terms related to the implementation and enforcement of the Act, including to the institutions involved and their roles and functions.

▪ Rights

57. Is the cybercrime law based on fundamental rights (defined in Constitutional law or International binding documents)?

The **IT (Amendment) Act** does not explicitly address this question.

58. What are the rights of the victim and the accused?

The **IT (Amendment) Act** specifies that no compensation awarded, penalty imposed, or confiscation made under the Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force. It allows for the compounding of contraventions or offences in some circumstances, and also specifies that offences with up to three years of imprisonment are available. Beyond this, rights that are specific to cybercrime are not specified in either the **IT (Amendment) Act** or the Indian Evidence Act.

▪ Procedures

59. Is there a specific procedure to identify, analyse, relate, categorise, assess and establish causes associated with forensic data regarding cybercrimes?

The **Indian Evidence Act** was amended by the **IT (Amendment) Act** to include electronic records explicitly in the definition of 'documentary evidence', as well as to include terms such as 'digital signature', 'electronic form' and 'secure electronic record', as defined by the **IT (Amendment) Act,** in the evidentiary mechanisms that the Indian Evidence Act provides for. This includes a lengthy section on the admissibility of electronic evidence (section 65B of the Indian Evidence Act).

60. In case of transnational crimes, how is cooperation between the national law enforcement agency and the foreign agents regulated?

The **IT (Amendment) Act** does not address this question. Most commonly, requests to foreign agents for the content of stored electronic communication are made through the MLAT process. As specified in the Allocation of Business Rules of the Government of India, the Ministry of Home Affairs is the nodal Ministry and the Central authority for seeking and providing mutual legal assistance in criminal

law matters. Section 105 of the Criminal Procedure Code speaks of reciprocal arrangements to be made by the Central Government with foreign governments with regard to the service of summons/warrants/judicial processes. Accordingly, the Ministry of Home Affairs (MHA) has entered into Mutual Legal Assistance Treaties/Agreements on criminal Matters with 39 countries, which provide for the serving of documents. Requests can also be made through the letters rogatory process, which involves the courts in both countries. Such requests can be based on MLATs, MoUs or reciprocity and they, too, need approval from the MHA. Investigating agencies can take the help of the International Police Cooperation Cell (IPCC) of the Central Bureau of Investigation (CBI), an Indian intelligence agency, in preparing such requests. The IPCC is also the nodal point in India for cooperation with and through INTERPOL. Finally, the Indian Computer Emergency Response Team (CERT-IN) also has signed Memorandums of Understanding with agencies in a number of countries to further cooperation on cybersecurity.

61. Are there any exceptions to the use of mutual legal assistance procedure to investigate the crime?

There are. For example, the India-US MLAT excludes political offences as well as offences under military law, subject to some exceptions, while the India-Malaysia MLAT excludes, among other things, requests where there is substantial ground to believe that these were made for the purpose of investigating, prosecuting, punishing or otherwise causing prejudice to a person on account of the person's race, religion, sex, ethnic origin, nationality or political opinions.

62. Does the national law require the use of measures to prevent cybercrimes? If so, what are they?

Specific measures are specified in the rules attendant to several provisions of the **IT (Amendment) Act**, such as those made under section 16, regarding secure procedures and practices for electronic records and signatures, and under section 43A, regarding compensation for failure to protect data. Further, under section 70B, **CERT-IN** can provide guidance that needs to be adhered to. Under section 89, the Controller is granted the power to make regulations on matters such as standards.

▪ Obligations and Sanctions

63. What obligations do law enforcement agencies have to protect the data of the suspect, the accused and the victim?

The Information Technology (Procedure and Safeguard for Monitoring and Collection Traffic Data or Information) Rules, 2009, made under section 69B of the **IT (Amendment) Act**, prohibit the disclosure or use of traffic data or information by the agency authorised to monitor or collect traffic data for any purpose other than the forecasting of imminent cyber threats or general trends of port-wise traffic on the Internet, or general analysis of cyber incidents, or for investigation or in judicial proceedings before a competent court in India. Section 69B provides the Central Government with the power to authorise the monitoring and collection of traffic data through any computer resource

for cyber security. Beyond this, neither the **IT (Amendment) Act** nor the **Indian Evidence Act** address this question explicitly in the context of cybercrime. In the draft **Personal Data Protection Bill**, 2018, processing for the prevention, detection, investigation and prosecution of contraventions of law or for the purpose of legal proceedings are included in the exemptions, severely restricting law enforcement agencies' obligations to protect personal data.

64. What are the duties and obligations of the National Prosecuting Authorities in cases of cybercrime?

Section 80 of the **Act** outlines the power of police officers and other officers to enter, search, etc. Procedural guidelines under section 69B of the Act are provided in the Information Technology (Procedure and Safeguard for Monitoring and Collection Traffic Data or Information) Rules, 2009. Further details on the duties and obligations of the prosecuting authorities specifically in cases of cybercrime are not provided in either the **IT (Amendment) Act** or the Indian Evidence Act.

65. Does the law impose any obligations on service providers in connection with cybercrime?

Section 79 of the **IT (Amendment) Act** and the attendant rules provide intermediaries with exemption from liability, provided that they, among other things, observe due diligence while discharging their duties under the Act. This includes warning users, in their rules and regulations, privacy policy and user agreement, about content that violates the law; taking prompt action when informed about the presence of violative content on their platform; and providing any assistance required to government agencies when required by a lawful order to do so. Intermediaries are also required to take all reasonable measures to secure their computer resources and the information they contain, as outlined in ***Section 43A*** of the **IT (Amendment) Act** and the attendant rules; to report and share information on cybersecurity incidents with **CERT-IN**; and to ensure that technical or infrastructural modifications do not facilitate circumvention of the law. Proposed changes to the Intermediary Guidelines Rules 2011, under discussion at the time of writing, would add further obligations. Cyber cafés are subject to an additional set of rules, with their own set of requirements.

Intermediaries are also required to provide any assistance necessary to assist the government in exercising its powers to intercept, monitor, or decrypt any information through any computer resources (***Section 69*** of the **IT (Amendment) Act** and the attendant rules); to block for public access information through any computer resource (***Section 69A*** of the **IT (Amendment) Act** and the attendant rules); or to monitor and collect meta data through any computer resource for cyber security (section 69B of the **IT (Amendment) Act** and the attendant rules).

In addition, ***Section 67C*** of the **IT (Amendment) Act** requires intermediaries to preserve and retain information for the duration and in the manner prescribed by the Central Government.

66. To which extent can a legal person be held liable for actions in connection with cybercrimes?

Section 85 of the **IT (Amendment) Act** holds that where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Liability of companies is also addressed in select other provisions in the Act. For example, ***Section 43A*** provides for compensation where a body corporate fails to protect data. Section 70B specifies that body corporates who do not comply with directions issued by **CERT-IN** are punishable with imprisonment and fine.

▪ Actors

67. What bodies implement the cybercrime legislation?

The **IT (Amendment) Act** designates CERT-IN as the national agency for incident response. **CERT-IN**, the Controller of the Certifying Authorities for electronic signature certificates, and a number of government bodies and agencies can all issue directions. The Controller and adjudicating officers to be appointed by the government can investigate contraventions of the Act or specific sections of it. Appeals to orders made by the Controller or an adjudicating officer can be made to the Cyber Appellate Tribunal. Further appeals need to be made to the High Court. Although India has a growing number of cybercrime police cells, any police officer not below the rank of Inspector can investigate offences under the Act. Further, the Central Government has appointed a number of government bodies as Examiners of Electronic Evidence, to provide expert opinion on electronic evidence before any court or other authority.

68. Is there a special public prosecutor office for cybercrime? If so, how is it organised?

The **IT (Amendment) Act** does not address this question.

69. Does the cybercrime legislation create any specific body?

The **IT (Amendment) Act** establishes CERT-IN, the Controller of Certifying Authorities for electronic signatures and the Cyber Appellate Tribunal.

4. Public Order

▪ Definitions

70. How are public order, threats to public order and the protection of public order defined?

None of these terms are defined as such in Indian law.

71. Is the protection of public order grounded in constitutional norms?

The laws that apply to public order and cyberspace do not explicitly address this question.

▪ Measures

72. What cyber measures address threats to public order?

In the **IT (Amendment) Act**, public order is listed as one of the grounds on which

- the Central Government, State Governments, or any officer specifically authorised by them can issue directions for intercepting, monitoring or decrypting of any information generated, transmitted, received or stored in any computer resource (section 69);
- the Central Government or any officer specifically authorised by it can issue directions to block for public access any information generated, transmitted, received, stored or hosted in any computer resource (section 69A).
- In addition, Internet shutdowns, frequently ordered to address alleged threats to public order, are imposed under:
- ***Section 144*** of the **Criminal Procedure Code**, which grants a District Magistrate, a Sub-divisional Magistrate or any other Executive Magistrate specially empowered by the State Government in this behalf, the power to issue orders in urgent cases of nuisance or apprehended danger;
- ***Section 5(2)*** of the **Indian Telegraph Act**, 1885, which, on the occurrence of a public emergency or in the interest of public safety, allows the Central Government or a State Government or any officer specially authorised by them to direct that any message or class of messages to or from any person or class of persons or relating to any particular subject, shall not be transmitted or shall be intercepted or detained, or shall be disclosed to the government or officer making the order, if it is necessary or expedient to do so in the interests of, among other things, public order; the Temporary Suspension of Telecom Services (Public Emergency and Public Safety) Rules, 2017, notified under ***Section 7*** of the Indian Telegraph Act, which provides the Central Government with the power to make rules for the conduct of telegraphs.
- ***Section 66F*** of the **IT (Amendment) Act** provides for punishment for cyber terrorism, which is believed to have taken place, among other things, when a person knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to any restricted information, data or computer database which, there is reason to believe, may be used to cause or is likely to cause injury to, among other things, public order.

▪ Actors

73. What public authorities are responsible for the implementation of surveillance techniques?

In December 2018, the Cyber and Information Security Division of the Ministry of Home Affairs, Government of India, publicly released an order authorising ten security and intelligence agencies to intercept, monitory and decrypt information in any computer resource, a power granted by section 69

of the **IT (Amendment) Act**. These agencies are the Intelligence Bureau; the Narcotics Control Bureau; the Enforcement Directorate; the Central Board of Direct Taxes; the Directorate of Revenue Intelligence; the Central Bureau of Investigation; the National Investigation Agency; Cabinet Secretariat (RAW); the Directorate of Signal Intelligence (for service areas of Jammy & Kashmir, North-East and Assam only); and the Commissioner of Police, Delhi. A similar order has not been issued publicly for section 69A.

Internet shutdowns can be ordered under ***Section 144*** of the **Code of Criminal Procedure** by a district magistrate, a sub divisional magistrate or any other executive magistrate specially empowered by the State Government in this behalf. Where Internet shutdowns are ordered under the Temporary Suspension of Telecom Services Rules, the order can be given by the Secretary in the Ministry of Home Affairs, in the case of the Central Government, and the Secretary to the State Government in-charge of the Home Department, in the case of a State Government. In 'unavoidable circumstances', other officers who have been duly authorised to do so, can issue the order as well. Details on the agencies responsible for ordering Internet shutdowns under section 5(2) of the Indian Telegraph Act are not publicly available; the Act only notes that such an order needs to be given by the Central or a State Government or an officer authorised by them to do so.

74. What are obligations of these public authorities?

Procedural guidelines under ***Section 69*** of the **IT (Amendment) Act**, outlining a number of obligations, can be found in the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, while procedural guidelines under section 69A of the same Act can be found in the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. The Temporary Suspension of Telecom Services also provide procedural guidelines. Where orders are issued under ***Section 144*** of the **Code of Criminal Procedure** or ***Section 5(2)*** of the **Indian Telegraph Act**, the obligations of the authorities have not been detailed.

75. Can private actors be involved in the implementation of cyber measures to address threats to public order?

Where public order is concerned, intermediaries are required to provide any assistance necessary to assist the government in exercising its powers to intercept, monitor, or decrypt any information through any computer resources (***Section 69*** of the **IT (Amendment) Act** and the attendant rules) and to block for public access information through any computer resource (***Section 69A*** of the **IT (Amendment) Act** and the attendant rules).

Section 79 of the **IT (Amendment) Act** and the attendant **Intermediaries Guidelines Rules**, 2011 provide intermediaries with exemption from liability, provided that they, among other things, observe due diligence while discharging their duties under the Act. This includes taking prompt action when informed about the presence of violative content on their platform, such as content that is a threat to

public order; and providing any assistance required to government agencies when required by a lawful order to do so. Proposed changes to the Intermediary Guidelines Rules 2011, under discussion at the time of writing, would add further obligations, including on the ground of threats to public order.

Where Internet shutdowns are concerned, telecom operators are also required to comply with any orders made under ***Section 144*** of the **Criminal Code of Procedure** and under ***Section 5(2)*** of the ***Indian Telegraph Act***, as well as under the Temporary Suspension of Telecom Services Rules, in addition to the general obligations imposed on them under their license conditions.

5. Cyberdefence

▪ Scope

76. Is there a national cyberdefence strategy or is cyberdefence mentioned in the national defence strategy?

India does not have a formal national security strategy or national cyberdefence strategy.

77. What is the legal status of the national defence or cyberdefence strategy?

India does not have a formal national security strategy or national cyberdefence strategy.

78. What national laws or other normative acts regulate cyberdefence in the country?

Of primary importance to understand India's developing policy on cyberdefence is the Joint Doctrine Indian Armed Forces 2017. Other military documents that touch on the issue are the Indian Army Land Warfare Doctrine 2018, the Basic Doctrine of the Indian Airforce 2012, the Indian Maritime Security Strategy 2015 and the Indian Maritime Doctrine 2015.

The National Cybersecurity Policy, 2013, highlights the need for a Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety or security of the nation, as well as addressing the need to ensure the protection and resilience of critical information infrastructure and the need to reduce supply-chain risks. Several sections of the **IT (Amendment) Act** and of the Indian Telegraph Act are of relevance as well.

79. Is the country party of any international cooperation agreement in the sphere of cyberdefence ?

There is no publicly available information on whether India became a party to the Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organisation (SCO) when it became a full member of the SCO in 2017.

80. Does the national cyberdefence strategy provide for retaliation?

The Joint Doctrine Indian Armed Forces notes that India's national security policy 'shall entail inherent right of self-defence', among other things. Other documents of the armed forces, too, mention retaliation; the Indian Army Land Warfare Doctrine 2018 specifically mentions a mandate to retaliate in cases of information warfare.

▪ Definitions

81. How are national security and national defence defined?

The Joint Doctrine Indian Armed Forces notes that 'national security to us implies the protection, preservation and promotion of our national interests against internal and external threats and challenges. Maintenance of our national security is critical as it provides us the necessary freedom, and removes all fear and hindrance in our pursuit of prosperity and happiness. India's security is an integral component of its development process. National security and the underpinning strategies have both national and international dimensions. National Security not only entails military security but also influences our politico-diplomatic structure, water, economy, energy, food, health, education, technology, cyber, space, nuclear deterrence and environment'. The Joint Doctrine does not define 'national defence'.

82. How are cybersecurity and cyberdefence defined?

The Joint Doctrine Indian Armed Forces does not define 'cybersecurity' or 'cyberdefence '.

83. How are threats to national security and cyberthreats defined?

While not providing a definition as such, the Joint Doctrine Indian Armed Forces classifies threats into internal and external threats and challenges. The latter are further broken down into traditional and non-traditional threats. The Joint Doctrine does not provide a similar discussion of cyberthreats.

84. How is a cyberattack defined?

The Joint Doctrine Indian Armed Forces does not define 'cyberattack'.

85. Does the national law provide any other definitions instrumental to the application of cyberdefence legislation?

The Joint Doctrine discusses 'national security policy', 'national security strategy', 'armed forces doctrine', 'national power', 'military instrument of national power', and 'cyber power', as well as laying out India's national security objectives and national military objectives. The national security objectives contain explicit reference to the defence of cyberspace.

▪ National Framework

86. Is cyberdefence grounded on the constitutional provisions and/or international law?

The Joint Doctrine Indian Armed Forces takes as its starting point India's national values, aim and interests as enshrined in its Constitution.

87. Which specific national defence measures are related to cybersecurity?

The Joint Doctrine Indian Armed Forces emphasises the need for greater integration of the structures of the army, navy and air force in order for the Indian armed forces to be able to effectively address cyberthreats. In specific, it notes the launch of the Defence Communication Network (DCN), which seeks to ready the armed forces for network centric wars by enabling all stakeholders to share

situational awareness for a faster decision-making process. It also highlights the setting up of the tri-service Defence Cyber Agency, as one step towards coordination and integration of the efforts of the army, navy and air force where cyberspace is concerned. It further notes that 'cyber defence structures envisage monitoring of own cyberspace at the metadata level, real-time detection of threats in data flow, identifying types and sources of threats and responding suitably to limit and mitigate the adverse impact. The necessary crisis management plans are being incorporated to deal with the potential fallout'.

Several sections of the **IT (Amendment) Act** are of relevance as well, in particular ***Section 66F***, Punishment for cyber terrorism; ***Section 69***, Powers to issue directions for interception or monitoring or decryption of any information through any computer resource; and ***Section 69A***, Power to issue directions for blocking for public access of any information through any computer resource. Threats to the sovereignty or integrity of India, the security of the State and friendly relations with foreign states are included in the grounds on which each of these provisions can be invoked**.** ***Section 69*** and ***69A*** can also be invoked where it is necessary or expedient to do so in the name of the defence of India. ***Section 69B*** of the **IT (Amendment) Act** further allows for the monitoring and collection of traffic data for cybersecurity.

Section 5 of the **Indian Telegraph Act** allows the government to take possession of licensed telegraphs and to order that messages shall be intercepted or detained or not transmitted when there is a public emergency or in the interest of public safety, again when it is necessary or expedient to do so in the interests of, among other things, the sovereignty and integrity of India, the security of the state, or friendly relations with foreign states. A number of obligations imposed on telecom operators in their licence agreements are justified on the ground of national security as well.

88. Is there a national defence doctrine and does the law or strategy refer to it?

The Joint Doctrine Indian Armed Forces is the main national defence doctrine. As noted earlier, India does not have a formal national security strategy or national cyberdefence strategy.

89. What measures are mentioned in the national law and strategy in order to implement cyberdefence ?

See above.

90. How can Internet users' online activities be limited for the reasons of protection of national security and cyberdefence ?

As noted above, ***Section 69*** of the **IT (Amendment) Act** provides the government with the powers to issue directions for interception or monitoring or decryption of any information through any computer resource, while ***Section 69A*** of the Act provides it with the power to issue directions for blocking for public access of any information through any computer resource. Threats to the sovereignty or integrity

of India, the security of the State and friendly relations with foreign states, as well as the defence of India are included in the grounds on which each of these provisions can be invoked.

Section 5(2) of the **Indian Telegraph Act** allows the government to take possession of licensed telegraphs and to order interception of messages when there is a public emergency or in the interest of public safety, again when it is necessary or expedient to do so in the interests of, among other things, the sovereignty and integrity of India, the security of the state, or friendly relations with foreign states.

91. Does the national law or strategy foresee any special regime to be implemented in case of emergency in the context of cyberdefence ?

While a number of actors are highlighted as playing a pivotal role in the context of a national level threat, neither the relevant laws nor the Joint Doctrine Indian Armed Forces provide a specific regime to address such situations.

92. Is there any specific framework regulating threats to critical infrastructure?

Section 70 of the **IT (Amendment) Act** allows for the appropriate government to declare any computer resource which directly or indirectly affects the facility of critical information infrastructure to be a protected system. ***Section 70A*** of the **Act** provides for the Central Government to designate any organisation of the Government as the national nodal agency for the protection of critical information infrastructure.

▪ Actors

93. What actors are explicitly mentioned as playing a role regarding cyberdefence in the law or national cyber defence strategy or defence strategy?

The Joint Doctrine Indian Armed Forces mentions the Defence Cyber Agency, the Defence Information Assurance and Research Agency, the National Security Council Secretariat and the National Cyber Coordination Centre under the Ministry of Communications and Information Technology.

In addition, in 2014, the Government of India designated the National Critical Information Infrastructure Protection Centre (NCIIPC) as the national nodal agency for critical information infrastructure protection, as per the powers vested in it under section ***70A*** of the **IT (Amendment) Act.**

94. Is there a specific cyber defence body?

The Defence Cyber Agency, mentioned in the Joint Doctrine Indian Armed Forces, and the NCIIPC, designated the national nodal agency for critical information infrastructure protection under ***Section 70A*** of the **IT (Amendment) Act** in 2014, are bodies that are specifically concerned with cyber defence or aspects of it.

95. What are the tasks of aforementioned actors?

The NCIIPC is responsible for all measures relating to critical information infrastructure, including research and development. Further details on its tasks can be found in the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013, that designated the NCIIPC as the national nodal agency for critical information infrastructure protection.

Little information is publicly available on the mandate and tasks of other actors. Formally established in 2019, the exact mandate of the Defence Cyber Agency has not been made public. The Joint Doctrine Indian Armed Forces describes it as a tri-service advice mechanism, but media reports indicate that its mandate may go beyond that. The Joint Doctrine also describes the Defence Information Assurance and Research Agency as the nodal agency mandated in dealing with all cyber security needs of the Tri-Services and the Ministry of Defence. Media reports indicate that the Agency might have been incorporated in the Defence Cyber Agency. Also according to the Joint Doctrine, the efforts at cyberdefence undertaken by various stakeholders are synchronised by the National Security Council Secretariat (NSCS) through the National Cyber Coordination Centre (NCCC) under the Ministry of Communications and Information Technology. The NSCS is a specialised unit in the Prime Minister's Office under the direct charge of the National Security Advisor and headed by the Deputy National Security Advisor. The NCCC, according to the Joint Doctrine, is entrusted with the responsibility of coordination, identification and mitigation of cyber risks, threats and vulnerabilities. In media reports it has been described as a cybersecurity and e-surveillance.

5. Cybersecurity Policies in China

Min Jiang

5.1. Cybersecurity in China: An Introduction[285]

Cybersecurity is a hotly debated concept worldwide with various policy dimensions. It is often associated with cybercrime[286], cyberwar and cyberdefence [287], and increasingly with personal data protection[288]. A series of crises, in particular, has led to growing public debate over cybersecurity, safety of digital technology and online privacy: Snowden's 2013 revelation of NSA's massive surveillance programs; the colossal failure of US tech giants such as Facebook, Twitter and Google in the Russian interference of the 2016 US president election; and the massive Equifax data breach in 2017 affecting nearly 150 million consumers. Drawing from recent works[289] theorizing cybersecurity as data protection, securing financial interest, protecting public and political infrastructures, and control of information flows, the CyberBRICS Project focuses on personal data protection, consumer protection, cybercrime, public order and cyberdefence .

China's cybersecurity policies constitute an important component of global and BRICS cybersecurity discussions in our current geopolitical environment. China's rise against America's relative decline has not only presented China and its Internet as an alternative to the Western model of economic and technological development, but has also fuelled the great power rivalry between China and the U.S. especially in trade and technology. The US-China conflict is also taking place at a time when waves of populism are sweeping through the world including "BRICS" countries, eager to assert sovereignty at home and abroad. As Internet economies and cyber policymaking increasingly gravitate towards the three main models set by the US, China and EU, Chinese cybersecurity policies remain central to global and BRICS cyber policy debates and research.

China started to adopt the Internet in 1994 and connectivity grew exponentially over the last 25 years to 854 million Internet users, over 847 million mobile Internet users[290] and a relatively independent ecosystem composed of many world-class Internet firms like Huawei, ZTE, Alibaba, Tencent, Baidu, and TikTok. Following the precipitous NSA episode, China's cybersecurity approach has visibly evolved from a "whole-of-government" and "whole-of-nation" approach to one that is "whole-of-systems" that advocates a systematic formula characterizing cybersecurity as holistic rather than

[285] The author thanks Dr. Luca Belli and Ms. Mei Nelson for their feedback and acknowledges graduate students Faith Klatt and Brianna Morrison's library research support that contributed to this chapter.

[286] See Bauer & Eeten (2009); Goodman (2015).

[287] See Kaplan (2017); Singer & Friedman (2014).

[288] See Raul (2018).

[289] See Fichtner (2019).

[290] See Cyber Administration of China (2019).

fragmented, dynamic rather than static, open rather than closed, relative rather than absolute, common rather than isolated[291].

Guided by an overarching framework of cyber sovereignty[292], China has made several important institutional, legislative and developmental adjustments. First, the Chinese government consolidated cyber policy decision-making previously distributed amongst various ministries now back to a central regulator, the Cyberspace Administration of China (CAC). As the official Internet regulator providing oversight, the CAC is answerable to the Central Cyberspace Affairs Comission, an inter-ministerial government agency, headed by President Xi and composed of Chinese Leaders at the highest level. Created in 2014, CAC has also established 31 provincial-level offices, largely associated with propaganda and content control[293], with growing cybersecurity oversight. Second, a canopy of cyber laws and policies have been drafted and passed at various levels in the last few years to both address internal needs[294] and respond to external geopolitical and policy trends including the NSA scandal and EU's introduction of the General Data Protection Regulation (GDPR) in 2018. Among the newly introduced laws and policies, the most eminent is the *Cybersecurity Law of the PRC* that went into effect in 2017 to serve as the foundation of China's cybersecurity policyaking. Third, the Chinese government issued several large-scale industrial policies to boost the country's technological capacities: the "Made in China 2025" plan to turn China from the world's "factory" of cheap goods to a nation that produces higher value products and services; the "Internet Plus" plan unveiled in 2015 to upgrade the nation's traditional industries from agriculture to manufacturing; and the "Digital Silk Road" adopted as part of the larger "Belt & Road Initiative" in 2015 to seek new technological markets around the world that involves Internet infrastructure upgrades, common technology standards, and improvement in policing systems[295].

In 2014, the Chinese president famously remarked: "Without cybersecurity, there is no national security"[296]. It is important to note that the Chinese state's understanding of cybersecurity is much broader than the traditional foci on cybercrime, cyberwar, and protection of critical infrastructures. Rather, cybersecurity and "information security"[297] are seen as intertwined, critical for maintaining the viability of the Chinese society, nation and the Chinese Communist Party[298]. For Chinese authorities, cybersecurity is thus first and foremost grounded in "internal security" that has

[291] See Austin (2018, pp.5-6).

[292] See Jiang (2010).

[293] See Alsabah (2016).

[294] See this book's China Country Report.

[295] See Hong (2017).

[296] See Xinhua Net (2015).

[297] See CAC (2017).

[298] See Schia & Gjesvik (2017).

historically placed a heavy emphasis on "content security" and led to measures ranging from the Great Firewall of China to the employment of human censors to monitor and remove online content the Party deems "harmful"[299]. Such close and extensive political supervision has a profound impact on virtually every facet of China's social and political life including regimes of security and cybersecurity.

The CyberBRICS Project's framework encompassing data protection, cyberdefence , cybercrime, consumer protection, and public order captures the multi-faceted phenomenon of cybersecurity that are of relevance and importance to China as it strives to become a cyber superpower.

5.2. Data Protection

While as early as 2012 China's National Congress had passed the *Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks* to provide in principle the legal framework for personal data protection, EU's movement towards GDPR nudged China to establish more robust personal data protection policies. Previously, China had also been observing APEC's development of Cross Border Privacy Rules (CBPR) that attempts to regulate transnational data flow and trade within an APEC framework[300]. However, it became clear to Chinese policymakers that the US-dominated CBPR framework, which mandates lower levels of personal data protection for cross-border data among participating APEC countries, favours the extraction and circulation of personal data – notably by tech giants in Silicon Valley – instead of empowering data subjects in other APEC countries[301]. In the last few years, China has forged its own path towards personal data protection.

Various Chinese governmental agencies have passed laws or issued policies on personal data protection ranging from national laws, judicial interpretations to administrative regulations and industry standards. Among them, Article 111 of the *General Rules of the Civil Law of the PRC* (2017) provides language to broadly protect personal information. China's *Criminal Law* also adopted several amendments in 2005, 2009 and 2015 to reflect increasing criminal activities involving personal information. The *Cybersecurity Law of PRC* (2017) similarly has a few provisions to regulate the collection, storage, transmission and use of "personal information" by network operators and critical information infrastructure operators.

Personal Information Security Specification (GB/T 35273-2017), issued in 2017, provides the most detailed interpretations of China's personal data policies to date and is widely considered the most comprehensive regulatory standard in China, including many elements similar to provisions found in GDPR. A new draft of the *Specification* is currently under consideration. *Personal Information Security*

[299] See Austin (2018).

[300] See Callo-Muller (2018).

[301] See Hong (2018).

Specification (2017), known as "China's GDPR"[302], is a technical standard, the compliance with which is voluntary, not mandatory. Scholars in China, hence, have characterized the *Specification* (2017) as a "soft law" which lacks legal authority but carries administrative effectiveness to regulate individual and organizational behaviours[303]. The *Specification* includes some innovative elements, such as the "Privacy Policy Template" that provides concrete guidance for organizations to meet data protection standards through their terms of service. However, its "soft law" status means that in terms of enforcement, administrative agencies cannot levy legally binding punishments according to the *Specification*, but can resort to non-compulsory measures such as warnings to provide guidance or rewards for exemplary practice[304]. While the *Specification* allows for flexibility, its lack of legal authority is also its Achilles' Heel, prompting some Chinese scholars[305] to argue that China needs to adopt a formal law for protecting personal information.

In the coming years, China is likely to combine technical standards such as the *Specification* (2017) with national laws in personal data regulation. In 2019, CAC issued a draft of *Data Security Administrative Measures* (2019) to regulate the collection, storage, transmission, processing and use of personal data in Chinese territories. Once formally approved, the *Measures* will be legally binding and carry more enforcement power than the *Specification*. However, while the *Measures* in development is largely consistent with the *Specification* (2017), it lacks the details of the *Specification* (2017) regarding the specific provisions for personal information collection, storage, and use, thus undercutting the regulatory power of the *Measures* in protecting personal information.

In terms of cross-border transfer, a draft of *Measures on Security Assessment of the Cross-border Transfer of Personal Information* was released in June 2019. Both GDPR and China's approach have "extraterritorial" features. GDPR is applied to all EU citizens, data processors/controllers established in EU or the processing of information pertaining to EU citizens beyond EU borders. While China's *Cybersecurity Law* (2017) is largely "territorial" by restricting its application to the PRC territory, *Measures on Security Assessment of the Cross-border Transfer of Personal Information* (2019) drafted by the CAC also applies to foreign operators gathering information from Chinese "domestic users" online. Particularly, the CAC requires foreign operators to "fulfill the responsibilities and obligations of network operators in these *Measures* through a legal representative or entity within the territory," which is an attempt of "reterritorialization". While the feasibility of China's cross-border personal data transfer measures, especially for small foreign businesses, is unclear, the likely intent of the Chinese government here seems to be for larger foreign businesses regularly transacting

[302] See Wang (2018).

[303] See Xu (2019).

[304] See Xu (2019).

[305] See Liu & Lin (2018).

Chinese user data to comply. Additionally, *Cybersecurity Law* (2017) requires data localization for "critical information infrastructure operators," domestic or foreign.

In terms of user rights, China's *Specification* (2017) in principle, like GDPR, outlines the rights of data subjects, specifies the obligations for data controllers, and endorses the principles of data security, user consent, minimization of data collection, data anonymization and other protective measures. Also, similar to GDPR, China's *Specification* (2017) guarantees a range of rights for data subjects such as data erasure, data rectification, data portability, explicit consent, withdrawal of consent and account cancellation[306]. However, the rights provided under China's *Specification* (2017) are more limited in type and scope[307]. For instance, the *Specification* (2017) does not include the right to access or the right to object. Further, regarding the right to data erasure or "the right to be forgotten," GDPR presents six types of situations user requests can be granted. Under China's *Cybersecurity Law* (2017) and *Specification* (2017), erasure occurs only when information controllers when illegally use personal data against user agreement. In addition, GDPR provides a general right to data portability, whereas China's *Specification* (2017) only allows it for portability of basic individual information as well as individuals' health, psychological, education, and work information.

In terms of core concepts, compared to GDPR, the *Specification* (2017) uses "personal information" instead of "personal data," both referring to data that on its own or in combination with other information can identify a natural person. Additionally, whereas GDPR defines "sensitive data" as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic and biometric data, as well as health data and data concerning a person's sex life or sexual orientation, China's *Specification* (2017) defines "sensitive data" more broadly as "any information which, if unlawfully disclosed, may endanger a person's physical and mental wellbeing, their reputation and/or their property and/or lead to discrimination." In terms of consent, the *Specification* (2017) is arguably stricter and more prescriptive specifying "explicit consent" as personal data subject making voluntary declarations (electronically or in written). In terms of economic sanctions, GDPR carries stiffer penalties than its Chinese counterpart: data controllers and processors, under GDPR, can be fined up to 20,000,000 EUR or 4% of total worldwide annual revenue; in the Chinese *Cybersecurity Law* (2017), the highest penalty is 500,000 RMB (approximately $71,000 USD).

5.3. Consumer Protection

Consumer protection laws view online users as consumers, economic agents who engage in transactions in need of fair treatment and protection from economic fraud and harm inflicted by often more powerful corporations. The rapid growth of the digital economy which now renders the value of

[306] See Wang (2018).

[307] See Liu & Lin (2018).

our data more valuable than oil[308] makes electronic transactions within and beyond a country's physical borders all the more crucial and the protection of consumer rights and interests all the more urgent. In 2019, for instance, China's e-commerce exceeds 35% of the country's retail sales with a market size expected to reach USD $5.6 trillion, 100 billion more than that of the U.S[309]. Meanwhile, in 2018 alone, Chinese market supervision authorities reportedly received over 11 million consumer complaints and consultation requests[310]. How to better regulate the online market and provide protection for consumers presents a serious challenge in policy and practice.

In China, several laws provide legal protection for consumers. First, the *Law of the PRC on the Protection of the Rights and Interests of Consumers* ("*Consumer Protection Law"* hereafter) went into effect in 1994. Shortly after, *Advertising Law of the PRC* was passed in 1995. These laws were clearly enacted to help regulate a fast-growing consumer market and economy in China after the country adopted reform and opening-up policies in the late 1970s. Since then, the *Consumer Protection Law* has been amended twice, in 2009 and 2013 respectively. The *Advertising Law* was updated in 2015. Shortly after, a new *E-commerce Law* went into effect in 2018 to regulate e-commerce activities and extend the protection of consumer rights and interests within Chinese territories[311].

In addition, the Chinese Supreme People's Court has been compiling and publishing since 2014 prominent cases, usually eight to ten a year, to expose malpractices and raise awareness for the protection of consumer rights. Institutionally, the State Council[312] also approved in 2016 to establish the Inter-Ministerial Joint Meeting System for the protection of consumer rights and interests. The joint conference led by the State Administration for Industry and Commerce (SAIC) is composed of 22 ministries and departments including SAIC, the National Development and Reform Commission, the General Administration of Quality Supervision, China Food and Drug Administration, and China Consumers Association. Overall, the system is meant to "better protect the legal rights of consumers, and fully play the guiding role of consumption for economic development"[313].

The *Consumer Protection Law* (1994) is the core legal document in consumer rights protection in China. It lays out the principles of consumer rights, including the rights to safety, choice, truthful information, fair treatment, rights to form social organizations, fair compensations and so on. Acknowledging the increasing frequency of online transactions, the 2013 amendment to the *Consumer Protection Law* provides general guidelines to extend consumer protection to Internet

[308] See Economist (2017).

[309] See eMarketer (2019).

[310] See Sina Financial (2019).

[311] See Xue (2019).

[312] The State Council is the chief administrative authority in China, chaired by the Premier. It also includes the heads of the cabinet-level executive departments and directly oversees the provincial-level governments.

[313] See State Council (2016).

transactions (Articles 25 and 28), strengthens regulation of business operators' responsibilities (Chapter III), and enhances legal assistance to consumers in civil litigations (Article 35). Particularly, the new law stipulates legal protection of personal information (Article 14), requires business operators to explicitly state the purpose, method, scope of collection or use of information and obtain consumer consent (Article 29), requests businesses to keep consumer information strictly confidential, and forbids them to disclose, sell, or illegally provide such information to others without consent (Article 29). Companies are also expected to remedy data loss. Violations can result in a fine of up to RMB 500,000 (approximately USD $71,000). Serious violations can lead to business license suspension or revocation of business license and other criminal liabilities.

The revised *Advertising Law* (2015) includes regulations for online advertising that broadly relate to consumer protection. The law defines Internet advertising, lays down rules for online ads publishers, and outlines investigation measures and penalties for violators. Under the new law, online ads include: product promotion via text, pictures, videos, links; email ads; paid search ads; ads within commercial presentations. The broad scope subjects a wide spectrum of advertisements under consumer scrutiny. Ads publishers include those displaying or submitting online ads and those verifying or moderating submitted ads for publishing. This effectively subjects platform operators to the new *Advertising Law*. In addition, approval is legally required for certain products and services to be advertised online including medicine, medical treatments and devices, foods for special medical purposes, dietary supplements, veterinary drugs and pesticides. The new law also requires pop-up ads to be closed in one-click, prevents advertisers to send emails to consumers without permission, and mandates email advertisements to include opt-out links. Accordingly, platform operators are responsible for monitoring third-party ads on their platforms, subject to the same or steeper penalties that advertisers face in cases of violation. Ads are required to be clearly labelled for users to differentiate between advertising and regular content. Similarly, search engines are required to differentiate between paid and organic search results. The law requires platform operator to verify the advertiser's identity and remove illegal ads where advertiser qualifications and ad content are expected to be verified by an ads review team.

Finally, the new *E-commerce Law* (2018) extends the protection of consumer rights and interests to e-commerce activities in China. The law defines three major types of e-commerce operators: e-commerce platform operators (e.g. Alibaba), operators on platform (e.g. third-party merchants operating an online store on Taobao) and online sellers (e.g. independent seller operating their own website or app). Under this new law, regulation extends to many non-traditional channels for e-commerce activities including social media apps like WeChat and TikTok. In addition to the usual protection afforded to consumers in terms of safety of products, services and information, the new law enforces a number of novel consumer rights in the e-commerce domain. For instance, in addition to search results of products and services based on consumer characteristics, platform operators are also

required to present research results *not* based on such characteristics to prevent data and pricing discrimination (Article 18). Second, platforms are forbidden to bundle goods or services by default but can do so as an option (Article 19). Third, "advertised" products or services must be clearly labeled in search results displays (Article 40). Fourth, platforms are forbidden to remove reviews by consumers (Article 39). In addition, e-commerce platforms are required to protect IP rights and can face fines of up to 2 million RMB (or 280,000 USD).

5.4. Cybercrime

With the largest number of Internet users in the world[314], China faces increasing challenges presented by cybercrime. It is reported that 1/3 of crimes in China are cybercrimes with an annual growth rate of 30%[315] and a loss of RMB 95 billion per year[316]. In 2016, Qihoo, a Chinese Internet security company, reported 70,000 mobile phone extortion attempts, 197 million intercepted phishing attacks, 20,000 reported monetary loss, and security vulnerabilities in 99.99% of Android phones in China[317]. This makes cybercrime the most prevalent type of crimes in China. Not only does cybercrime straddle both virtual space and real space, but it is also becoming increasingly cross-border demanding international cooperation.

The regulation of cybercrime in China follows a series of laws and policies. The most important national law is *Criminal Law* (1997), which over the years has added two amendments – VII (2009) and IX (2015) – to reflect the evolving nature of cybercrime. *Cybersecurity Law of the PRC* (2017) also contains cybercrime provisions similar to those found in the *Criminal Law*. *Anti-Terrorism Law of the PRC* (2015) has specific regulations for Internet service providers to remove and report terrorist online content. Several judicial interpretations and supreme court opinions have expanded on cyber extensions of crimes already outlawed by China's *Criminal Law* such as online pornography (2010), online gambling (2010), online defamation (2013), criminal procedures in cybercrime cases (2014), and infringement on personal information (2017). The Ministry of Public Security, additionally, also issued related regulations including *Regulations on Internet Security Supervision and Inspection by Public Security Organs* (2018) and *Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases* (2019).

The most prevalent types of cybercrimes in China are: 1) online financial fraud; 2) attacks on online ecosystem such as DDoS attacks, Internet ransom, online traffic/SEO fraud; and 3) extensions of offline crimes such as online pornography and gambling[318]. Accordingly, legislation targeting cybercrime in

[314] See CAC (2019).

[315] See Xinhua Net (2017).

[316] See Xinhua Net (2018).

[317] See Austin (2018).

[318] See Tencent (2016).

China has tried to keep pace. As early as 1997, Articles 285, 286 and 287 of the *Criminal Law* in China recognized several types of cybercrimes that: 1) illegally access computer systems to interfere with state affairs, defence, and cutting-edge technology areas; 2) delete, modify memory, data transmission and programs in computer systems resulting in damage; 3) disable or destroy computer systems; and 4) intentionally create and disseminate computer virus resulting in damage. Amendments VII (2009) and IX (2015) of the *Criminal Law* included more Internet-enabled and Internet-facilitated crimes with provisions targeting: 5) online financial fraud, theft, corruption, embezzlement of public funds, and stealing state secrets; 6) creation of websites or online groups to commit fraud, teach methods of committing crimes, make and sell goods forbidden by law; 7) distribution of information about making or selling illegal drugs, guns, pornography and other prohibited products; and 8) being an accomplice to computer crimes resulting in serious damage.

Notably, in 2015, Amendment IX to the *Criminal Law* criminalized "online rumour." Article 291-1 of the *Criminal Law* stipulates that individuals, who fabricate or deliberately spread, on the Internet or other media, false information regarding dangerous situations, epidemics, disasters or police emergencies, which seriously disturb social order, can face up to 3 years of criminal detention or surveillance, and in serious situations, may be sentenced to 3-7 years in prison. While some rumours are fabricated, driven by profit, attention, or revenge that can cause individual or social harm[319], others are earnest social and political inquiries that can be labeled by authorities as "rumours" to prevent potential social discontent and instability. Previously, netizens who questioned official statistics or narratives during SARS in 2003, Sichuan Earthquake of 2008, and the Tianjin chemical blast in 2015 were detained in the name of preventing "rumours"[320].

Amendment IX to the *Criminal Law* in 2015 also asks network service providers to assume intermediary liability for controlling information the government deems illegal. Specifically, Article 286-1 states that service providers failing to perform security management obligations or refusing to make corrections ordered by regulatory authority can face up to 3-year imprisonment, criminal detention or surveillance in addition to a fine when their services cause the spread of a large amount of "illegal information"; leakage of users' information and the loss of criminal case evidence with serious consequences. The *Cybersecurity Law* (2017) also contains several provisions targeting critical information infrastructure operators for violating specific obligations and duties such as data localization governing "personal information" and "important data"[321]. Noncompliance can result in punishable fines of up to 500,000 RMB (or $71,000 USD) and imprisonment of up to 5 years in serious cases. Such provisions pose

[319] See Ji (2014).

[320] See Jenkins (2015).

[321] "Important data," according to a draft of the *Data Security Administrative Measures* of the PRC under consideration, refers to "the data that might directly affect national security, economic security, social stability and public health and security in case of disclosure, such as non-public government information, population data covering a large area, gene health data, geographic data and mining data." In practice, authorities have discretion in interpreting what important data is.

considerable intermediary liability on network operators, producing a chilling effect. In effect, the *Cybersecurity Law* has expanded the definition of cybercrime from crimes that target or utilize computers or networks to managerial negligence by network operators.

In the international arena, China has advocated for an UN-led anti-cybercrime framework on the one hand, and built a regional alliance with like-minded countries on the other. Although China is often seen as a perpetrator of cyberattacks and espionage[322], it is also on the receiving end of foreign cyberattacks, suffering from considerable vulnerability[323]. While China is not a member or observer of the Budapest Convention (or Convention on Cybercrime), it is a signee of the World Intellectual Property Organization Copyright Treaty (WIPO Copyright Treaty) of 1985 and the U.N. Convention Against Transnational Organized Crime of 2000. Since 2012, China became a member state of the Shanghai Cooperation Organization (SCO) and participates in efforts to fight against terrorism, separatism, extremism, and international cybercrime. Along with other member states Russia, Kyrgyzstan, Kazakhstan, Tajikistan, and Uzbekistan, China wants to further conduct cybersecurity exercises within the SCO framework[324].

5.5. Public Order

As noted earlier, the Chinese state's approach to cybersecurity is grounded in "information security" and social stability. For Chinese authorities, public order in cyberspace is intricately connected to public order in physical space. Instead of viewing the Internet as a freewheeling space for expression and association that is inherently emancipatory, the Chinese government treated the Internet from the very beginning with fear, caution and a determination to reconfigure and regulate the Web to its liking. These words from Wu Jichuan, the then-Minister of Posts and Telecommunications, in 1995 were telling[325]:

> "By linking with the Internet, we don't mean absolute freedom of information. I think there is a general understanding about this. If you go through customs, you have to show your passport. It's the same with management of information. There is no contradiction at all between the development of telecommunications infrastructure and the exercise of state sovereignty".

Given the authorities' ultimate concern for regime stability, the state adopted countless policies to ensure "information security." As early as 1997, *Measures for Security Protection Administration of the International Networking of Computer Information Networks* was issued by the Ministry of Public Security (approved by the State Council) to safeguard Internet security. Article 5 of the *Measures*

[322] See Lindsay, Cheung & Reveron (2015).

[323] See CNCERT (2019).

[324] See Sputnik International (2018).

[325] See Goldsmith & Wu (2006, p.467).

specifically forbids individuals to use the Internet to create, replicate, retrieve, or transmit information which "fabricates or distorts the truth, spreads rumours, and disturb public order". Over time, the state has developed an expansive content management system to police online content, supervised by propaganda department and outsourced to Internet companies.

The protection of public order is also recognized in the Chinese *Constitution*. Article 28 of the Chinese *Constitution* states: "The state maintains public order and suppresses treasonable and other counter-revolutionary activities; it penalizes criminal activities that endanger public security and disrupt the socialist economy as well as other criminal activities; and it punishes and reforms criminals". The latest *Cybersecurity Law* (2017) spells out in detail the importance of maintaining "public order":

> "Any person and organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they must not endanger cybersecurity, and must not use the Internet to engage in activities endangering national security, national honour, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts" (article 12).

The desire to maintain public order has also led the state to pass the *Emergency Response Law of the PRC* (2006) that covers a wide range of emergencies including natural disasters, accidental disasters, public health incidents and social safety incidents. A national emergency monitoring and reporting system has been set up to anticipate and prepare for such emergencies. Further, the *Cybersecurity Law* has mandated the establishment of an emergency monitoring and response information communication system[326]. In extreme circumstances, Article 58 of the *Cybersecurity Law* allows for shutting down the Internet in an area for the sake of protecting "national security and the social public order":

> "To fulfil the need to protect national security and the social public order, and to respond to the requirements of major security incidents within the society, it is possible, as stipulated or approved by the State Council, to take temporary measures regarding network communications in a specially designated region, such as limiting such communications" (article 58).

To ensure public order, the Chinese state has put considerable resources into cyber policing, including high-tech surveillance programs like the social credit system. Between 2015 and 2017, the Ministry

[326] See Chapter V of the Cybersecurity Law.

of Public Security quickly established 1,116 cybersecurity police units, including "level one" units within major Chinese Internet companies such as Baidu, Tencent and Sina[327]. While these Internet firms are mainly tasked to police political content, their capacity has expanded to supply criminal intelligence as well[328]. Policy-wise, the *Cybersecurity Law* mandates real-name registration policy and self-regulation by network operators. The *Regulations on Internet Security Supervision and Inspection by Public Security Organs* (2018), issued by the Ministry of Public Security, also give police forces considerable latitude to inspect network operators, Internet service providers and organizational users to prevent crime and establish order.

Meanwhile, advanced technologies such as artificial intelligence, facial recognition have been increasingly integrated into China's policing system, bringing the country closer and closer to a surveillance state. China now boasts a giant facial recognition database that uses artificial intelligence to identify citizens within seconds[329], 200 million private and public surveillance cameras which are expected to grow to 300 million by 2020[330], and 500-megapixel facial recognition cameras that can spot individuals from crowds of tens of thousands[331]. Finally, China's now-notorious Social Credit System, constructed partly to boost trust and reduce fraud, is widely seen as a massive national surveillance data infrastructure expected to monitor and rate the trustworthiness of citizens, firms, and organizations[332]. In 2019, a bill has been proposed to link the Social Credit System to users' online expressions[333], a move seen by many to further curtail public speech.

5.6. Cyberdefence

The issues surrounding cyberspace and cybersecurity are not only technical and socio-political in nature, but also international in scope, impacting power relations and conflict resolutions between countries. A world dominated by non-Western authoritarian states and a loss of confidence in traditional liberal democracies is conflict-prone[334]. Ubiquitous Internet connection and annihilation of distance on a global scale also present vulnerabilities for exploitations. Former NSA Senior Counsel Joel Brenner was quoted in a Pew cyberattacks report stating: "The Internet was not built for security, yet we have made it the backbone of virtually all private sector and government operations"[335]. Judging

[327] See Wang (2017).

[328] See Austin (2018).

[329] See Chen (2017).

[330] See Mozur (2018).

[331] See Hayward (2019).

[332] See Liang et al (2018).

[333] See Cyber Administration of China (2019).

[334] See Demchak (2016).

[335] See Raine, Anderson & Connolly (2014).

by the NSA/Snowden Affair and Russia's alleged interference in the U.S. 2016 election, the U.S. is both a beneficiary and a victim of such network vulnerabilities. As cyberspace becomes increasingly re-nationalized and militarized in the current geopolitical climate[336], cyberdefence has moved beyond the confines of government and academic discussions and entered public discourse.

Like the U.S., China is on both the sending and receiving ends of international cyberattacks. On the one hand, the high-profile U.S. Justice Department's indictment of five Chinese military officers for hacking and economic espionage in 2014 spotlighted China's cyber-espionage capabilities and will[337] that goes back to the Titan Rain cyberattacks in 2003 and 2005[338]. On the other hand, China considers itself a vulnerable target overshadowed by American dominance in information technologies and military offense/defence capacities[339]. A report released by the *National Computer Network Emergency Response Technical Team/Coordination Centre of China*[340] cited America, Canada and Russia as the primary sources of malicious cyberattacks on Chinese targets at 63%, 17% and 2% respectively. The same report states 14,752 Trojan or botnet-infected servers located in the U.S. controlled 3.34 million host computers inside China in 2018, an increase of 90.8% from 2017. Sounding the alarm that the U.S. may be preparing for a large-scale "cyberwar" against China, Qin An, Director of the Beijing-based Institute of China Cyberspace Strategy, argues China should brace for such eventualities[341].

On the policy front, the current Chinese administration has issued several national laws and strategies to strengthen China's cyberdefence capabilities. *National Security Law of the PRC* (2015) provides a broad framework for national security and cybersecurity. Article 25 of the *National Security Law* positions network and information security as an important component of national security; places emphasis on scientific development, innovation, and national control over core information technologies, critical infrastructures, important information systems and data; sets goals to prevent, stop and manage cyberattacks, intrusions, theft, online distribution of harmful information; and ultimately hopes to achieve cyberspace security and sovereignty.

In terms of the cyber strategies released by the Cyberspace Administration of China (CAC), *International Strategy of Cooperation on Cyberspace* (2016) stands out as China tries to take the lead on international cyber governance and propagate President Xi's call to "establish a community of shared future in cyberspace." Specifically, it outlines the principles of peace, sovereignty, shared governance and shared benefits and explicitly states: "Countries should reject the Cold War mentality,

336 See Inkster (2016).

337 See U.S. Department of Justice (2014).

338 See Oppermann (2010)

339 See Qin (2019B).

340 See CNCERT (2019).

341 See Global Times (2019).

zero-sum game and double standards, uphold peace through cooperation..." and "The tendency of militarization and deterrence build-up in cyberspace is not conducive to international security and strategic mutual trust." With these international strategies, it appears China wishes to establish a global Internet governance framework based on "state sovereignty".

Two important white papers on Chinese defence strategies—*China's Military Strategy* (2015) and *China's National Defence in the New Era* (2019)—provide more details of China's cyber military strategies. Specifically, *China's Military Strategy* (2015) frames information war as the next frontier of international warfare, and emphasizes the need for the Chinese military to respond to international trends to make military equipment more "precise, intelligent, stealthy, and unmanned." Citing China as one of the most affected victims of hacking and cyberattacks, the paper notes China's deficiencies in cybersecurity and urgent need to protect critical infrastructures.

The newly released 2019 white paper *China's National Defence in the New Era* assesses the current national and international security situations and outlines China's defence missions, reforms, and spending. Painting the U.S. as the ultimate cyberspace hegemon, the paper states the Chinese military needs to adapt to the "new era" of strategic competition by strengthening its preparedness and improve its combat capabilities to match China's global standing while preserving "world peace." In terms of cyberdefence , the white paper makes it clear that China is interested in applying cutting-edge technologies to the military domain including artificial intelligence, big data, cloud computing, quantum computing, and the Internet of Things (IoT). Notably, the white paper also introduces a key innovation in the structuring of its military forces: a new People's Liberation Army (PLA) unit — the Strategic Support Force (SSF) — was created to consolidate the military's strategic space, electronic, and cyber warfare missions into the PLA's joint operations system.

The growing US-China trade war and tech war have heightened the tensions between the two countries and a sense of cyber insecurity in China. In April 2019, Russia introduced a "sovereign internet" bill to prepare itself to be cut off from the rest of the Internet[342]. Two months later, China also created six mirror copies of root name servers to "offer the country more backups in an Internet breakdown led by the US[343]". A cold war mentality in this geopolitical climate has led China to implement several national cybersecurity and cyberdefence strategies in the last few years. First, recognizing the country's cybersecurity industry is particularly weak[344], the Chinese government actively promotes and invests in the growth of its network security market[345]. Second, the government advocates the strategy of "military-civilian fusion" to strengthen the synergy between the military and civilian sphere[346]. The Chinese military essentially could

[342] See AFP (2019).

[343] See Cao & Leng (2019).

[344] See Austin (2018).

[345] See Cao & Leng (2019).

[346] See Qin (2019A).

benefit from technological advances in many areas including cloud computing, robotics, aviation, nuclear technology and so on[347]. Third, state-level cyberdefence exercise is also seen as a necessity for cyberdefence preparedness. Through the Shanghai Cooperation Organization (SCO), China has been conducting exercises to ready itself for external cyberterrorism and cyberattacks.

5.7. Conclusion

Cybersecurity is an increasingly challenging issue for many countries as the world now is highly cyber-connected in commercial, political, civil society and military affairs. This chapter provides an overview of the Chinese government's latest cybersecurity policies in the areas of personal data protection, consumer protection, cybercrime, public order and cyberdefence . It is evident that while China, on the one hand, has strengthened its policies in personal data protection and consumer protection, it has also put significant emphasis on and resources into cybercrime, maintenance of public order and cyberdefence , the latter far outpacing the former. That China has the world's largest internal surveillance infrastructure[348], still growing, is at odds with its own posture to provide more privacy and personal data protection.

Overall, China, the world's second-largest economy, is both cyber-ambitious and cyber-vulnerable[349]. Against all odds, China has managed to build in the last two decades the only cyber ecosystem that can arguably compete against the U.S. While America often points to China for cyber theft and cyber intrusion, it is also undeniable that the U.S. is the most technologically advanced country with an unmatched military capacity and a proven record of exploiting network vulnerability on a global scale[350]. The ongoing US-China trade and technology wars are fuelling an international environment that is more combative than cooperative, and conflict-prone. In a world of increasing volatility, the call to "cyber sovereignty" by nations like China, Russia, and India[351] expresses valid concerns, but in an interconnected world, cooperation based on mutual interests and user-centric values should be identified to solve the myriad urgent cybersecurity problems facing individuals, organizations and societies.

5.8. References

AFP. (April 11, 2019). Russia passes bill to allow Internet to be cut off from foreign servers. The Guardian. Available at <https://is.gd/hOduIB>. Accessed 04 November 2019.

[347] See Ford (2019).

[348] See Austin (2018).

[349] See Austin (2018); Lindsay (2014).

[350] See Lindsay et al. (2015).

[351] See Jiang (2010); Kovacs (2016).

Alsabah, N. (2016). Information control 2.0: The cyberspace administration of China tames the internet. Merics China Monitor. Available at <https://is.gd/QkblLb>. Accessed 04 November 2019.

Austin, G. (2018). Cybersecurity in China: The next wave. Cham: Springer.

Bandurski, D. (2017). Xi Jinping's web of laws. China Media Project. Available at <https://is.gd/c6Ck2N>. Accessed 04 November 2019.

Bauer, J. & Eeten, M. (2009), Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommunications Policy, 33(10–11), 706-719.

Callo-Muller, M. (2018). GDPR and CBPR: Reconciling personal data protection and trade. APEC. Available at <https://is.gd/wYvtUP>. Accessed 04 November 2019.

Cao, S. & Leng, S. (September 16, 2019). Cybersecurity week kicks off in China. Global Times. Available at <http://www.globaltimes.cn/content/1164607.shtml>. Accessed 04 November 2019.

Chen, S. (October 12, 2017). China to build giant facial recognition database to identify any citizen within seconds. South China Morning Post. Available at <https://is.gd/Ac1Ekj>. Accessed 04 November 2019.

CNCERT. (2019). 2018 summary of China's Internet network security status. National Computer Network Emergency Response Technical Team/Coordination Centre of China. Available at <https://is.gd/z10SHh> [Chinese]. Accessed 04 November 2019.

Cyberspace Administration of China (CAC). (2017). Cybersecurity Law of the PRC [English trans. by R. Creemers, P. Triolo, & G. Webster]. New America Foundation. Available at <https://is.gd/Nva3H8>. Accessed 04 November 2019.

Cyberspace Administration of China (CAC) (2019). The 44th Statistical survey report on Internet development in China. Cyber Administration of China. Retrieved from <https://is.gd/Ra07Ai>. [Chinese]

Cyberspace Administration of China (CAC). (July 22, 2019). Measures on Credit Information Management for Seriously Untrustworthy Internet Information Services Entities (Draft for solicitation of comments). Available at <https://is.gd/YMcaUF> [Chinese]. Accessed 04 November 2019.

Demchak, C. (2016). Uncivil and post-Western cyber Westphalia: Changing interstate power relations of the cybered age. The Cyber Defence Review, 1(1), 49-74.

Economist, The. (May 6, 2017). The world's most valuable resource is no longer oil, but data. The Economist. Available at <https://is.gd/PQ6Vrj>. Accessed 04 November 2019.

eMarketer. (January 22, 2019). China to surpass US in total retail sales. Available at <https://is.gd/Da7ask>. Accessed 04 November 2019.

Fichtner, L. (2019). What kind of cyber security? Theorising cyber security and mapping approaches. Internet Policy Review, 7(2), 1-19.

Ford, C. (2019). Huawei and its siblings, the Chinese tech giants: National security and foreign policy implications. U.S. Department of State. Available at <https://is.gd/R9QnTs>. Accessed 04 November 2019.

Goldsmith, J. & Wu, T. (2006). Who controls the Internet? Illusions of a borderless world. New York, NY: Oxford University Press.

Goodman, M. (2015). Future crimes: Inside the digital underground and the battle for our connected world. New York: Anchor.

Hayward, F. (September 26, 2019). China unveils 500 megapixel camera that can identify every face in a crowd of tens of thousands. Telegraph. Available at <https://is.gd/coBnaM>. Accessed 04 November 2019.

Hong, Y. (2017). Networking China: The digital transformation of the Chinese economy. Urbana Champagne: University of Illinois Press.

Hong, Y. Q. (February 1, 2018). The politics and economics behind APEC's CBPR. Research Alliance for Data Governance and Cyber Security. Available at <https://is.gd/SXJPdl>. Accessed 04 November 2019. [Chinese]

Inkster, N. (2016). China's cyber power. London: Routledge.

Jenkins, N. (August 17, 2015). China shutters 50 websites for "inciting panic" over the Tianjin disaster. Time. Available at <https://is.gd/MjIRYw>. Accessed 04 November 2019.

Ji, X. (2014). Analysis of the status and trends of crime. China Criminal Law Magazine, 14(3), 116-124.

Jiang, M. (2010). Authoritarian informationalism: China's approach to Internet sovereignty. SAIS Review of International Affairs, 30(2), 71-89.

Jiang, M. & Fu, K. W. (2018). Chinese social media and big data: Big data, big brother, big profit? Policy & Internet, 10(4), 372-392. doi: 10.1002/poi3.187

Kaplan, F. (2017). Dark territory: The secret history of cyber war. NY: Simon & Schuster.

Kovacs, A. (2016). India and the Budapest Convention: To sign or not? Considerations for Indian stakeholders. Internet Democracy Project. Available at <https://is.gd/ffGBeA>. Accessed 04 November 2019.

Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: Some economic and institutional considerations. Electronic Commerce Research, 13, 41-69.

Liang, F., Das, V., Kostyuk, N. & Hussain, M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. Policy & Internet, 10(4), 415-453.

Lindsay, J. (2014). The impact of China on cybersecurity: Fiction and friction. International Security, 39(3), 7-47.

Lindsay, J., Cheung, T., & Reveron, D. (Eds.) (2015). China and cybersecurity: Espionage, strategy, and politics in the digital domain. Oxford, UK: Oxford University Press.

Liu, Y. & Lin, L. (2018). How China should respond to GDPR. Information and Communications Technology and Policy, 9, 74-77. [Chinese]

Mozur, P. (July 8, 2018). Inside China's dystopian dreams: A.I., shame and lots of cameras. New York Times. Available at <https://is.gd/keI3nH>. Accessed 04 November 2019.

Oppermann, D. (2010). Virtual attacks and the problem of responsibility: the case of China and Russia. Carta Internacional, 5(2), 11-25.

Qin, A. (February 20, 2019A). Military strategy behind Russia's preparation to cut itself from the Internet: Lessons for China? Kunglunce Web. Available at <https://is.gd/sgLaSJ>. Accessed 04 November 2019.

Qin, A. (June 12, 2019B). High vigilance for American cyberwar at its last stage of preparation. Kunglunce Web. Available at <https://is.gd/QbyeYi>. Accessed 04 November 2019.

Raine, L., Anderson, J., & Connolly, J. (October 29, 2014). Cyber attacks likely to increase. Pew Research Centers" Internet American Life Project. Available at <https://is.gd/0TkJzx>. Accessed 04 November 2019.

Raul. A. (Ed.) (2018). Privacy, data protection and cybersecurity law review (5th Ed.). London: Law Business Research.

Schia, N. & Gjesvik, L. (2017). China's cyber sovereignty: Policy brief. Norwegian Institute of International Affairs.

Shen, H. (2016). China and global Internet governance: Toward an alternative analytical framework. Chinese Journal of Communication, 9(3), 304-324.

Singer, P. & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford, UK: Oxford University Press.

Sina Financial. (March 14, 2019). Consumer complaints and consultation requests over 10 million in 2018. Sina. Available at <https://is.gd/aOCjg0>. Accessed 04 November 2019.

Sputnik International. (March 13, 2018). China to continue cybersecurity drills within SCO. Sputnik International. Retrieved from <https://is.gd/7Ij51U

State Council. (2016). Inter-ministerial joint conference to help protect consumer rights. State Council of the PRC. Available at <https://is.gd/1NGXGJ>. Accessed 04 November 2019.

Tencent. (March 5, 2016). China's online black market participants exceed 400,000; Tencent implements five measures to ensure security. Tencent Daqing Net. Available at <https://xian.qq.com/a/20160305/035854.htm [Chinese]>. Accessed 04 November 2019.

U.S. Department of Justice. (2014). U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage. Available at <https://is.gd/uNhOUl>. Accessed 04 November 2019.

Xinhua Net (August 6, 2015). Study strategies: 5 keywords to understand President Xi's new proposal on cyber security. Xinhua Net. Retrieved from <https://is.gd/sEcug7>. [Chinese]

Xinhua Net. (September 16, 2017). Insiders explain how to "hit where it hurts" when it comes to cybercrime. Xinhua Net. Available at <https://is.gd/tXlkGW> [Chinese]. Accessed 04 November 2019.

Xinhua Net. (August 28, 2018). Cyber black and gray markets cause annual loss of nearly RMB 100 billion in China. Xinhua Net. Available at <https://is.gd/SBfwib> [Chinese]. Accessed 04 November 2019.

Xu, K. (2019). Effects and functions of Personal Information Security Specification. China Information Security, 3, 44-47. [Chinese]

Xue, H. (2019). An instant analysis of Chinese Electronic Commerce Law. CyberBRICS Project. Retrieved from <https://is.gd/5PUOu3>.

Wang, C. (2018). Comparing GDPR's personal data rights and Cybersecurity Law's personal information rights. China Information Security, 7, 41-44. [Chinese]

Wang, H. (February 14, 2017). China has established 1116 "cybersecurity police units." Guangmin Daily. Available at <https://is.gd/FwebOV> [Chinese]. Accessed 04 November 2019.

Yu, Z. & Wu, S. (2018). Historical summary of cybercrime legislation, judicial interpretation and theories. Politics & Law, 1, 59-78. [Chinese]

Annex

Country Report: China

1. Data Protection

▪ Scope

1. What national laws (or other type of normative acts) regulate the collection and use of personal data?

These mainly include the following categories:

National-level laws and decisions:

Criminal Law (1997) Amendment V (2005), VII (2009), and IX (2015)

Law of the People's Republic of China on the Protection of Consumer Rights and Interests (1994) with Amendment in 2013

Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks (2012)

Cybersecurity Law of the People's Republic of China (2017)

General Rules of the Civil Law of the People's Republic of China (2017)

E-Commerce Law of the People's Republic of China (2019)

Measures on Security Assessment of the Cross-border Transfer of Personal Information (Draft for comments, 2019)

Data Security Administrative Measures (Draft for comments, 2019)

Judicial interpretations:

Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement on Citizens' Personal Information (2017)

Administrative regulations:

Provisions on Protecting the Personal Information of Telecommunications and Internet Users (2013) issued by Ministry of Industry and Information Technology

Measures on Security Assessment of the Cross-border Transfer of Personal Information (June 13, 2019 Draft) issued by Cyberspace Administration of China

Industry standards:

Information Security Technology – Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems (GB/Z 28828-2012) (2013)

Information Security Technology – Personal Information Security Specification (GB/T 35273-2017) (2017)

Among them, the *Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks* (2012) is the earliest national law providing a broad legal framework for protecting personal data. The *Cybersecurity Law of PRC* (2017) broadly regulates the collection, storage, transmission and use of "personal information" by network operators and critical information infrastructure operators. Article 111 of the *General Rules of the Civil Law of the PRC* (2017) also broadly protects personal information. *Personal Information Security Specification* (GB/T 35273-2017) (2017), thereafter referred to as *Specification* (2017), is the most comprehensive interpretation of personal data regulations in China. However, the GDPR-like *Specification* (2017) is a technical standard to be followed voluntarily, not a compulsory law that one must comply with. A new draft (January 30, 2019) of the *Specification* is under consideration. The Cyberspace Administration of China (CAC) in 2019 also released a draft of *Data Security Administrative Measures* for public comment, thereafter referred to as *Measures* (2019). The *Measures* are consistent with other regulations and specifications in this area but if approved, will be legally binding and have more enforcement power than the *Specification*.

2. Is the country a party of any international data protection agreement?

No.

3. What data is regulated?

Article 76 of the *Cybersecurity Law of the PRC* (2017) and ***Article 38.3*** of the *Measures* (2019) define "personal information" as:

"all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including but not limited to natural persons' full names, birth dates, national identification numbers, personal biometric information, addresses, telephone numbers, and so forth."

Article 3.1 of the *Specification* (2017) defines "personal information" as:

"personal information, recorded by electronic or other means, that can be used, alone or combined with other information, to identify a specific natural person or reflect activities of a specific natural person."

4. Are there any exemptions?

Yes. **Article 8.5** of the *Specification* (2017) – Exemptions From Obtaining Authorized Consent Prior to Sharing, Transfer, and Public Disclosure of Personal Information – explains that:

The personal information controller does not need to obtain authorized consent from the personal information subject prior to sharing, transfer, or public disclosure of personal information in the following circumstances:

- Those directly related to national security and national defence;

- Those directly related to public safety, public health, and significant public interests;
- Those directly related to criminal investigation, prosecution, trial, and judgment enforcement, etc.;
- When safeguarding the major lawful rights and interests such as life and property of personal information subjects and other individuals, and it is difficult to obtain consent from personal information subject;
- When the personal information subject voluntarily opened the collected personal information to the general public;
- When the personal information is collected from legitimate public information channels, such as legitimate news reports and open government information.

Article 27 of the *Measures* (draft, 2019) states the following exemptions:

- the personal information was collected from legitimate and public channels in a manner that is not evidently against the will of the personal information subject;
- the personal information has been made public by the personal information subject voluntarily;
- the personal information has undergone anonymization;
- the provision is necessary for law enforcement agencies to perform their duties in accordance with law;
- the provision is necessary for the purposes of safeguarding national security, social and public interests, or the life and safety of the personal information subject.

5. To whom do the laws apply?

Article 2 of *Data Security Administrative Measures* (2019 Draft) states the law applies to entities that carry out "activities such as the collection, storage, transmission, processing and use of data" as well as the protection, regulation and administration of data security within China. The *Measures* (2019 draft) also states household and personal affairs are not covered by the law.

6. Do the laws apply to foreign entities that do not have physical presence in the country?

In general, no. However, in Appendix D "Privacy Policy Template" of the *Specification* (2017), Section 7 of the Appendix "How your information will be transferred globally" explains that for countries and territories without or with different personal data protection laws, China will provide at the bare minimum equal protection afforded to persons and entities within Chinese territory.

Further, ***Article 20*** of *Measures on Security Assessment of the Cross-border Transfer of Personal Information* (draft, 2019) can have impact on foreign entities that collect data from Chinese subjects even though they don't have physical presence in China:

"If the business activities of an organization located outside China result in the collection of personal information of domestic users through the Internet and other means, then that organization

shall fulfil the responsibilities and obligations of network operators in these Measures through a legal representative or entity within the territory."

- **Definitions**

7. How are personal data defined?

Article 3.1 of the *Specification* (2017) defines "personal information" as:

All kinds of information, recorded by electronic or other means, that can be used, alone or combined with other information, to identify a specific natural person or reflect activities of a specific natural person.

8. Are there special categories of personal data (e.g. sensitive data)?

Yes. ***Article 3.2*** of the *Specification* (2017) defines "personal sensitive information" as:

Personal information that, once leaked, illegally provided, or abused, can threaten personal and property security and/or easily cause personal reputational damage, physical and mental health damage, or discrimination.

9. How is the data controller and the data processor/operator defined?

Article 3.4 of the *Specification* (2017) defines "personal information controller" as:

An organization or individual that has the authority to determine the purposes and/or methods of the processing of personal information.

10. What are the data protection principles and how are they defined?

Article 4 of the Specification (2017) includes the following "Basic Principles of Personal Information Security":

Personal information controllers should follow the basic principles below when processing personal information:

1) Commensurability of Powers and Responsibilities Principle: Bear responsibility for damage to the lawful rights and interests of the personal information subject caused by personal information processing.

2) Purpose Specification Principle: Process personal information for legal, justified, necessary, and specific purposes.

3) Consent Principle: Obtain authorized consent from the personal information subject after expressly providing the personal information subject with the information including the purpose, method, scope, and rules of the processing.

4) Minimization Principle: Unless otherwise agreed by the personal information subject, only process the minimum types and quantity of personal information necessary for the purposes for which the authorized consent is obtained from the personal information subject. After the purposes have been achieved, the personal information should be deleted promptly according to the agreement.

5) Openness and Transparency Principle: The scope, purposes, and rules, etc., of personal information processing should be open to public in an explicit, intelligible, and reasonable manner, and outside supervision should be accepted.

6) Ensuring Security Principle: Possess the appropriate security capacity taking into account the security risks [the controller] faces, and implement sufficient management and technical measures to safeguard the confidentiality, integrity, and availability of personal information.

7) Subject Participation Principle – Provide the personal information subject with means to access, correct, and delete the personal information, to withdraw consent, and to close accounts.

11. Does the law provide any specific definitions with regards to data protection in the digital sphere?

The law does not mention "digital sphere" but it is generally understood that network and online activities engaged in "the collection, storage, transmission, processing and use of data" occur in the digital sphere. The Data Security Administrative Measures (2019 Draft) provides details for proper data collection, data processing and use, as well as data security regulation and administration. Chapter V specifically provides definitions for "network operators," "network data," "personal information," "personal information subject" and "important data."

▪ Rights

12. Is the data protection law based on fundamental rights (defined in Constitutional law or International binding documents)?

The *Specification* (2017) or *Measures* (draft, 2019) does not explicitly refers to the Chinese Constitution or international binding documents. "Introduction" of the *Specification* states the necessity for the *Specification* to also comply with other pre-existing Chinese laws and regulations including all the rights and responsibilities of citizens outlined in Chapter II of the Constitution.

13. What are the rights of the data subjects according to the law?

Article 5.6 of the *Specification* (2017) states the data subject has the right to: "access, correct, or delete data; to deactivate the account, to withdraw consent; to obtain a copy of the data; to restrain automated decision-making by the information system; etc."

Article 7.7 of the *Specification* states the data subject has the right to: "refuse to receive business advertisements delivered on the basis of their personal information"

In Appendix D "Privacy Policy Template" of the *Specification* (2017), Section 5 "Your rights" specifies the following user rights:

1) Access your personal information such as account information, search information etc.

2) Correct your personal information

3) Delete your personal information

4) Modify the scope of your consent such as the collection and use of extra personal information and decline of business advertisements

5) Personal information subject deletes the account

6) Personal information subject obtains a copy of personal information

7) Restrain automated decision-making by the information system

8) Responds to the above requests

2. Obligations and Sanctions

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

The main body of the *Specification* (2017) lays out in detail the obligations for "personal information controllers": the collection of personal information (***in Article 5***), retention of personal information (**in *Article 6*),** use of personal information **(in *Article 7*)**, processing, sharing, transfer, and public disclosure of personal information **(in *Article 8*),** as well as the handling of personal information during security incident **(in *Article 9*).**

Article 6 of the *Measures* (draft, 2019) states:

"Network operators must perform their obligations to protect data security, establish an accountability and assessment system for data security management, formulate data security plans, implement technical safeguards for data security, conduct data security risk assessments, formulate emergency response plans for cyber security incidents, promptly deal with security incidents and organize data security education and training."

15. Is notification to a national regulator or registration required before processing data?

Yes, operators are expected to obtain approval for cross-border data transfer from provincial-level office of Cyberspace Administration of China (CAC) according to Measures on Security Assessment of the Cross-border Transfer of Personal Information (see Question #24 for this section)

16. Does the law require privacy impact assessment to process any category of personal data?

Yes. ***Article 10.2*** of the *Specification* (2017) details the process of "Carrying Out Personal Information Security Impact Assessments." It should be understood however that compliance with the entire *Specification* is voluntary, not mandatory.

17. What conditions must be met to ensure that personal data are processed lawfully?

The explicit authorization and consent by the personal information subject is required.

Article 9 of the *Measures* (draft, 2019) states:

"Where the rules for the collection and use of personal information are included in a privacy policy, such rules shall be relatively focused with clear instructions for ease of understanding. In addition, network operators may collect personal information only if the user is aware of and explicitly consents to such rules."

Article 5.3 of the *Specification* (2017) states that:

"Prior to the collection of the personal information, clearly provide the information subject with the following information and obtain the authorized consent from the personal information subject: the respective types of the personal information collected by different operational functions of the products or services; the rules of collecting and using the personal information (e.g., purpose of collection and use; manner and frequency of collection; storage location; storage period; [the controller's] data security capabilities; information related to sharing, transferring, and public disclosure; etc.)."

18. What are the conditions for the expression of consent?

Article 3.6 defines "Explicit Consent" as:

"The explicit authorization by the personal information subject of specific personal information processing through a written statement or an affirmative action on the personal information subject's own initiative.

Note: Affirmative action includes the personal information subject, on his or her initiative, making a statement (in electronic form or on paper), checking a box, or clicking "agree," "sign up," "send," "dial," etc."

19. If the law foresees special categories of data, what are the conditions to ensure the lawfulness of processing of such data?

The *Specification* (2017) calls attention to "sensitive information" (defined in ***Article 3.2***). It details in ***Article 5.5*** the "Explicit Consent for Collection of Personal Sensitive Information" as well as the requirements for "Personal Sensitive Information Transfer and Storage" in ***Article 6.3***.

20. What are the security requirements for collecting and processing personal data?

As a basic principles of personal information security, ***Article 4*** of the *Specification* (2017) states that information controllers should possess the appropriate security capacity to address potential security risks, implement sufficient management and technical measures to safeguard the confidentiality, integrity, and availability of personal information.

In terms of organizational arrangements, ***Article 10.1*** states responsible departments and personnel should be designated to take measures to protect personal information including security assessment, training and audits.

Article 10.2 spells out the details regarding "Carrying Out Personal Information Security Impact Assessments."

Article 10.3 asks information controllers to establish data security capabilities.

Article 10.4 specifies the main aspects of managing and training personnel for information security.

Article 10.5 spells out the requirements for security audits.

21. Is there a requirement to store (certain types of) personal data inside the jurisdiction?

Yes. ***Article 37*** of *Cybersecurity Law of the People's Republic of China* (2017) specifies:

"Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China."

22. What are the requirements for transferring data outside the national jurisdiction?

Article 37 of *Cybersecurity Law* (2017) specifies:

"Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions."

The draft of a new law regulating cross-border personal data transfer – *Measures on Security Assessment of the Cross-border Transfer of Personal Information* – specifies that network operators must apply for security assessment for cross-border transfer of personal data from the provincial-level cybersecurity regulator (provincial branch of Cyber Administration of China).

23. Are data transfer agreements foreseen by the law?

So far, China is not part of any international treaty for personal data/information protection. Its *Cybersecurity Law* (2017) recognizes the need for cross-border data transfer and asks information controllers to follow relevant laws to conduct security assessment (Article 37).

The Cyber Administration of China issued a draft of *Measures on Security Assessment of the Cross-border Transfer of Personal Information* in 2019 for public comments for protecting the cross-border transfer of personal information. **Article 20** of the new *Assessment* specifies:

"If the business activities of an organization located outside China result in the collection of personal information of domestic users through the Internet and other means, then that organization shall fulfil the responsibilities and obligations of network operators in these Measures through a legal representative or entity within the territory."

24. Does the relevant national regulator need to approve the data transfer agreements?

Yes. ***Article 37*** of *Cybersecurity Law* (2017) specifies:

"Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatisation departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions."

The draft of a new law regulating cross-border personal data transfer – *Measures on Security Assessment of the Cross-border Transfer of Personal Information* – specifies that network operators must apply for security assessment for cross-border transfer of personal data from the provincial-level cybersecurity regulator (provincial branch of Cyber Administration of China).

25. What are the sanctions and remedies foreseen by the law for not complying with the data transfer obligations?

For non-compliance, either by "storing network data outside the mainland territory, or provide network data to those outside of the mainland territory," ***Article 66*** of the *Cybersecurity Law* (2017) states punishments can include:

- fines between 50,000 and 500,000 RMB,
- temporary suspension of operations,
- suspension of business for corrective measures,
- closing down of websites,
- revocation of relevant operations permits, or cancellation of business licenses
- fines between RMB 10,000 and 100,000 for responsible personnel.

Amendment IX to the Criminal Law of the PRC (2015) also states:

"Any network service provider that fails to perform the information network security management obligation as prescribed in any law or administrative regulation and refuses to make corrections after being ordered by the regulatory authority to take correction measures shall be sentenced to imprisonment of not more than three years, criminal detention or surveillance in addition to a fine or be sentenced to a fine only under any of the following circumstances:

- Causing the spread of a large amount of illegal information
- Causing the leakage of users' information, with serious consequences
- Causing the loss of criminal case evidence, with serious circumstances
- Any other serious circumstance.

Where an entity commits the crime as provided for in the preceding paragraph, a fine shall be imposed on it, and its directly responsible person in charge and other directly liable persons shall be punished in accordance with the provisions of the preceding paragraph."

3. Actors

26. What actors are responsible for the implementation of the data protection law?

Actors responsible for the implementation of the data protection provisions are not specified in the law or the *Specification* (2017).

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

Not specified, but operators are expected to obtain approval for cross-border data transfer from Cyberspace Administration of China (CAC) according to *Measures on Security Assessment of the Cross-border Transfer of Personal Information* (see Question #24 above).

28. What are the powers of the actors responsible for the implementation of the data protection law?

Not specified. Overall, the *Cybersecurity Law of PRC* (2017) broadly regulates the collection, storage, transmission and use of "personal information" by network operators and critical information infrastructure operators. The country's top cyber policymaking body, Cyberspace Administration of China (CAC), coordinates cybersecurity work including personal data protection laws.

2. Consumer Protection

4. Scope

29. What national laws (or other type of normative acts) regulate consumer protection?

The following laws and policies regulate consumer protection:

National-level laws:

Law of the People's Republic of China on the Protection of Consumer Rights and Interests (passed in 1994, amendments in 2009 and 2013)

Advertising Law of the People's Republic of China (passed in 1995, revisions in 2015)

E-Commerce Law of the People's Republic of China (2018)

Judicial opinions:

Ten Model Cases Involving the Protection of Consumer Rights Issued by the Supreme People's Court (2014)

Ten Model Cases of Consumers' Rights Protection Published by the Supreme People's Court (2015)

Eight Model Cases involving Procuratorial Organs' Cracking down on Crimes Infringing on Consumers' Rights and Interests Published by the Supreme People's Procuratorate (2019)

Administrative regulations:

Guiding Opinions of the General Office of the State Council on Strengthening the Protection of Financial Consumers' Rights and Interests (2015)

Letter of the General Office of the State Council on Approval of the Establishment of the Inter-Ministerial Joint Meeting System for the Protection of Consumer Rights and Interests (2016)

30. Is the country a party of any international consumer protection agreement?

The China Consumer Association joined the non-for-profit international organization – International Organization of Consumers Unions – in 1987. As a UN member state, China abides by the *United Nations Guidelines on Consumer Protection* (2016).

31. To whom do consumer protection laws apply?

The *Law of the PRC on the Protection of Consumer Rights and Interests* (1994) applies to consumers and business operators. The *Advertising Law of the People's Republic of China* applies

to business operators and service providers that advertise their products and services. The *E-Commerce Law* (2018) applies to e-commerce activities in Chinese territories.

32. Do the laws apply to foreign entities that do not have physical presence in the country?

No.

5. Definitions

33. How is consumer protection defined?

The *Law of the PRC on the Protection of Consumer Rights and Interests* (1994) declares that: "The State shall protect consumers' legal rights and interests against infringement."

34. How are consumers defined?

The *Law of the PRC on the Protection of Consumer Rights and Interests* (1994, with 2013 amendment) does not clearly define "consumer." In most circumstances, the law applies to natural persons within Chinese territory, not companies or legal persons.

35. How are providers and producers defined?

The *Law of the PRC on the Protection of Consumer Rights and Interests* (1994, with 2013 amendment) does not provide an explicit definition for providers or producers. In the context of the law, a provider or producer is "a business operator providing a commodity or service to a consumer."

36. Does the law provide any specific definitions with regards to consumer protection in the digital sphere?

Article 25 and ***28*** of the *Law of the PRC on the Protection of Consumer Rights and Interests* (1994, with 2013 amendment) acknowledge the increasing frequency of online transactions and provide general guidelines for business operations and resolutions of related disputes, but it does not provide specific definition with regards to consumer protection in the digital sphere.

The new *E-commerce Law* (2018) extends the protection of consumer rights and interests to e-commerce activities in Chinese territory. It defines a number of relevant concepts including "e-commerce," "e-commerce operators," "e-commerce platform operators," "operators on platform" who are accorded different rights and obligations.

6. Rights

37. Is the consumer protection law based on fundamental rights (defined in Constitutional law or International binding documents)?

Neither the *Law of the PRC on the Protection of Consumer Rights and Interests* (1994, with 2013 amendment) nor the new *E-commerce Law* (2018) references the Chinese Constitution or other international binding documents. However, as a UN member state, China abides by the *United Nations Guidelines on Consumer Protection* (2016). The drafting of the new *E-commerce Law* also invited

commentary from the United Nations Commission on International Trade Law (UNCITRAL), United States, European Union, Germany, Singapore, Japan and etc.

38. What are the rights of the consumer defined by the law with reference to digital goods and services?

Article 25 of the *Law of the PRC on the Protection of Consumer Rights and Interests* (2013 amendment) excludes the return of digital goods and services from the list of commodities that can be returned within 7 days of transactions.

Article 2 of the *E-commerce Law of the PRC* (2018) specifies that: "This Law shall not apply to financial products and services, or services providing news and information, audio and video program, publication and cultural products through information network." The law covers tangible goods sold online as well as certain digital goods and services such as software, apps or platforms (e.g. ridesharing, online payment). Presumably the *transaction* of digital content products such as online news, e-books, digital music, and online games falls under the *E-commerce Law* (2018), whereas the *legitimacy* of digital content to be made available to consumers is under the purview of content regulators like CAC or SARFT.

Various articles of the *E-commerce Law of the PRC* (2018) declare to protect a wide range of consumer rights and interests such as (only a sample):

1) the right to accurate information and selection of products and services ***(Article 17)***,
2) the right to search results of products and services not based on consumer characteristics ***(Article 18)***,
3) the right to having bundled goods or services as an option rather than as a default ***(Article 19)***,
4) the right to agreed-upon modes and means of delivery of goods and services with online sellers and platforms ***(Article 20)***,
5) the right to refund of deposits ***(Article 21)***,
6) the right to safety, accuracy, correction, removal of personal information ***(Articles 23, 24, and 25)***,
7) the right to easy access to service agreements and transaction rules on e-commerce platforms ***(Article 33)***,
8) the right to provide feedback to amendments to platform agreement and transaction rules ***(Article 34)***,
9) the right to personal and property safety, free from harm as a result of platform operators knowingly selling faulty goods or products *(Article 38)*,
10) the right to product or service reviews where platforms are forbidden to remove customer reviews ***(Article 39)***,

11) the right to "advertised" products or services clearly labelled in search results displays ***(Article 40)***,

12) the right to clear, comprehensive and accurate information about establishing a contract ***(Article 50)***.

39. Is consumer protection law applicable to users of zero price services i.e. free of charges?

No.

7. Obligations and Sanctions

40. Does the law establish specific security requirements to provide digital services or goods?

Article 30 of the *E-commerce Law* (2018) requires platform operators to provide network security, ensure transaction safety, prevent cybercrimes and report incidents promptly to relevant authorities.

Article 38 of the *E-commerce Law* (2018) requires platform operators to conduct due diligence to ensure the safety of consumers and their property. If found irresponsible, for instance, knowingly selling faulty goods or products, platform operators could assume partial responsibility.

Article 54 of the *E-commerce Law* (2018) requires platform operators to comply with government requirements regarding electronic payment safety and assume responsibility as a result of harm to consumers.

Article 57 of the *E-commerce Law* (2018) requires platform operators to take precautions to secure consumer passwords, electronic signatures and other security measures and be liable to losses proportional to their responsibility.

41. What are the sanctions and remedies foreseen by the law for not complying with the obligations?

In principle, **Section 7** of the *Law of the PRC on the Protection of Consumer Rights and Interests* (1994, with 2013 amendment) outlines the sanctions and remedies foreseen by the law regarding noncompliance.

Section 6 of the *E-commerce Law* (2018) also specifies the sanctions and remedies pertaining to e-commerce, online transaction, digital goods and services.

8. Actors

42. What bodies are responsible for the implementation of the consumer protection law?

Article 32 of the *Law of the PRC on the Protection of Consumer Rights and Interests* (1994, with 2013 amendment) specifies the *Administrative Department for Industry and Commerce* to be the main department to lead the implementation of the consumer protection law.

Article 6 of the *E-commerce Law* (2018) requires local governments above the county-level to establish the division of duties concerning e-commerce regulation. A newly created department in

2018 – State Administration for Market Regulation – is tasked to coordinate e-commerce regulation efforts.

43. Is there a specific consumer protection body? If so, what is its administrative structure?

The State Administration for Market Regulation (SAMR) has the regulatory authority over a broad umbrella of areas including market competition, monopoly, intellectual property, drug safety, and standardization. Consumer protection now falls under its purview as it oversees the operations of non-profit organizations such as China Consumer Association and China Association for Consumer Products Quality and Safety Promotion. The Department of Online Transaction Regulation under the SAMR is tasked to supervise e-commerce.

44. What are the powers of the bodies responsible for the implementation of the consumer protection law?

The Department of Online Transaction Regulation under the SAMR is tasked to formulate and implement institutional measures to regulate online commodity transactions and related services; enforce law in the online market; organize and guide the standardized management of online transaction platforms and online operators; monitor online markets; supervise and manages and coordinates the administrative contracts and auctions according to law; and guide the construction of the consumption environment.

3. Cybercrime

▪ Scope

45. What national laws (or other type of normative acts) regulate cybercrime?

Cybercrime in China is regulated by a series of laws and policies at the following levels:

National-level laws and decisions:

1) Articles 253-1, 285, 286, and 287 of the *Criminal Law* (1997)
2) Amendments VII (2009) and IX (2015) to the *Criminal Law*
3) *Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security* (2000)
4) *Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks* (2012)
5) *Anti-Terrorism Law of the People's Republic of China (2015)*
6) *Cybersecurity Law of the People's Republic of China* (2017)

Judicial interpretations:

7) *Interpretations (II) of Several Issues on Application of Law in Handling Criminal Cases about Producing, Reproducing, Publishing, Selling and Disseminating Pornographic Electronic*

Information via the Internet, Mobile Communication Terminals and Sound Message Stations (2010)

8) *Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Internet Gambling (2010)*

9) *Interpretations on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks (2012)*

10) *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Specific Application of Law in the Handling of Defamation through Information Networks and Other Criminal Cases (2013)*

11) *Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Several Issues concerning the Application of Criminal Procedures in the Handling of Cyber Crime Cases (2014)*

12) *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement on Citizens' Personal Information* (2017)

Ministerial regulations:

13) *Measures for Security Protection in the Administration of the International Networking of Computer Information Networks (1997) issued by the Ministry of Public Security*

14) *Regulations on Internet Security Supervision and Inspection by Public Security Organs (2018) issued by Ministry of Public Security*

15) *Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases (2019) issued by the M*inistry of Public Security

46. Is the country a party of any international cybercrime agreement?

Yes. As a member state of the Shanghai Cooperation Organization, China agreed in 2012 at a Meeting of the Council of the Heads of Member States to participate in efforts to fight against terrorism, separatism, extremism, and international cybercrime. China is also a member of the Interpol.

47. What cybercrimes are regulated?

First, cybercrime is covered under the Criminal Law (1997) and two amendments (VII and IX) including the following offences mainly:

1) Illegally infringing on or selling personal information resulting in serious harm (Article 253-1),
2) illegally accessing computer systems to interfere with state affairs, defence, and cutting-edge technology areas (Article 285),
3) illegally accessing, changing or controlling data held on computer systems (Article 285),

4) providing programs and tools to access or illegally control computer systems (Article 285, Amendment VII),
5) disabling or destroying computer systems (Article 286),
6) deleting, modifying memory, data transmission and programs in computer systems resulting in damage (Article 286),
7) intentionally creating and disseminating computer virus resulting in damage (Article 286),
8) ISPs repeatedly failing to fulfil their responsibility to safely manage information and network security according to laws and administrative regulations resulting in wide spread of illegal information, serious data leak, serious loss of criminal evidence, and other serious situations (Article 286-1, Amendment IX),
9) committing various crimes using computers including financial fraud, theft, corruption, embezzlement of public funds, stealing state secrets (Article 287),
10) creating websites or online groups to commit fraud, teach methods of committing crimes, make and sell goods forbidden by law (Article 287-1, Amendment IX),
11) distributing information about making or selling illegal drugs, guns, pornography and other prohibited products (Article 287-1, Amendment IX),
12) distributing information to facilitate illegal activities such as fraud (Article 287-1, Amendment IX),
13) being an accomplice to computer crimes resulting in serious damage, e.g. providing Internet access, server custody, network storage, communication transmission or any other technical support, or provides advertising, payment settlement (Article 287-1, Amendment IX),
14) an entity committing any crime described above (Article 287-2, Amendment IX)
15) fabricating or deliberately spreading, on the Internet or other media, false information regarding dangerous situations, epidemics, disasters or police emergencies, which seriously disturb social order (Article 291-1, Amendment IX)

Cybersecurity Law (2017) carries articles similar to the above. In addition, a series of judicial interpretations provide detailed explanations for online pornography, online defamation, online gambling, and infringements of right to disseminate information online.

48. To whom do the laws apply?

Provisions dealing with cybercrime are in the *Criminal Law*. Hence, the jurisdiction principles for the *Criminal Law* (see ***Articles 6*** to ***11***) apply to cybercrime.

49. Do the laws apply to foreign entities that do not have physical presence in the country?

Yes, in some instances. ***Article 8*** of the *Criminal Law* states:

"This law may be applicable to foreigners, who outside PRC territory, commit crimes against the PRC state or against its citizens, provided that this law stipulates a minimum sentence of not less

than a three-year fixed term of imprisonment for such crimes; but an exception is to be made if a crime is not punishable according the law of the place where it was committed."

- **Definitions**

50. How is cybercrime generally defined by the national law?

While the *Criminal Law* outlines different types of cybercrime, in the *Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Several Issues concerning the Application of Criminal Procedures in the Handling of Cyber Crime Cases* (2014), cybercrime is defined as:

1) cases concerning crimes of endangering the security of a computer information system;
2) cases concerning crimes of theft, fraud, and extortion that are committed by endangering the security of a computer information system;
3) cases concerning crimes of publishing information on the network or establishing a website or a communication group mainly for committing crimes, committing crimes on an unspecific majority of people, or organizing, instigating, or assisting an unspecific majority of people in committing crimes; and
4) other cases in which major criminal activities are committed on the network.

51. What are the cybercrimes provided for by the law and how are they defined?

No specific definitions are provided for various cybercrimes. See the answer to Question 3 in this section on Cybercrime.

52. How is a computer system defined?

There is no specific definition for "computer system." However, ***Article 76-1*** of *Cybersecurity Law* (2017) defines "network" as: "a system comprised of computers or other information terminals and related equipment that follows certain rules and procedures for information gathering, storage, transmission, exchange, and processing."

53. How are computer data defined?

There is no specific definition for "computer data". However, *Article 76-4* of *Cybersecurity Law* (2017) defines "network data" as: "all kinds of electronic data collected, stored, transmitted, processed, and produced through networks."

54. How are forensic data defined?

Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Several Issues concerning the Application of Criminal Procedures in the Handling of Cyber Crime Cases (2014) defines "forensic data" as two types of data during cybercrime investigations:

1) Electronic data that can be displayed directly such as electronic documents, images and webpages;

2) Electronic data that cannot be displayed directly such as computer programs, tools and virus in computer information systems illegally attacked and controlled.

55. How are service providers defined?

No, but ***Article 76-3*** of *Cybersecurity Law* 2017) defines "network operators" as "network owners, managers, and network service providers."

56. Does the national law provide any other definitions instrumental to the application of cybercrime legislation?

No.

▪ Rights

57. Is the cybercrime law based on fundamental rights (defined in Constitutional law or International binding documents)?

Cybercrime laws in China do not explicitly reference the Chinese Constitution or international binding documents.

58. What are the rights of the victim and the accused?

Rights of the victim and accused should comply with other pre-existing Chinese laws and regulations including all the rights and responsibilities of citizens outlined in Chapter II of the Constitution.

▪ Procedures

59. Is there a specific procedure to identify, analyse, relate, categorize, assess and establish causes associated with forensic data regarding cybercrimes?

Section V (***Articles 13-18***) of the *Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Several Issues concerning the Application of Criminal Procedures in the Handling of Cyber Crime Cases* (2014) and *Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases* (2019) outline the detailed procedure to obtain forensic date regarding cybercrime.

60. In case of transnational crimes, how is cooperation between the national law enforcement agency and the foreign agents regulated?

Although China is not a party or observer of the *Budapest Convention* (or *Convention on Cybercrime*), it is a signee of the *World Intellectual Property Organization Copyright Treaty* (WIPO Copyright Treaty) in 1985 and the *U.N. Convention Against Transnational Organized Crime* in 2000.

In addition, China actively explores regional (e.g. through Shanghai Cooperation Organization) and international (e.g. through UN anti-crime framework) avenues to seek cooperation against

transnational crimes including cybercrime. Through the Shanghai Cooperation Organization, China actively pursues avenues to conduct cybersecurity exercises.

61. Are there any exception to the use of mutual legal assistance procedure to investigate the crime?

According to ***Article 14*** of *International Criminal Judicial Assistance Law of the People's Republic of China* (2018), mutual legal assistance can be refused in the following circumstances:

1) According to the laws of the People's Republic of China, the requested act is not a crime;
2) At the time of receipt of the request, the inquiry, investigation, prosecution, and trial of the crime in the request are under way within the territory of the People's Republic of China, an effective judgment has been made, the criminal procedure has been terminated, or the limitation of the offence has expired;
3) The crime against which the request is made is a political offence;
4) The crime against which the request is made is purely a military offence;
5) The purpose of the request is to examine, investigate, prosecute, sue, or execute a sentence based on race, ethnicity, religion, nationality, gender, political opinion or identity, or the parties may be unfairly treated for the above reasons;
6) There is no substantive link between the requested matter and the case of assistance;
7) Other circumstances under which the request can be refused.

62. Does the national law require the use of measures to prevent cybercrimes? If so, what are they?

Apart from specifying punishments for various parties implicated in cybercrime through the *Criminal Law* and other related laws to deter cybercrime (see Question #3 above), China's national law (e.g. *Cybersecurity Law*) also requires network owners, operators, and ISPs to bolster cybersecurity measures and report crimes. In addition, Article 24 of the *Cybersecurity Law* (2017) effectively implements the "Real Name Registration" policy requiring users to provide real identity information to network operators upon signing agreements for products and services online.

▪ Obligations and Sanctions

63. What obligations do law enforcement agencies have to protect the data of the suspect, the accused and the victim?

Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement on Citizens' Personal Information (2017) provides legal protection for citizens' personal information investigated in criminal cases.

More specifically, according to *Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases* (2019) issued by the Ministry of Public Security,

law enforcement agencies protect "state secrets, police work secrets, trade secrets, individual privacy, and confidentiality" (Article 4) while collecting and processing forensic electronic data. Procedurally, for instance, two or more inspectors are supposed to gather electronic evidence supervised by technical experts (Article 6), ask data owners or witnesses to provide signature when appropriate (Article 9), and so on.

64. What are the duties and obligations of the National Prosecuting Authorities in cases of cybercrime?

Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Several Issues concerning the Application of Criminal Procedures in the Handling of Cyber Crime Cases (2014) outlines the duties of the Supreme People's Procuratorate, China's national prosecuting authorities in terms of jurisdiction (Article 2), data collection and prosecution (Article 5) and its relationships with the court and the police.

65. Does the law impose any obligations on services providers in connection with cybercrime?

Network operators are obliged under the *Cybersecurity Law* (2017) to keep logs for no less than six months. Operators are also expected to report cybercrime threats, attacks and breaches to relevant authorities, initiate contingency plans, and take remedial measures (Article 25).

66. To which extent can a legal person be held liable for actions in connection with cybercrimes?

Depending on the cybercrime, the relevant offence may incur a penalty of life imprisonment and/or a maximum fine of 500,000 RMB (***Articles 285, 286*** and ***287*** of the *Criminal Law*). Under the *Cybersecurity Law* (2017), engaging in activities that jeopardize cybersecurity, or providing programs or tools specifically used to engage in activities that jeopardize cybersecurity, is punishable by a fine of up to 500,000 RMB.

▪ Actors

67. What bodies implement the cybercrime legislation?

Presumably a wide range of governmental actors are involved in implementation including Ministry of Public Security, the Supreme Court, the Supreme People's Procuratorate, State Security, and Cyber Administration of China (the country's top authority of cybersecurity). More specifically, *Regulations on Internet Security Supervision and Inspection by Public Security Organs* (2018) issued by the Ministry of Public Security gives police forces considerable latitude to inspect network operators, Internet service providers and organizational users to prevent cybercrime.

68. Is there a special public prosecutor office for cybercrime? If so, how is it organised?

Article 6 of *People's Police Law of the People's Republic of China* (1995) assigns the police to protect the security of computer information systems. Between 2015 and 2017, the Ministry of Public Security has quickly established 1116 "cybersecurity police units" including "level one"

units within major Chinese Internet companies such as Baidu, Tencent and Sina tasked mainly to police online content and prevent cybercrime.

69. Does the cybercrime legislation create any specific body?

No.

4. Public Order

▪ Definitions

70. How are public order, threats to public order and the protection of public order defined?

Public order is not clearly defined in the *Chinese Constitution*, *National Security Law of the PRC* (2015), *Cybersecurity Law of the PRC* (2017), *Emergency Response Law of the PRC* (2006) or *Measures for Security Protection Administration of the International Networking of Computer Information Networks* (1997).

Article 5 of the *Measures* specifically forbids individuals to use the Internet to create, replicate, retrieve, or transmit information which "fabricates or distorts the truth, spreads rumours, and disturb public order."

Article 3 of the *Emergency Response Law of the PRC* (2006) defines "emergency incidents" as threats to public order in general that demand management:

"An emergency incident as mentioned in this Law shall refer to a natural disaster, accidental disaster, public health incident or social safety incident, which takes place by accident, has caused or might cause serious social damage and needs the adoption of emergency response measures."

Further, the *Cybersecurity Law* (2017) has mandated the establishment of an emergency monitoring and response information communication system (see Chapter V).

71. Is the protection of public order grounded in constitutional norms?

Article 28 of the *Constitution of the PRC* states:

"The state maintains public order and suppresses treasonable and other counter-revolutionary activities; it penalizes criminal activities that endanger public security and disrupt the socialist economy as well as other criminal activities; and it punishes and reforms criminals."

▪ Measures

72. What cyber measures address threats to public order?

Article 12 of the *Cybersecurity Law* states:

"Any person and organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they must not endanger cybersecurity, and must not use the Internet to engage in activities endangering national security, national honour, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and

ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts."

Article 58 of the *Cybersecurity Law* states:

"To fulfil the need to protect national security and the social public order, and to respond to the requirements of major security incidents within the society, it is possible, as stipulated or approved by the State Council, to take temporary measures regarding network communications in a specially designated region, such as limiting such communications."

- **Actors**

73. What public authorities are responsible for implementation of the surveillance techniques?

The law does not make explicit reference to nationwide surveillance measures, but the *Cybersecurity Law* (2017) establishes institutional structures and procedures to monitor, provide early warning and emergency responses to cybersecurity incidents (see Section V).

74. What are the obligations of these public authorities?

In general, Chinese laws give public authorities great power to implement surveillance systems in the name of cybersecurity.

Article 8 of the *Cybersecurity Law* (2017), for instance, states:

"State departments of cyber administration are responsible for comprehensively planning and coordinating cybersecurity efforts and related supervision and management efforts. The State Council departments for telecommunications, public security, and other relevant organs, are responsible for cybersecurity protection, supervision, and management efforts within the scope of their responsibilities, in accordance with the provisions of this Law and relevant laws and administrative regulations."

75. Can private actors be involved in the implementation of cyber measures to address threats to public order?

Private network operators and service providers are encouraged to self-regulate.

Article 28 of the *Cybersecurity Law* (2017) states: "Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."

Article 50 of the *Cybersecurity Law* (2017) specifies that state authorities can order network operators to stop the transmission of information prohibited by law both inside and from outside Chinese territories:

"State departments of cyber administration and relevant departments will perform network information security supervision and management responsibilities in accordance with law; and where they discover the publication or transmission of information which is prohibited by laws or administrative regulations, shall request that network operators stop transmission, employ disposition measures such as deletion, and store relevant records; for information described above that comes from outside the mainland People's Republic of China, they shall notify the relevant organization to adopt technical measures and other necessary measures to block transmission."

5. Cyberdefence

▪ Scope

76. Is there a national cyberdefence strategy or is cyberdefence mentioned in the national defence strategy?

Cyberdefence in China is regulated by a series of laws and policies at the following levels:

National-level laws:

1) *National Security Law of the People's Republic of China* (2015)

National strategies:

2) *China's Military Strategy* (2015), white paper released by the State Council Information Office of the PRC
3) *International Strategy of Cooperation on Cyberspace* (2016) released by CAC
4) *China National Cyberspace Security Strategy* (2017) released by CAC
5) *China's National Defence in the New Era* (2019), white paper released by the State Council Information Office of the PRC

77. What is the legal status of the national defence or cyberdefence strategy?

National Security Law of the PRC was passed in 2015 as an overarching framework for China's security policies. The Cyberspace Administration of China (CAC) also released two sets of prominent strategies for international and domestic cyberspace security (see above). Two white papers, *China's Military Strategy* (2015) and *China's National Defence in the New Era* (2019), provide more details of China's assessment of the current security situation as well as China's defence missions, reforms, and spending. More recently, industry standards have been developed to implement and conduct security review for network products and services including *Cybersecurity Review Measures* (2019 draft) and *Information Security Technology: Baseline for Classified Protection of Cybersecurity* (2019).

78. What national laws or other normative acts regulate cyberdefence in the country?

Counterterrorism Law of the People's Republic of China (2016).

79. Is the country party of any international cooperation agreement in the sphere of cyberdefence ?

Through the Shanghai Cooperation Organization, China signed an agreement with member states including Russia on cooperation in the field of international information security to confront terrorism, separatism and extremism.

80. Does the national cyberdefence strategy provide for retaliation?

No.

81. Is there any specific framework regulating threats to critical infrastructure?

Two have been drafted and under revisions:

1) *Regulation on the Protection of the Security of Critical Information Infrastructure* (Draft, 2017)
2) *Information Security Technology: Security Controls of Critical Information Infrastructure* (Draft, 2018)

▪ Definitions

82. How are national security and national defence defined?

National Security Law of the PRC (2015) defines national security as "a status in which the regime, sovereignty, unity, territorial integrity, welfare of the people, sustainable economic and social development, and other major interests of the state are relatively not faced with any danger and not threatened internally or externally and the capability to maintain a sustained security status."

National defence is not clearly defined.

83. How are cybersecurity and cyberdefence defined?

Cybersecurity Law of the PRC (2017) defines "cybersecurity" as "taking the necessary measures to prevent cyberattacks, intrusions, interference, destruction, and unlawful use, as well as unexpected accidents, to place networks in a state of stable and reliable operation, as well as ensuring the capacity for network data to be complete, confidential, and usable."

"Cyberdefence " is not defined.

84. How are threats to national security and cyberthreats defined?

No.

85. How is a cyberattack defined?

The *Specifications of Definition and Description for Network Attack* (2017) defines cyberattack as: "An act that uses computers, routers and other network equipment to takes advantage of loopholes and security deficiencies in a network in order to steal, revise, and destroy information in storage or transmission; to slow down or intercept network services; or to damage, destroy or control network infrastructures" (Article 4).

86. Does the national law provide any other definitions instrumental to the application of cyberdefence legislation?

Article 76 of the *Cybersecurity Law of the PRC* (2017) provided definitions for "network," "network security," "network operator," "network data," and "personal information."

▪ National Framework

87. Is cyberdefence grounded on the constitutional provisions and/or international law?

It is not explicitly stated in the related legal documents but generally assumed that cyberdefence is part of national defence and is grounded in the Chinese Constitution.

88. Which specific national defence measures are related to cybersecurity?

Article 25 of the *National Security Law of the PRC* (2015) provides general language about the importance of cyberdefence .

The *Cybersecurity Law of the PRC* (2017) provides general guidance for cybersecurity, but not cyberdefence per se. Different chapters of the law address state support and promotion for network security; guidelines for network operators, critical infrastructure and network information security; cybersecurity monitoring, forecasting, and emergency response; and legal responsibility of different actors.

89. Is there a national defence doctrine and does the law or strategy refer to it?

China's National Defence in the New Era (2019), a white paper released by the State Council Information Office of the PRC, provides more specific details for national defence issues (e.g. international security assessment, its "defensive" national defence policy, missions and reforms in China's national defence and armed forces, approach to defence spending, its vision for contribution to the international community) outlined in the *National Security Law of the PRC* (2015).

90. What measures are mentioned in the national law and strategy in order to implement cyberdefence ?

The State Council white paper *China's National Defence in the New Era* (2019) states: "Cyberspace is a key area for national security, economic growth and social development. Cyber security remains a global challenge and poses a severe threat to China. China's armed forces accelerate the building of their cyberspace capabilities, develop cyber security and defence means, and build cyber defence capabilities consistent with China's international standing and its status as a major cyber country. They reinforce national cyber border defence, and promptly detect and counter network intrusions. They safeguard information and cyber security, and resolutely maintain national cyber sovereignty, information security and social stability."

91. How can Internet users' online activities be limited for the reasons of protection of national security and cyberdefence ?

Article 12 of the *Cybersecurity Law* (2017) stipulates a wide range of user online activities can be limited for the sake of protecting national security and cyberdefence :

"Any person and organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they must not endanger cybersecurity, and must not use the Internet to engage in activities endangering national security, national honour, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts."

92. Does the national law or strategy foresee any special regime to be implemented in case of emergency in the context of cyberdefence ?

Chapter 5 of the *Cybersecurity Law* (2017) outlines the general guidelines for various entities including network operators, state agencies, provincial governments in the case of cybersecurity emergencies.

The State Council's white paper *China's National Defence in the New Era* (2019) affirms: "cooperation agreement in the sphere of identifying and cutting off the channels used by the individuals involved in terrorist, separatist and extremist activities to enter the Shanghai Cooperation Organization member states."

▪ Actors

93. What actors are explicitly mentioned as playing a role regarding cyberdefence in the law or national cyberdefence strategy or defence strategy?

The State Council's white paper *China's National Defence in the New Era* (2019) outlines the divisions of the People's Liberation Army (PLA) including army, air force, joint logistic support force, navy, rocket force and strategic support force (SSF). Among them, the SSF centralizes strategic space, electronic, cyber warfare missions.

94. Is there a specific cyberdefence body?

The Strategic Support Force (SSF) of the People's Liberation Army (PLA), formed in 2016.

95. What are the tasks of the aforementioned actors?

China's National Defence in the New Era (2019) asserts:

"The PLASSF is a new type of combat force for safeguarding national security and an important driver for the growth of new combat capabilities. It comprises supporting forces for battlefield environment, information, communications, information security, and new technology testing. In line with the strategic requirements of integrating existing systems and aligning civil and military

endeavours, the PLASSF is seeking to achieve big development strides in key areas and accelerate the integrated development of new-type combat forces, so as to build a strong and modernized strategic support force."

6. Cybersecurity in South Africa: Towards Best Practices

Sagwadi Mabunda

6.1.Introduction

Cybersecurity in South Africa is a topic that has been on the agenda for a number of years. The government has expressed great concern over the proliferation of cybersecurity risks. It asserts that cybersecurity threats and the combatting thereof have a personal, national and international dimension[352].

South Africa is experiencing the manifestations of the "digital paradox[353]". This is an acknowledgement of the opportunities that technological advances present to the development of the country on the one hand and the threats that are posed by the cybercriminals on the other hand. Essential services such as water and electricity supply rely heavily on ICT, so too do businesses, organisations and citizens. While ICT applications such as e-government, e-commerce, e-health and e-education are considered enablers of development, they are also vulnerable to the threats that present with the promise of technology particularly, in the form of rampant cybercriminality[354]. The digital paradox presents itself in the way that the potential of ICT for development is stifled or threatened by the proliferation of cybercrime and cybersecurity threats[355].

The South African government faces great challenges when it comes to regulating cybersecurity which include the coordination of cybersecurity activities and data protection across the whole government structure at the national, regional and municipal levels. It must also ensure the same level of coordination for independent agencies such as regulators, businesses, civil society, households and individuals[356]. While there are positive efforts being made, it is clear that much more needs to be done to improve; particularly when it comes to South Africa's Cybersecurity legislative frameworks.

The International Telecommunication Union (ITU) has developed the Global Cybersecurity Index (GCI) to measure the commitment of countries to cybersecurity at a global level. This index measures countries along five pillars – (i) legal measures, (ii) technical measures (iii) organisational measures (iv) capacity building and (v) cooperation. These pillars were adopted because cybersecurity has a broad field of application which cuts across various sectors and industries[357].

[352] See NCPF (2012) at 75.

[353] See DTPS(2017) at 3.

[354] See SABRIC (2018) at 1; Hubbard (2019) at 1.

[355] See Baseline Cybersecurity readiness report (2017) at 3.

[356] See Sutherland (2017) at 84.

[357] See ITU (2018) at 1.

According to the 2018 GCI report, South Africa was determined to be in the 56th place globally. To put that in perspective, when compared to the other BRICS countries it is in the fourth place before Brazil, which sits at 70th position globally, while Russia is 26th, followed by China at 27th and India at 47th. Regionally, South Africa is fourth behind Mauritius, Kenya and Rwanda which hold first, second and third place respectively; it is followed by Nigeria, Tanzania and Uganda which hold the fifth, sixth and seventh positions respectively[358].

Importantly, when considering the South African cybersecurity landscape, the National Cybersecurity Policy Framework (NCPF) is the first port of call. The NCPF was developed in line with the Justice Crime Prevention and Security (JCPS) Delivery Agreement which is aimed at ensuring that "all people in South Africa are and feel safe". Output 8, for example, seeks to foster integrated ICT systems that will combat cybercrime[359].

National cybersecurity per the NCPF is a broad term that encompasses many aspects of electronic information, data, and media services which affect the economy, security and wellbeing of a country[360]. Cybersecurity is defined as "the practice of making the networks that constitute cyberspace secure against intrusions, monitoring confidentiality, availability and integrity of information, detecting intrusions and incidents that occur, and responding to and recovering from them[361]". Therefore, the NCPF has identified that the most important policy domains are those that (1) address the reduction of vulnerabilities of cyberspace, (2) prevent cyber threats and attacks in the first instance, and (3) where an attack does occur, ensure the swift recovery and functioning of critical information systems[362].

Cyber threats necessitate a cybersecurity culture which is driven mainly by the State to ensure that citizens are able to take full advantage of the information age whilst remaining conscious of the threats and vulnerabilities that exist in cyberspace. In other words, the risks associated with ICT must be counterbalanced with its role in the functioning of modern and open societies[363].

As South Africa ventures into exploring the Fourth Industrial Revolution[364], an acute awareness of this balancing exercise is paramount. Achieving overall national cybersecurity is no small feat, the

[358] See ITU (2019) at 55.

[359] See South Africa Government (2010) at 1.

[360] See National Cybersecurity Policy Framework (2012) at 76.

[361] See National Cybersecurity Policy Framework (2012) at 73.

[362] See National Cybersecurity Policy Framework (2012) at 76.

[363] See National Cybersecurity Policy Framework (2012) at 76

[364] The 10th BRICS Summit: Johannesburg declaration was dedicated to the inclusivity and mutual prosperity in the context of technological developments and advancements. See The Presidency (2018) at 1.The President has appointed a commission on Fourth Industrial Revolution in April 2019. The commission is chaired by the President and will be responsible for identifying relevant policies, strategies and action plans to position South Africa as a competitive global player. See The Presidency (2018) at 1; Government Gazette General Notices (December 2018) at 18; DTPS (2019). Critics argue that South Africa is caught up in the hype of 4IR without giving due caution to the unfinished business of inequality and the preconditions that need to be created in order to have an inclusive digital economy and society. See Gillwald (2019) at 1.

government must ensure that the policies and regulations adopted do not take a myopic view, rather they should address the challenges particular to South Africa while keeping in mind its international obligations. While the NCPF may not be able to address every aspect of cybersecurity, it does pronounce on the critical areas such as data protection and privacy, cybercrime, interception of communication, and cyberdefence.

6.2. Data Protection

South Africa holds the right to privacy in very high esteem owing to the gross violations witnessed during the Apartheid regime. There is both a common law right to privacy[365] and a Constitutional right to privacy provided for in section 14.

Data protection is regulated by the Protection of Personal Information Act (POPI) which was passed in 2013. POPI, which is closely modelled after an early draft of the EU General Data Protection Regulation (GDPR), seeks to regulate (amongst other things) the processing of personal data, setting obligations for the data processors and controllers and enabling data subjects to bring civil actions against entities (both public and private) who violate their individual rights[366].

Section 39 of POPI establishes the Information Regulator as an independent juristic person for the purpose of enforcing POPI. While the office of the Information Regulator has been created, it is not yet fully operational due to administrative delays. Unfortunately, this means that while data subjects in South Africa have rights and protections under POPI, they are currently unenforceable.

It has become well established that the exponential advancements in technology have increased the capabilities of companies and other organisations to gather, store, process and disseminate personal data as people inadvertently leave a digital footprint as they use their mobile phones and computers[367].

POPI was the result of thorough research done by the South African Law Reform Commission (SALRC) which based the principles of the Act on the principles implemented by the Organisation of Economic Cooperation and Development (OECD) and the European Union[368]. It is also substantially similar to the United Kingdom's Data Protection Act (DPA). Those that have studied both Acts have noted that one can anticipate the impact that POPI will have in South Africa by investigating the impact that the DPA has had in the UK[369].

---

[365] See *O'Keefe v Argus Printing and Publishing (Pty) Ltd* 1954 3 SA 247 (C). Second Line of Defence (2018) SANDF Way Ahead: Priorities and Challenges" <https://sldinfo.com/2018/06/sandf-way-ahead-priorities-and-challenges/> Accessed 13 June 2019.

[366] See Sutherland (2017) at 95.

[367] De Bruyn (2014) 1318.

[368] Heyink (2011) at 2.

[369] De Stadler (2013) & Tubbs (2014).

It is anticipated that once POPI comes into full effect, it will have a significant impact on the ways that companies gather, save, utilise and distribute personal information. A 2014 study done by IQ business in conjunction with the South African Institute of Chartered Accountants (SAICA) predicted that in addition to civil and criminal liability that can attach to non-compliant companies, the possible reputational damage that can occur could be severely detrimental to the company's future[370].

Greenleaf argues that the key to effective data privacy law is in the adoption of a comprehensive set of data privacy principles which accord with international standards such as the OECD guidelines as well as having mandatory legal enforcement mechanisms in place[371]. Furthermore, data privacy laws should cover most of the country's private and public sectors in other words, they should not place their focus on a few subsectors such as "credit reporting" or "health[372]".

Greenleaf identifies ten principles which are at the core of data privacy and should be included in privacy legislation. These are: "1) fair data collection, 2) data quality, 3) purpose specification, 4) purpose notification when data are collected, 5) limitation to specified data uses, 6) reasonable security safeguards, 7) openness, 8) access and correction of an individual's data, 9) accountability of the responsible parties and 10) implementation or instruction of data export restrictions"[373].

POPI encompasses nine out of ten of these principles. Condition 1 deals with the principle of accountability of the data controller to implement and monitor adherence to the conditions of POPI. Condition 2 provides for the collection of private data which may only be done in a manner which is fair, lawful and within the knowledge and consent of the data subject. Condition 3 provides for the purpose specification which states that data must be collected for a specific use as well as requiring that the purpose be specified at the time of collection. Condition 3 also provides for the purpose and rights notification where the data subject must be notified that her data is being collected and what it will be used for. Condition 4 prohibits the excessive collection of personal data i.e. personal data may only be used or processed for the purpose that it was originally collected for. Condition 5 provides for the quality of data which must be accurate and relevant. Condition 7 provides for reasonable security safeguards which state that the necessary technical and procedural practices should be implemented so as to ensure the safety of personal data. Condition 8 provides the right of data subjects to know what information on them is stored and processed by the data controller. The data controller has the responsibility in that regard to affect any corrections the data subject may inform them of. Finally, chapter 9, section 72 provides for data export restrictions which states that cross-border data transfers may only be done to countries that have adequate data privacy legislation in place[374].

370 IQ Business (2014) 37.

371 Greenleaf (2013) 224-5.

372 Greenleaf (2013) 225.

373 De Bruyn (2014) 1319. See Greenleaf (2013) 237.

374 De Bruyn (2014) 1319.

These principles, properly applied, inform the implementation of the Act and ensure that it will be an effective law. While comparisons can be made with the UK DPA, the similarities should not be overstated because ultimately, the unique South African context will determine how successful the quest for data privacy it.

6.3. Consumer Protection

The South African National Consumer Protection Act (CPA)[375] seeks "to promote a fair, accessible and sustainable marketplace for consumer products and services … [and] to prohibit certain unfair marketing and business practices[376]". The Act does not have specifically formulated provisions that directly address cybersecurity issues. This is a missed opportunity considering today's increasingly digitized society.

One of the areas that the CPA could provide guidance on is with regard to the 'right to be forgotten'. On the back of the European Court of Justice judgment of *Google Spain v AEPD and Mario Costeja González*[377] the question becomes whether customers of multinational corporations such as Google can enforce that right in South Africa. Without pronouncing on the desirability or practicality of the right to be forgotten, South Africa would be an interesting case study given its strong privacy, access to information, and consumer protection values.

The right to be forgotten is typically spoken of in the context of the right to privacy[378]. The South African Constitution recognises the right to privacy as a fundamental right enshrined in the Bill of Rights and so it is encapsulated in all other rights. This is contemplated by section 39(2) of the Constitution which provides that "[w]hen interpreting any legislation … every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights." This means that when interpreting the consumer rights provided for in the CPA, due regard must be given to the right to privacy.

Currently, the CPA is limited as it only recognises the right to privacy when it comes to restrictions on unwanted direct marketing[379]. It may be argued that when a consumer uses the services of a supplier, she should have the right to have her personal information erased from the supplier's databases upon termination of their transactional relationship, subject, of course, to other legal obligations the supplier may have[380]. Unfortunately, this proposition is currently only theoretical as it has not yet played out in the courts, but one can postulate that a court would be in favour of finding

---

375 See Consumer Protection Act No 68 of 2008.

376 See Preamble of the CPA, (2011). <https://www.gov.za/sites/default/files/gcis_document/201409/321864670.pdf>. Accessed 30 October 2019.

377 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, ECLI:EU:C:2014:317.

378 See Basson (2015).

379 See Section 11 of CPA.

380 These obligations may include, for example, being required to retain information for a prescribed time frame during an investigation.

that a consumer does have a right to be forgotten, particularly given that the CPA recognise a consumer's right to be heard and obtain redress[381].

6.4. Cybercrime

It is important to stress that Africa was the last continent to embrace ICTs, and a decade ago only a handful of African countries had local Internet access[382]. There has been since a significant growth in the adoption of ICTs across sub-Saharan Africa. However, this occurred in the context of inadequate telecommunication infrastructures[383].

The endless possibilities created by Internet connectivity for millions across the continent have created also unlimited capabilities for those tied to the criminal world. Those who wish to engage in criminal activities have taken full advantage of the internet's power to commit a host of cybercrimes[384]. However, expanding bandwidth and increases in the use of wireless technologies and infrastructures have been coupled with high levels of computer illiteracy and insufficient or ineffective regulatory measures, making African countries especially vulnerable to cybersecurity breaches[385].

South Africa is no stranger to cybercrime attacks and the NCPF reinforces the need to take progressive steps to combat it. It notes a need to promote, guide and coordinate activities that would be aimed at improving cybersecurity measures which include the fight against cybercrime. These measures include ensuring that the collection of intelligence is strengthened and the state's capacity to investigate, prosecute and combat cybercrime (amongst other threats) is improved[386].

Parliament has been working on passing South African Cybercrimes legislation since 2015. The first attempt at a draft bill was unsuccessful as it appeared to have tried to do too much. As stated above, the first draft sought to regulate cybercrime and cyberdefence issues. It was overly broad and practically unenforceable. The bill consequently saw two major revisions to become the Cybercrimes Bill that is currently being debated in parliament. It is anticipated that it may get signed into law very soon.

6.5. Interception of Communications

Interception of communication is a core pillar of the preservation of national public order in South Africa and is regulated by the Regulation of Interception of Communication and Provision of

[381] See Section 68(1) of CPA. It is worth noting however, that this right too is limited as it applies only to the rights that are provided for in the Act. Should one wish to rely on this provision to claim a right to be forgotten, one would need to engage in a section 39(2) interpretation exercise.

[382] See Longe (2009) at 155.

[383] See Longe (2009) at 156.

[384] See Stander (2009) at 217.

[385] See Grobler (2012) at 1.

[386] See National Cybersecurity Policy Framework (2012) at 81.

Communication-Related Information Act (RICA). RICA was enacted in 2002 to address what was understood to be the nature of the telecommunications environment at that time. This environment has evolved significantly 17 years on.

It is stated in the preamble that the purpose of the Act is to regulate the interception of certain communications and other communication-related information. It also seeks to regulate the processes of application for, issuing of and directions authorizing interception of communications. It also establishes interception centres, the Office for Interception Centres and the Internet Service Providers Assistance Fund. Its goal is also to protect the privacy of communications subject to certain exceptions in the case of serious crimes or threats to national threats.

One of the features of RICA is that an electronic communication service provider who provides a mobile cellular electronic communications services is prohibited from activating a SIM card on its electronic communication system unless it has recorded and stored (at its own cost) the Mobile Subscriber Integrated Service digital Network Number (MSISDN-number) of the SIM card against the details of the customer along with their full name, identity number and at least one address[387]. This information becomes essential when it comes to the need for security forces to intercept communication. A controversial issue which played out in Court, as explained in the following section.

6.5.1. Amabhungane v Minister of State Security

On the 16th of September 2019, the High Court of South Africa Gauteng Division, Pretoria delivered a judgment per Sutherland J in the case of Amabhungane and Others v The Minister of State Security and Others[388] which declared parts of RICA unconstitutional. The declaration of invalidity was suspended for two years to allow the legislature to remedy the defects of the Act.

The High Court found that there were several examples of abuse of RICA by the respondents which included undisputed first-hand experience of investigative journalist Sam Sole and Advocate Down, a State Prosecutor, of being spied upon. Furthermore, it stated that Mr Sole has no right under RICA to demand disclosure because it forbids him from being informed. His efforts to obtain details about the spying were met with a contemptuous response and unsubstantiated allegations that no irregularities have occurred[389]. Although the Respondents has claimed that because RICA was undergoing some developmental changes, the challenge was abstract and not based on a set of fact, the Court found that the irregularities noted above alone were good enough reason to hear the matter.

The controversy that shrouded RICA was centred around the question of what effect the authorisation of interceptions has on the rights conferred by the Constitution, namely the section 14 privacy rights,

[387] See Section 40(1)-(2) of RICA, (2002).

[388] See *Amabhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* (25978/2017) [2019] ZAGPPHC 384 *(Amabhungane).*

[389] See Amabhungane paras 18-9.

section 16(1) freedom of expression rights, section 34 access to court rights and section 35(5) fair trial rights[390]. While it is common cause that RICA and bulk interceptions practice is an intrusion on privacy rights, the controversial issue was whether the infringement could be justified in terms of section 36 and section 39 of the Constitution[391].

Two discrete issues were raised.

1) The first was a challenge to the constitutionality of parts of RICA. The statute permits the interception of communications of any person by authorised state officials subject to the conditions prescribed in the Act.
2) The second was whether there exists lawful authority for the admitted practice of the State in conducting 'bulk interceptions' of telecommunication traffic. The National Strategic Intelligence Act 30 of 1994 and the Intelligence Services Control Act 40 of 1990 were implicated in this issue[392]. For the sake of brevity, this second issue will not be discussed here.

The Court considered the first challenge with reference to the following considerations:

---

390 The Constitutional provisions are –
Section 14. Privacy
Everyone has the right to privacy, which includes the right not to have-
(a) their person or home searched;
(b) their property searched;
(c) their possessions seized; or
(d) the privacy of their communications infringed.
Section 16(1) Freedom of expression
Everyone has the right to freedom of expression, which includes-
(a)freedom of the press and other media;
(b) freedom to receive or impart information or ideas;
(c) freedom of artistic creativity; and
(d) academic freedom and freedom of scientific research.
Section 34 Access to courts
Everyone has the right to have any dispute that can be resolved by the application of law decided in a fair public hearing before a court or, where appropriate, another independent and impartial tribunal or forum.
Section 35(5) Right to a fair trial
Evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice.

391 The Constitutional provisions are –
Section 36. Limitation of rights
(1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including –
(a) the nature of the right;
(b) the importance of the purpose of the limitation;
(c) the nature and extent of the limitation;
(d) the relation between the limitation and its purpose; and
(e) less restrictive means to achieve the purpose.
(2) Except as provided in subsection (1) or in any other provision of the Constitution no law may limit any right entrenched in the Bill of Rights.
Section 39 Interpretation of Bill of Rights
(1) When interpreting the Bill of Rights, a court, tribunal or forum –-
(a) must promote the values that underlie an open and democratic society based on human dignity, equality and freedom;
(b) must consider international law; and
(c) may consider foreign law.
(2) When interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights.
(3) The Bill of Rights does not deny the existence of any other rights or freedoms that are recognised or conferred by common law, customary law or legislation, to the extent that they are consistent with the Bill.

392 See Amabhungane at paras 2-3.

a) The Act does not afford a right of notice to a person who has been surveilled of such surveillance.

The Court held that once it is assumed that secret surveillance is justifiable, the controversy presents when one considers the possibility of abuse by overzealous or corrupt officials. Without the right to notice, a subject of surveillance whose privacy has been wrongly violated has no recourse for relief in the courts. This means that her right to access to court as contemplated in section 34 of the Constitution would have been compromised as it is critically instrumental to the right to access to courts, for without a right, there can be no remedy[393].

The challenge supposed that the purposes of RICA could be achieved without a total ban on post-surveillance disclosure whereas the respondents stood fast on the need for a total ban. The Court, after considering foreign legal precedence[394], embraced the right to post-surveillance notice as a facet of a democratic social order, subject to the safeguards against undoing the very objective of legitimate surveillance[395]. It found that there is no reason in the South African condition to deny such a right[396].

The Court found that RICA, including sections 16(7), 17(6), 18(3)(a), 19(6), 20(6) and 22(7), is inconsistent with the Constitution and accordingly invalid to the extent that it fails to prescribe a procedure for notifying the subject of the interception. In an interim order, the Court read into sections 16(11) and (12) the right to notification[397].

b) The model of safeguards in respect of the selection of the designated judges is deficient.

Section 16 of RICA provides for the procedure that must be followed for application for, and issuing of, directions and entry warrants to a designated judge. Section 16(4) – (7) stipulates the duties of a designated judge[398].

The safeguard model was criticised by the applicants in two respects; the first was that the independence of the designated judge is compromised by the selection process and the *de facto* unlimited duration of appointment, and second, that the absence of an adversarial process may compromise the efficacy of the judicial role[399].

---

393 See Amabhungane at para 43.

394 The Court considered the jurisprudence of the European Court of Human Rights which recognises a post surveillance model that complies with article 8 of the European Convention of Human Rights. It also found that in Germany, as in the USA and Japan, a right to a notification is mandatory when it is safe to do. See *Klass v Germany ECHR* [1978] 5029/71 and *Weber & Saravia v Germany* [2008] 46 EHRR SES; [2006] ECHR 1173 at [51] and at [133-135]. In Russia however, there is no such right and so in the case of Zakharov, it was held to be in violation of Article 8. See *Zakharov v Russia* [2016] 63 EHRR 17 at [289] – [291] and [298] – [302].

395 See Amabhungane at para 51.

396 See Amabhungane at para 51.

397 See Amabhungane at para 53.

398 See Section 1 of RICA defines a designated judge as a "any judge of a High Court discharged from active service… or any retired judge, who is designated by the Minister [of the administration of justice or state security] to perform the functions of a designated judge for purposes of this Act."

399 See Amabhungane at para 61.

The applicants sought an interim order which read into the definition of a designated judge that she should be appointed by the Judicial Services Commission for a non-renewable term of two years. The Court held that such an order would not be appropriate in the interim. It held that the Minister should continue to appoint the designated judge but that she or he should be nominated by the Chief Justice and the Minister should be obliged to accept the nomination. The appointment should be for a non-renewable term of two years[400].

The second part of the challenge was the absence of a prescribed procedure for the proper evaluation of the evidence placed before the designated judge in keeping with the adversarial tradition of the South African judicial system. This, it was argued, implicates the section 34 rights to a fair hearing and excludes *audi alteram partem*. The applicants argued for the introduction of a public advocate to play the role of devil's advocate, something which is not a default position in South Africa. This would allow the designated judge to have the benefit of hearing the matter ventilated by two opposing parties so she can apply her mind to the final decision fully[401].

The Court found that RICA is inconsistent with the Constitution in as far as it fails to provide a system for appropriate safeguards to deal with *ex parte* orders. It held, however, that there are a number of considerations that must be factored in when determining what the appropriate safeguards should be, therefore, it elected to leave that to Parliament. The declaration of invalidity is suspended for two years[402].

c) The model of safeguards concerning custody and management of information gathered by surveillance is deficient.

RICA provides for two types of interception of communication; the first is real-time interception, and the second, is trawling through past data. Telecommunications service providers are obliged to retain all data in terms of section 30(2) of RICA, between a minimum of three and a maximum of five years at their own discretion.

The applicants argued that the minimum three-year period is too long for service providers to archive data because that period is not reasonably connected to a legitimate objective of RICA. Other jurisdictions prescribe, at most, a two-year period. Secondly, having accessed and stored these data in servers at Interception Centres, the regulations on how those data are used and managed, i.e. stored and transferred, are unsatisfactory[403].

The Court, while recognising other jurisdictions, held that there is no injustice done to the limitations enquiry by recognising that there may be disagreements what may be deemed as a reasonable period

[400] See Amabhungane at para 70-1.

[401] See Amabhungane at para 72.

[402] See Amabhungane at para 82.

[403] See Amabhungane at para 89.

length. It held that while a period of five years may seem excessive when emphasis is given to comparative jurisdictions; it is not inconsistent with section 36 of the Constitution[404].

However, on the second issue, the Court held that RICA, especially section 35 and 37, are inconsistent with the Constitution and accordingly invalid for two years (to allow Parliament to cure the defect) to the extent that the statute itself fails to prescribe proper procedures to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions.

The alleged shortcomings in the RICA of the model of safeguards to effectively:

Preserve legal privilege in respect of lawyers and their clients, and,

Preserve the confidentiality of the sources of investigative journalists[405].

It was uncontested that both lawyers and journalists have obligations to preserve confidential information. The issue, however, is whether their confidential exchanges, either in absolute or in relative terms, ought to be prevented. It is also accepted that the right to privacy is not absolute, but the question is whether interception impacts on their professional roles and the efficacy with which those roles are performed[406].

The Court distinguished between the role of a lawyer and that of a journalist and dealt with each discreetly. It held that the conditions and restrictions imposed by the Act are the appropriate mechanisms to manage intrusions on lawyers[407]. With regard to journalists, the Court held that the absence of express provisions which instruct the designated judge to examine the justifications presented to her for spying on journalists is evidence of the failure of RICA to align with section 16 of the Constitution, which makes RICA unconstitutional[408].

Overall, this case highlights the difficulties that present with the interception of communications. The Courts have to balance competing interests carefully with a perfect understanding of the impact that each will have. This was a very complex case which the Court dealt with skilfully and tellingly illustrates the pivotal role that the Courts play, as there will always be tensions between the rights of citizens and the obligations of the State with regard to cybersecurity.

6.6. Cyberdefence

At the South African level, the Department of Defence and Military Veterans has been given the overall responsibility for coordination, accountability, and implementation of cyberdefence measures

[404] See Amabhungane at paras 94-5.

[405] See Amabhungane at para 26.

[406] See Amabhungane at paras 110-2.

[407] See Amabhungane at paras 114-128.

[408] See Amabhungane at para 140.

as an integral part of its National Defence mandate. The first draft of the 2015 Cybercrimes Bill was called the Cybercrimes and Cybersecurity Bill. Subsequent drafts of the Bill did away with the cybersecurity section of the Bill, electing to limit the scope of the Bill to Cybercrimes so as to not encumber it with too much. The drafters decided it would be better to enact a separate Cybersecurity Bill which would deal with issues pertaining to cyberdefence and cyberwarfare.

As of 2016, a cyberwarfare strategy was said to be in the advanced stages of development, having been submitted to the Chief of the South African National Defence Force[409]. It was earmarked for approval and partial implementation in the 2018/2019 fiscal year[410]. The cyberdefence strategy seeks to ensure the military's readiness to continue operating at an optimal level should it come under a cyber-attack of any kind. It should also have the capability and capacity to not only launch conventional attacks, but also cyber-attacks[411].

The cybersecurity strategy must ensure national security and elevate efforts for protecting critical information infrastructure. These efforts must be on par with traditional defence interests[412]. While the NCPF is the overarching cybersecurity strategy, and although this is not prescribed by the law, it may need to be updated as more research is conducted about South Africa's vulnerabilities to cyberwarfare, for instance.

Importantly, Sutherland remarks that the Department of Defence offers very little indication of possible threats that may exist or where they would be likely to originate from. Therefore, it is arguable whether cyberwarfare is even a real threat to South Africa that would necessitate a cyberwarfare strategy or dedicated cyberdefence legislation. Nevertheless, it is conceivable that there may be some States which may wish to attack South Africa with the aim of destabilising its government, although this is somewhat unlikely[413]. Even if a majority of the cyber-attacks that South Africa could experience might not emanate from hostile nations, a cyberdefence and cyberwarfare strategy is nevertheless essential should the need arise someday.

6.7. Cybersecurity Best Practices

The NCPF urges civil society, government and the private sector to play their part in fostering a cybersecurity culture inter alia, implementing cybersecurity awareness programmes; supporting

[409] See Department of Defence (2015a); Department of Defence (2015b) <http://www.dod.mil.za/documents/annualreports/DoD%20Annual%20Performance%20Strat%20Plan%202403.pdf>. Accessed 30 September 2019.

[410] See Second Line of Defence (2018) at 1

[411] See National Cybersecurity Policy Framework (2012) at 94.

[412] See National Cybersecurity Policy Framework (2012) at 76.

[413] See Sutherland (2017) at 93.

outreach to civil society, children and individual users; updating and reviewing existing privacy regimes; and so forth[414].

The Cybersecurity Hub[415] is a key feature of the NCPF. It has been created to conduct cybersecurity audits, assessments and readiness exercises. It is also responsible for providing best practices guidance on ICT security for Government, business and civil society, as well as initiate cybersecurity awareness campaigns[416]. Additionally, it seeks to facilitate the creation of additional sector-specific Computer Security Incident Response Teams (CSIRTs) that will, in addition to conducting sector cybersecurity audits, assessments and readiness exercises, provide best practice guidance on ICT security[417].

In 2017, the Department of Telecommunications and Postal Services (DTPS), through the Cybersecurity Hub, engaged in a nationwide survey that sought to gather information about the cybersecurity readiness of South African organisations. It reported on the dearth of reliable data in South Africa from organisations both in the private and public sectors and found that where there is data available, much of it is anecdotal[418].

The aim of that survey was to gather information about the status of cybersecurity plans in organisations, identify cybersecurity vulnerabilities, determine the capability of organisations to respond to and recover from cybersecurity-related attacks and to survey the status of cybersecurity governance in organisations[419].

The report identified that the top three challenges that the organisations face were insufficient skills, lack of in-house skills and lack of awareness. It also identified that of the organisations surveyed, only 45% belonged to CSIRT and only 22% of them were obliged to report incidents. Furthermore, only 25% of the surveyed respondents reported that they had threat intelligence capabilities, whereas, 20% indicated that this was in development[420]. The report did note, however, that there appears to be a decrease in the number of incidents that have been reported between 2016 and 2017 by 47%. Furthermore, 29% of the organisations indicated that they had fully functioning cybersecurity plans while 37% of them indicated that they had discussed a cybersecurity plan which they would implement in the future[421].

---

414 See National Cybersecurity Policy framework (2012) at 25.

415 See Cybersecurity Hub at <https://www.cybersecurityhub.gov.za/>. Accessed 30 October 2019.

416 See National Cybersecurity Policy Framework (2012) at 18.

417 See National Cybersecurity Policy Framework (2012) at 19.

418 See Baseline Cybersecurity readiness report (2017) at 5.

419 See Baseline Cybersecurity readiness report (2017) at 10.

420 See Baseline Cybersecurity readiness report (2017) at 13.

421 See Baseline Cybersecurity readiness report (2017) at 5.

A majority of the respondents interviewed in the cybersecurity readiness survey indicated that they align to international standards[422] such as to the International Organisation for Standards (ISO) 27001 family of standards[423]. A third aligned with the National Institute of Standards and Technology (NIST)[424] and SANS standards[425].

It is worth mentioning that the banking industry in South Africa appears to be the one with more progressive regulations when it comes to cybersecurity[426]. Data protection is of particular interest. The South African Reserve Bank's Prudential Authority has issued a number of directives that outline the measures that banks need to adopt or implement so as to ensure compliance with domestic and international obligations.

One of the directives issued by the Prudential Authority was the directive on cloud computing and offshoring of data[427] which was issued in terms of section 6(6) of the Banks Act[428] to all banks, controlling companies, branches of foreign institutions and auditors of banks or controlling companies (collectively referred to as banks).

The aim of the directive is to clarify the South African Reserve Bank's (SARB) policy and regulatory stance on cloud computing and offshoring of data. Banks are increasingly extending their use of cloud computing to more significant activities such as offshoring their data through an insourcing relationship with a parent company, for example[429]. To this end, banks are expected to follow a risk-based approach when implementing cloud computing and/or offshoring of data. Banks are encouraged to consider of critical importance their risk, risk appetite, due diligence, compliance, ensuring the protection of confidentiality, integrity and availability of their systems. They must also have

[422] See Baseline Cybersecurity readiness report (2017) at 27.

[423] The ISO 27001 family of standards set of best practices and recommendations for information security management and risk management through security controls. These standards have a wide scope which covers confidentiality, privacy and the technical aspects of cybersecurity. They can also be applied to organisations of different sizes and industries. See <https://www.iso.org/isoiec-27001-information-security.html>. Accessed 30 October 2019.

[424] The NIST standards are also popular amongst international organisations. They were created in a collaborative effort between industry and governments. They entail guidelines, standards and practices which are aimed at protecting critical information infrastructure. See <https://www.nist.gov/cyberframework>. Accessed 30 October 2019.

[425] The SANS institute serves as a resource for the security community. It seeks to aid in the development and implementation of security policies and guidelines for cybersecurity. It has a number of training programmes. See for example <https://cyber-defence .sans.org/>. Accessed 30 October 2019.

[426] The South African Banking Risk Information Centre (SABRIC) is an example of an organisation that seeks to collect information and educate the financial services industry of the latest scams and fraudulent activities that affects them. See <https://www.sabric.co.za/>. Accessed 30 October 2019.

[427] Cloud computing is defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage facilities, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Offshoring refers to "the storage and/or processing of data outside the borders so South Africa".

[428] No 94 of 1990.

[429] See South African Reserve Bank Prudential Authority (2018a) at 1.

contingency plans and measures to ensure that intellectual property and contractual rights are not compromised.

Some of the best practices identified by the DTPS in the cybersecurity readiness report include the following:

6.7.1. Membership in a CSIRT[430]

Membership in a sector CSIRT is essential for developing a good cybersecurity culture within organisations. CSIRTs that are dedicated to a particular sector or industry can play an integral role in information gathering particular to that sector and coordinate response efforts. Cooperation between organisations, networking and sharing of incident information enhances organisations' capabilities when it comes to correcting weaknesses[431].

Creating a CSIRT level obligation to reporting of cybersecurity incidents is essential. In many cases, many organisations shy away from reporting cybersecurity breaches because of a fear of losing public trust. This is unhelpful because it creates an environment where a threat is able to thrive from one organisation to the other, whereas, if it had been reported immediately, other organisations in the sector would have been warned and given an opportunity to proactively protect themselves.

6.7.2. Cybersecurity Awareness Training

There is immense value in creating a proactive cybersecurity culture as opposed to one that is constantly reactive. A constant challenge faced by South African industries is an overall lack of awareness about the kinds of threats that exist. When asked whether organisations provide cybersecurity awareness training, 57% stated that they do, while 29% were not certain[432].

It is common for the cybersecurity awareness responsibilities to be shouldered by the IT department for example, even though networks, systems and devices in organisations are typically interconnected resulting in the weaknesses in one department negatively affecting another.

6.7.3. Upskilling of Staff

Cybersecurity training must not end with awareness training. It is necessary for employees to be up-skilled consistently. In this regard, it might be necessary to either outsource training programmes or to enrol employees in organisation-funded cybersecurity awareness and capacity building courses, and certifications which will ensure that they are prepared and up to date with the latest trends in cybersecurity. The cybersecurity readiness survey revealed that 61% of the organisations surveyed

[430] See Baseline Cybersecurity readiness report (2017) at 29.

[431] See Baseline Cybersecurity readiness report (2017) at 29.

[432] See Baseline Cybersecurity readiness report (2017) at 31.

had in-house training whereas 8% used external vendors and 4% used affiliated organisations. 10% provided no training at all[433].

Organisations must acknowledge the different skill levels that employees have and provide targeted training which meets their needs. In this perspective, 27% of the organisations reported that they offered beginner training, 25% offered hybrid training, 19% offered intermediate training and only 5% offered advanced training[434].

6.7.4. Identifying Threat Actors and Targets

It is difficult to adopt a comprehensive cybersecurity policy without a clear picture of the kinds of threats and threat actors that exist. Given that many organisations may not have big enough budgets to dedicate to comprehensive cybersecurity policies, it is even more important to prioritise how funds are allocated. It would be counterproductive, for example, for an organisation to dedicate 60% of its cybersecurity budget to creating a comprehensive strategy to defend against cyberwarfare and cyberterrorism when its greatest threat actors are its employees who may steal data for fraudulent purposes.

For any organisation to have effective response mechanisms to cybersecurity, it must know the kinds of threats and threat actors that it must contend with. The cybersecurity readiness report revealed that the majority of threat actors in South African organisations are employees[435] (69%) and criminals (64%). Other cybersecurity threat actors were contractors (41%), lone hackers (40%) and hacktivist groups (39%)[436].

It was clearly shown in the cybersecurity readiness report that employees pose a bigger threat to an organisation than external actors because they tend to be more difficult to detect and they are hard to defend against because they already have legitimate access to systems and networks.

6.7.5. Incident Response

Incident response is defined as "an organisation's ability to deal with a situation in which company infrastructure and technology is being attacked and requires action to limit the damage, cost and effects of the incident[437]." A majority of the respondents (64%) indicated that their organisations were in a position to respond to threats whereas 23% were uncertain of their capacity[438].

---

433 See Baseline Cybersecurity readiness report (2017) at 33.

434 See Baseline Cybersecurity readiness report (2017) at 32.

435 Employees can be threat actors either through a lack of skills and knowledge about cybersecurity or through active perpetration through fraud, leaking or theft of data.

436 See Baseline Cybersecurity readiness report (2017) at 41.

437 See Baseline Cybersecurity readiness report (2017) at 42.

438 See Baseline Cybersecurity readiness report (2017) at 42.

When implementing an incident response strategy, organisations must determine how quickly they can recover after a serious incident or disaster. They need to determine the amount of downtime they can 'afford', how quickly they can recover and how much money they can lose. Thereafter, they must take the necessary measures to offset those risks.

6.7.6. Frequent Risk Assessments

One of the best ways to ensure up-to-standard incident responses is to have frequent risk assessments. Risk assessment studies are useful to help an organisation identify whether the cybersecurity controls that it has implemented are appropriate to deal with certain cybersecurity risks[439].

The cybersecurity readiness report showed that just over one-third of organisations (36%) carry out annual risk assessments, whereas 20% are doing a risk assessment more than once a year. It also showed that 14% of the organisations were uncertain of when risk assessments are undertaken and 4% of the organisations do not do formal risk assessments at all[440].

The frequency of the risk assessment will depend on the particular needs of the organisation. The frequency of the risk assessments will also be in line with the risk appetite that the organisation has. For example, financial institutions may need to conduct risk assessments more frequently than a research institute would. Membership to a sector CSIRT may also influence the frequency with which risk assessments are conducted as organisations may be subject to certain prescribed industry norms and standards.

6.8. Conclusion

What can be observed from this discussion is that in order for any cybersecurity strategy to be effective, it must be created with a holistic view in mind, it needs to be a deliberate and well-intentioned exercise regardless of whether it is on a national or organisational level. Both the government and individual organisations need to understand that effective cybersecurity strategies cannot and should not be implemented piecemeal. Those creating the strategies need to instil a culture of collective responsibility.

Governments and organisations must be encouraged to think about cybersecurity in a way that transcends their individual needs. They must act with a global perspective that is cognisant of their international rights and obligations. This means that measures such as intelligence gathering and information sharing must be seen as a collective responsibility that is mutually beneficial. Citizens and customers may also be more inclined to trust them if they admit security breaches and share their experiences with others in an effort to foster greater resistance to cybersecurity threats.

---

439 See Baseline Cybersecurity readiness report (2017) at 37.

440 See Baseline Cybersecurity readiness report (2017) at 37.

South Africa still has a long road ahead of it when it comes to comprehensive and effective cybersecurity measures, but it is on the right track. Although there is a great dearth of empirical research on its cybersecurity readiness, there is an awareness of the problem and a need to address it expeditiously. South Africa is known for having good legislation and policies on many issues, such as the Cybercrimes Bill and POPI, however, its greatest challenge is always implementation. It is up to the public and private sectors to work together to and take collective responsibility for fostering a constructive cybersecurity culture.

6.9. References

Amabhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services (25978/2017) [2019] ZAGPPHC 384.

Basson A (2015) "The Right to be forgotten: a South African perspective" Masters Dissertation, University of Pretoria.

Department of Defence. (2015a). South African defence review. Pretoria. Available at <http://www.dod.mil.za/documents/defencereview/Defence%20Review%202015.pdf>. Accessed 30 September 2019.

Department of Defence. (2015b). Department of Defence strategic plan for 2015 to 2020. Pretoria. Available at <http://www.dod.mil.za/documents/annualreports/DoD%20Annual%20Performance%20Strat%20Plan%202403.pdf. Accessed 30 September 2019.

Department of Telecommunications and Postal services "A baseline study on Cybersecurity readiness" (2017). Available at <https://www.cybersecurityhub.gov.za/images/docs/Cyber-Readiness-Report.pdf>. Accessed 30 September 2019.

Department of Telecommunications and Postal Services "Annual Performance Plan" (2019-2020) available at <https://www.dtps.gov.za/index.php?option=com_phocadownload&view=category&download=694:annual-performance-plan-2019-020&id=111:annual_performance_plans&Itemid=453>. Accessed 30 September 2019.

Gillwald A (2019) "South Africa caught up in the global hype of the Fourth Industrial Revolution" Mail & Guardian available at <https://mg.co.za/article/2019-08-26-south-africa-is-caught-in-the-global-hype-of-the-fourth-industrial-revolution>. Accessed 15 October 2019.

Global Cybersecurity Index (2019) 55. Available at <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf>. Accessed 30 September 2019.

Government Gazette General Notices (December 2018) available at <http://www.gpwonline.co.za/Gazettes/Gazettes/MonthyIndexDecember2018.pdf>. Accessed 15 October 2019.

Greenleaf, G. (2013a). Chapter 10: Data protection in a globalised network. In Brown, I. [ed]. Research handbook on governance of the Internet. Northampton, MA: Edward Elgar. p221- 259.

Grobler M., van Vuuren J.J., Leenen L. (2012) Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward. In: Hercheui M.D., Whitehouse D., McIver W., Phahlamohlaka J. (eds) ICT Critical Infrastructures and Society. HCC 2012. IFIP Advances in Information and Communication Technology, vol 386. Springer, Berlin, Heidelberg

Hubbard J (2019) "SA business underplaying the danger of cybercrime?" Fin24 available at <https://www.fin24.com/Finweek/Business-and-economy/sa-business-underplaying-the-danger-of-cybercrime-20190313 [accessed 15 October 2019].

International Telecommunication Union's (ITU) Global Cybersecurity Index (2018) 1. Available at <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>. Accessed 30 September 2019.

Longe, O; Ngwa, O; Wada, F; Mbarika, V (2009). "Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives". Journal of Information Technology Impact, vol. 9, n. 3, pp. 155-172. Available at <https://www.researchgate.net/profile/Lynette_Kvasny/publication/228876250_Criminal_Uses_of_Information_Communication_Technologies_in_Sub-Saharan_Africa_Trends_Concerns_and_Perspectives/links/00463524215d1ce6c7000000/Criminal-Uses-of-Information-Communication-Technologies-in-Sub-Saharan-Africa-Trends-Concerns-and-Perspectives.pdf>.

O'Keefe v Argus Printing and Publishing (Pty) Ltd 1954 3 SA 247 (C). Second Line of Defence (2018) SANDF Way Ahead: Priorities and Challenges" <https://sldinfo.com/2018/06/sandf-way-ahead-priorities-and-challenges/>. Accessed 13 June 2019.

South Africa Government (2010) Justice Crime Prevention and Security (JCPS) delivery agreement <https://www.gov.za/media-statement-justice-crime-prevention-and-security-jcps-delivery-agreement>. Accessed 14 June 2019.

South African Banking Risk Information Centre (SABRIC) "Annual Crime Stats" (2018) available at <https://www.sabric.co.za/media-and-news/press-releases/sabric-annual-crime-stats-2018/>. Accessed 15 October 2019.

South African Constitution Act 108 of 1996.

South African Cybercrimes Bill [B6B-2017] (2017).

South African Reserve Bank Prudential Authority (2018a) 'Cloud computing and offshoring of data' directive D3/2018.

South African Reserve Bank Prudential Authority (2018b) "Guidance Note on computing and offshoring of data."

South African State Security Agency "National Cybersecurity Policy Framework" (2012) Government Gazette No. 39475. Available at <https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf>. Accessed 30 September 2019.

Stander, A; Dunnet, A; Rizzo, J. "A Survey of Computer Crime in South Africa", Proceedings of ISSA 2009 conference, pp. 217-226, (2009).

Sutherland E (2017) Governance of cybersecurity – the case of South Africa. The African Journal of Information and Communication (AJI) 20 at 93.

The Presidency (2018) "10th BRICS Summit: Johannesburg declaration" available at <http://www.thepresidency.gov.za/press-statements/10th-brics-summit%3A-johannesburg-declaration>. Accessed 15 October 2019.

The Presidency (2019) "President appoints commission on Fourth Industrial Revolution" available at <http://www.thepresidency.gov.za/press-statements/president-appoints-commission-fourth-industrial-revolution>. Accessed 15 October 2019.

Annex

Country Report: South Africa

1. Data Protection

▪ Scope

1. What national laws (or other type of normative acts) regulate the collection and use of personal data?

The Electronic Communications and Transactions Act, 25 of 2002. The Protection of Personal Information Act 4 of 2013. This Act has been signed into law, but it has not yet come into effect.

2. Is the country a part of any international data protection agreement?

No.

3. What data is regulated?

Section 4 of ECTA provides that this Act applies in respect of data relating to economic transactions which are defined as transactions of either a commercial or non-commercial nature, and includes the provision of information and e-government services. It also applies to data messages which are defined as data generated, sent, received or stored by electronic means.

POPI Act

Chapter 2, Section 3 "Application and interpretation of Act" explains that the POPI Act applies to the processing of personal information.

4. Are there any exemptions?

ECTA Act does not apply to any data which falls outside the definition of electronic transactions and data messages.

Chapter VIII of the Act provides for the protection of personal information which is limited to personal information which has been obtained through electronic transactions. Section 51(2) provides that a data controller may not electronically request, collect, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.

5. To whom do the laws apply?

This law was created for the public interest. The Act seeks to regulate electronic transactions between consumers, private and public bodies, institutions and citizens **(Section 2(1)(g) of ECTA).** It also seeks to promote SMMEs (Small, medium and Micro-sized Enterprises) within the electronic transactions environment. **(Section 2(1)(p) of ECTA).**

Chapter 2 section 3 of POPI Act

Applies to responsible party domiciled in South Africa and if not domiciled in South Africa, which makes use of automated or non-automated means in South Africa.

6. Do the laws apply to foreign entities that do not have physical presence in the country?

Not directly. According to the rules of jurisdiction of the courts, a foreign entity would only be held liable only as far as the effects of the conduct is felt in the Republic.

However, any service provider must be accredited and authenticated if they offer products or services in a foreign jurisdiction by the Minister.

- **Definitions**

7. How are personal data defined?

ECTA Definitions

"personal information" means information about an identifiable individual, including, but not limited to:

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol, or other particular assigned to the individual;

(d) the address, fingerprints or blood type of the individual;

(e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;

(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the individual;

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years;

POPI

Personal information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person including, but not limited to:

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature of further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure if the name itself would reveal information about the person.

8. Are there special categories of personal data (e.g. sensitive data)?

POPI Part B: Processing of special personal information

Section 26 of the POPI Act provides:

A responsible party may, subject to section 27, not process personal information concerning:

(a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

(b) the criminal behaviour of a data subject to the extent that such information relates to:

(i) the alleged commission by a data subject of any offence; or

(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

Section 28: Authorisation concerning data subject´s religious or philosophical beliefs

Section 29: Authorisation concerning data subject´s race or ethnic origin

Section 30: Authorisation concerning data subject´s trade union membership

Section 31: Authorisation concerning data subject´s political persuasion

Section 32: Authorisation concerning data subject´s health and sex life.

Section 33: Authorisation concerning data subject´s criminal behaviour or biometric information.

9. How is the data controller and the data processor/operator defined?

ECTA Definition

"data controller" means any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject;

"data subject" means any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of this Act;

POPI Act Definitions

Information officer of, or in relation to a:

(a) public body means an information officer or deputy information as contemplated in terms of section 1 or 17; or

(b) private body means the head of a private as contemplated in section 1

Of the Protection of Access to Information Act.

Operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

10. What are the data protection principles and how are they defined?

POPI provides for eight conditions for lawful processing of personal information.

Condition 1: Accountability

Section 8: *Responsible party to ensure conditions for lawful processing.*

The responsible party must ensure that the conditions set out in this chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

Condition 2: Processing limitation

Section 9: *Lawfulness of processing.*

Personal information must be processed (a) lawfully and (b) in a reasonable manner that does not infringe the privacy of the data subject

Section 10: *Minimality*

Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

Section 11: *Consent, justification and objection*

Section 12: *Collection directly from data subject*

Condition 3: Processing limitation

Section 13: *Collection for specific purpose*

Section 14: *Retention and restriction of records*

Condition 4: Purpose specification

Section 15: *Further processing to be compatible with purpose of collection*

Condition 5: Information quality

Section 16: *Quality of information*

Condition 6: Openness

Section 17: *Documentation*

Section 18: *Notification to data subject when collecting personal information*

Condition 7: Security safeguards

Section 19: *Security measures on integrity and confidentiality of personal information*

Section 20: *Information processed by operator or person acting under authority*

Section 21: *Security measures regarding information processed by operator*

Section 22: *Notification of security compromises*

Condition 8: Data subject participation

Section 23: *Access to personal information*

Section 24: *Correction of personal information*

Section 25: *Manner of Access*

11. Does the law provide any specific definitions with regards to data protection in the digital sphere?

Chapter VIII of ECTA

Section 50(1) provides that these provisions only apply to personal information that has been obtained through electronic transactions.

- **Rights**

12. Is the data protection law based on fundamental rights (defined in Constitutional law or International binding documents)?

The ECTA does not specify any fundamental rights as a legal basis.

Popi Act it is based on the right to privacy enshrined in the Constitution of the Republic of South Africa, 1996.

13. What are the rights of the data subjects according to the law?

The rights of the data subject in POPI Act are described in terms of the obligations of the data controller, therefore see below.

Section 5: Rights of the data subject

Chapter 8: *Rights of Data subjects regarding Direct marketing by means of unsolicited electronic communications, directories and automated decision making*

Section 69 Direct Marketing by means of unsolicited electronic communication italicise this piece about chapter 8.

Section 70 Directories

Section 71 Automated Decision making

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

Principles for electronically collecting personal information

Section 51 of ECTA

(1) A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.

(2) A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.

(3) The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.

(4) The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.

(5) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.

(6) A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject.

(7) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.

(8) The data controller must delete or destroy all personal information which has become obsolete.

(9) A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

Chapter 3

(see above)

15. Is notification to a national regulator or registration required before processing data?

ECTA does not require prior notification or registration. According to Chapter 6, section 57 of POPI Act one must obtain prior authorisation. Section 55(1) of POPI Act also establishes duties and responsibilities for the Information Regulator.

16. Does the law require privacy impact assessment to process any category of personal data?

Not directly, however, section 40(1)(b)(vi) of POPI Act provides that the duties, powers and functions of a Regulator include monitoring and enforcing compliance by conducting an assessment in respect of the the processing of personal information by that private or public body for the

purpose of ascertaining whether or not the information is processed according to the conditions for the lawful processing of personal information.

17. What conditions must be met to ensure that personal data are processed lawfully?

See answer for question 10 above.

18. What are the conditions for the expression of consent?

Section 11 of POPI Act provides for the measures to be taken regarding consent, justification and objection to collection of personal data.

Section 51(4) of ECTA: The express written permission of the data subject is required unless the data controller is required or permitted to handle the data subject's data by law.

(4) The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.

19. If the law foresees special categories of data, what are the conditions to ensure the lawfulness of processing of such data?

Sections 26 – 33 (Chapter 3, Part B) of POPI Act provide for the measures to be taken when processing special personal information.

20. What are the security requirements for collecting and processing personal data?

Condition 7 in sections 19-22 (Chapter 3) of POPI Act provides for the security safeguards for processing personal information which includes protecting the confidentiality and integrity of personal information.

ECTA Definitions

(Chapter VIII) Section 51(5) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.

(Chapter VIII) Section 51(8) The data controller must delete or destroy all personal information which has become obsolete.

21. Is there a requirement to store certain types of personal data inside the jurisdiction?

Chapter 9 of POPI provides for transfers of personal information outside of the Republic. It provides in section 72 that a responsible party may not transfer personal information about a data subject to a third party who is in a foreign country unless it meets certain requirements set out in the section.

A responsible party may not transfer personal info outside South Africa to a foreign third party unless the third party is subject to law, corporate rules or binding agreements which afford the data subject protection:

- Data subject consents;
- Transfer is necessary for performance of a contract etc;

- Transfer is for the benefit of the data subject.

22. What are the requirements for transferring data outside the national jurisdiction?

See answer to question 21.

23. Are data transfer agreements foreseen by the law?

Yes, ***Section 72:*** Binding corporate rules/binding agreements with an adequate level of protection.

24. Does the relevant national regulator need to approve the data transfer agreements?

Yes, section 57 of POPI Act provides for circumstances where a responsible party would be required to obtain prior authorisation from the Regulator in terms of section 58.

25. What are the sanctions and remedies foreseen by the law for not complying with the obligations?

Chapter 11 of POPI Act provides for offences, penalties and administrative fines as contained in sections 100-109.

▪ Actors

26. What actors are responsible for the implementation of the data protection law?

The ECTA envisions cyber inspectors however, they are not specifically created for issues relating to data protection.

Section 39 of POPI Act provides for the establishment of the Information Regulator

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

The Minister of the Department of Telecommunications and Postal Services.

Section 39 *of POPI Act*

The Information Regulator is an in independent juristic person subject only to the Constitution and to the law. The Information Regulator must be impartial and perform its functions and exercise its powers without fear, favour or prejudice.

It must exercise and perform its functions in accordance with POPI and the Promotion of Access to Information Act.

It is accountable to the National Assembly.

28. What are the powers of the actors responsible for the implementation of the data protection law?

The Minister is responsible for overseeing all aspects of the ECT Act. His or her powers and duties are provided for in chapter II of the ECT Act.

Section 5 to 9: The minister must develop and implement a national e-strategy.

Section 40 *of the POPI Act*

The powers, of POPI provides for duties and functions of the Regulator in terms of this Act are:

(a) To provide education...

(b) to monitor and enforce compliance...

(c) to consult with interested parties…

(d) to handle complaints...

(e) to conduct research and to report to Parliament...

(f) to administrate codes of conduct

(g) to facilitate cross-border cooperation in the enforcement of privacy laws by participate in any initiative that is aimed at such cooperation

(h) to perform any general functions incidental or conducive to the preceding functions

2. Consumer Protection

▪ Scope

29. What national laws (or other type of normative acts) regulate consumer protection?

Electronic Communications and Transactions Act, 2002.

National Consumer Protection Act, 68 of 2008.

30. Is the country a party of any international consumer protection agreement?

No.

31. To whom do consumer protection laws apply?

Chapter VII of the ECTA makes provision for consumer protection. Section 42 sets out the scope of of application. It applies mostly to suppliers of consumer goods and services as well as to the consumers.

32. Do the laws apply to foreign entities that do not have physical presence in the country?

Section 47 of the ECTA provides that "the protection provided to consumers in this Chapter, applies irrespective of the legal system applicable to the agreement in question."

Section 5(8) provides that the provisions in the CPA apply to a matter irrespective of whether the supplier resides or has principal office within or outside the Republic.

▪ Definitions

33. How is consumer protection defined?

It is not defined in the ECTA Act.

The term consumer protection is not defined.

34. How are consumers defined?

"consumer" means any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

''consumer'', in respect of any particular goods or services, means:

(a) a person to whom those particular goods or services are marketed in the ordinary course of the supplier's business;

(b) a person who has entered into a transaction with a supplier in the ordinary course of the supplier's business, unless the transaction is exempt from the application of this Act by section 5(2) or in terms of section 5(3);

(c) if the context so requires or permits, a user of those particular goods or a recipient or beneficiary of those particular services, irrespective of whether that user, recipient or beneficiary was a party to a transaction concerning the supply of those particular goods or services; and

(d) a franchisee in terms of a franchise agreement, to the extent applicable in terms of section 5(6)(b) to (e);

35. How are providers and producers defined?

"certification service provider" means a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with a data message;

''producer'', with respect to any particular goods, means a person who:

(a) grows, nurtures, harvests, mines, generates, refines, creates, manufactures or otherwise produces the goods within the Republic, or causes any of those things to be done, with the intention of making them available for supply in the ordinary course of business; or

(b) by applying a personal or business name, trademark, trade description or other visual representation on or in relation to the goods, has created or established a reasonable expectation that the person is a person contemplated in paragraph (a); **''importer''**, with respect to any particular goods, means a person who brings those goods, or causes them to be brought, from outside the Republic into the Republic, with the intention of making them available for supply in the ordinary course of business; **"distributor",** in relation to any particular goods, means a person who, in the ordinary course of business— (a) is supplied with those goods by a producer, importer or other distributor; and (b) in turn, supplies those goods to either another distributor or to a retailer; There are no provisions specific to consumer protection in the definition. The CPA applies to all transactions therefore it would be understood that the rights enjoyed in the 'terrestrial' sphere would be enjoyed in the digital sphere.

36. Does the law provide any specific definitions with regards to consumer protection in the digital sphere?

The focus of the provision is to protect consumers in the case of electronic transactions regardless of whether the goods or services sold or bought online.

There are no provisions specific to consumer protection in the definition. The CPA applies to all transactions therefore it would be understood that the rights enjoyed in the 'terrestrial' sphere would be enjoyed in the digital sphere.

- **Rights**

37. Is the consumer protection law based on fundamental rights (defined in Constitutional law or International binding documents)?

The ECTA has not specified any fundamental rights.

The preamble of the CPA provides that it seeks to redress the injustices of Apartheid by developing and employing innovative means to:

(a) fulfil the rights of historically disadvantaged people and to promote their full participation as consumers;

(b) protect the interests of all consumers, ensure accessible, transparent and efficient redress for consumers who are subjected to abuse or exploitation in the marketplace; and

(c) to give effect to internationally recognised customer rights;

38. What are the rights of the consumer defined by the law with reference to digital good and services?

The ECT Act makes provisions for goods and services purchased through electronic transactions.

Section 43(2)

The consumer has the right to review the entire electronic transaction; to correct any mistakes; to withdraw from the transaction, before finally placing any order.

Section 43(3)

If the consumer does not provide the consumer with the information provided for in section 43(1) and the opportunity provided for in section 43(2), the consumer has the right to cancel the right to cancel the transaction within 14 days of receiving the good or services under the transaction.

Section 44(1)

It provides that a consumer is entitled to a cooling off period which means that he or she has the right to cancel without reason and without penalty any transaction and any related credit agreement for the supply of goods or services within seven days of conclusion of the agreement.

The consumer is also entitled to a full refund within 30 days of cancellation if the consumer made the payment before he or she could exercise the right of a cooling off period.

However, these rights do not apply to electronic transactions specified in section 42.

The CPA does not have specific provisions for digital goods and services therefore it is understood that all the rights that are afforded in the terrestrial sphere will be afforded to digital services.

Chapter 2: Fundamental Consumer Rights

Part A: Right of equality in consumer market

Part B: Consumer's right to privacy

Part C: Consumer's right to choose

Part D: Right to disclosure and information

Part E: Right to fair and responsible marketing

Part F: Right to fair and honest dealing

Part G: Right to fair, just and reasonable terms and conditions

Part H: Right to fair value, good quality and safety

Part I: Supplier's accountability to consumers

39. Is consumer protection law applicable to users of zero price service i.e. free of charges?

The ECT Act does not provided for this.

The CPA speaks of free goods and services only within the context of "promotional offers"

''promotional offer'' means an offer or promise, expressed in any manner, of any prize, reward, gift, free good or service, price reduction or concession, enhancement of quantity or quality of goods or services, irrespective of whether or not acceptance of the offer is conditional on the offeree entering into any other transaction.

- **Obligations and Sanctions**

40. Does the law establish specific security requirements to provide digital services or goods?

The ECT Act does not have specific security requirements but it does oblige the supplier to provide certain information provided for in **section 43.**

The CPA does not have specific provisions for digital goods and services therefore it is understood that all the rights that are afforded in the terrestrial sphere will be afforded to digital services.

41. What are the sanctions and remedies foreseen by the law for complying with the obligations?

Penalties

Section 111 provided for in terms of the CPA.

(1) Any person convicted of an offence in terms of this Act is liable:

(a) in the case of a contravention of section 107 (1), to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and imprisonment; or

(b) in any other case, to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and imprisonment.

(2) Despite anything to the contrary contained in any other law, a Magistrate's Court has jurisdiction to impose any penalty provided for in subsection (1).

Administrative fines

Section 112

(1) The Tribunal may impose an administrative fine in respect of prohibited or required conduct.

(2) An administrative fine imposed in terms of this Act may not exceed the greater of:

(a) 10 per cent of the respondent's annual turnover during the preceding financial year; or

(b) R1 000 000.

(3) When determining an appropriate administrative fine, the Tribunal must consider the following factors:

(a) The nature, duration, gravity and extent of the contravention;

(b) any loss or damage suffered as a result of the contravention;

(c) the behaviour of the respondent;

(d) the market circumstances in which the contravention took place;

(e) the level of profit derived from the contravention;

(f) the degree to which the respondent has co-operated with the Commission and the Tribunal; and

(g) whether the respondent has previously been found in contravention of this Act.

(4) For the purpose of this section, the annual turnover of a supplier at the time when an administrative fine is assessed, is the total income of that supplier during the immediately preceding year, as determined in the prescribed manner.

(5) A fine payable in terms of this section must be paid into the National Revenue Fund referred to in section 213 of the Constitution.

- **Actors**

42. What bodies are responsible for the implementation of the consumer protection law?

The ECT Act does not provide for specific bodies but the CPA does.

Chapter 5: National Consumer Protection Institutions

Part B

Establishment of National Consumer Commission

Part C

Functions of Commission

43. Is there a specific consumer protection body? If so, what is its administrative structure?

There is none under the ECA Act.

Section 85: (1) The National Consumer Commission is hereby established as an organ of state within the public administration, but as an institution outside the public service.

44. What are the powers of the bodies responsible for the implementation of the consumer protection law?

None are specified.

Chapter 5

Part C: Functions of Commission

Section 92: General provisions concerning Commission functions;

Section 93: Development of codes of practice relating to Act;

Section 94: Promotion of legislative reform;

Section 95: Promotion of consumer protection within organs of state;

Section 96: Research and public information;

Section 97: Relations with other regulatory authorities;

Section 98: Advice and recommendations to Minister.

3. Cybercrime

▪ Scope

45. What national laws (or other type of normative acts) regulate cybercrime?

The Electronic Communication and Transaction Act, 25 of 2002 regulate a handful of cybercrimes.

Cybercrimes Bill B6-2017

46. Is the country a part of any international cybercrime agreement?

Signatory/observer to the Budapest convention

47. What cybercrimes are regulated?

The ECTA provides for cybercrimes in sections 86, 87 and 88.

Section 86: Unauthorised access to, interception of or interference with data

Section 87: Computer-related extortion, fraud and forgery

Section 88: Attempt, and aiding and abetting

The Cybercrimes Bill provides for cybercrime in sections 2 to 13, 17-19

Section 2: Unlawful access

Section 3: Unlawful interception of data

Section 4: Unlawful acts in respect of software or hardware tool

Section 5: Unlawful interference with data or computer program

Section 6: Unlawful interference with a computer data storage medium or computer system

Section 7: Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device

Section 8: Cyber fraud

Section 9: Cyber forgery and uttering

Section 10: Cyber extortion

Section 11: Aggravated offences

Section 12: Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit offence

Section 13: Theft of incorporeal property

Section 17: Data message which incites damage to property or violence

Section 18: Data message which threatens persons with damage to property or violence

Section 19: Distribution of data message of intimate image

48. To whom do the laws apply?

The provision refers to a person which is defined as including a public body.

Any person who commits offences in chapter 2.

49. Do the laws apply to foreign entities that do not have physical presence in the country?

Yes, in accordance with ordinary criminal law and the principles of jurisdiction.

▪ Definitions

50. How is cybercrime generally defined by the national law?

A single definition for cybercrime is not provided in either the Cybercrimes Bill nor the ECTA.

51. What are the cybercrimes provided for by the law and how are they defined?

ECTA defines

Section 85: **"access"** includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.

Section 86: Unauthorised access to, interception of or interference with data.

86.

(1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.

(2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

(4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.

(5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

Section 87: Computer-related extortion, fraud and forgery

87.

(1) A person who performs or threatens to perform any of the acts described in section 86, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, is guilty of an offence.

(2) A person who performs any of the acts described in section 86 for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence.

Section 88: Attempt, and aiding and abetting

(1) A person who attempts to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in section 89 (1) or (2), as the case may be.

(2) Any person who aids and abets someone to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in section 89 (1) or (2), as the case may be.

NB These provisions are will be repealed by the Cybercrimes Bill if/when it comes into force. As provided for in chapter 2 and 3.

52. How is a computer system defined?

The ECT Act does not define it. The Cybercrimes Bill defines it in:

Chapter 1, Section 1:

‘‘computer system’’ means:

(a) one computer; or

(b) two or more inter-connected or related computers, which allow these inter-connected or related computers to:

(i) exchange data or any other function with each other; or

(ii) exchange data or any other function with another computer or a computer system;

53. How are computer data defined?

The definitions in the cybercrimes bill are: **“data”** means electronic representations of information in any form; **“data message”** means data generated, sent, received or stored by electronic means and includes-:

(a) voice, where the voice is used in an automated transaction; and (b) a stored record;

There is a definition of “computer data storage medium”

Chapter 1, Section 1:

‘‘computer data storage medium’’ means any device or location from which data or a computer program is capable of being reproduced or on which data or a computer program is capable of being stored by a computer system, irrespective of whether the device is physically attached to or connected with the computer system;

54. How are forensic data defined?

The ECT Act does not define Forensic Data.

It is not defined in the Cybercrimes Bill.

55. How are service providers defined?

The ECT Act does not define service provider.

The cybercrimes Bill only defines an electronic communication service provider.

Electronic communications service provider means any person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic

Communications Act, 2005;

56. Does the national law provide any other definitions instrumental to the application of cybercrime legislation?

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet;

"Internet" means the interconnected system of networks that connects computers around the world using the TCP/IP and includes future versions thereof.

''computer'' means any electronic programmable device used, whether by itself or as part of a computer system or any other device or equipment, or any part thereof, to perform predetermined arithmetic, logical, routing, processing or storage operations in accordance with set instructions and includes any data, computer program or computer data storage medium that are related to, connected with or used with such a device;

''computer data storage medium'' means any device from which data or a computer program is capable of being reproduced or on which data or a computer program is capable of being stored, by a computer system, irrespective of whether the device is physically attached to or connected with a computer system;

''computer program'' means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

''computer system'' means:

(a) one computer; or

(b) two or more inter-connected or related computers, which allow these inter-connected or related computers to:

(i) exchange data or any other function with each other; or

(ii) exchange data or any other function with another computer or a computer system.

57. Is there a way that cybercrimes can jeopardize the national security of a country?

An early version of the Cybercrimes Bill (the cybercrimes and cybersecurity bill) had provisions dedicated to addressing the natioal cybersecurity risks of cybercrime. See section on cyberdefence below.

▪ Rights

58. Is the cybercrime law based on fundamental rights (defined in Constitutional law or International binding documents)?

The ECT Act does not specify one.

The Cybercrimes Bill has not specified one nor is one immediately clear from the Constitution of the Republic of South Africa, 1996.

59. What are the rights of the victim and the accused?

The ECT Act does not specify them.

The Cybercrime Bill provides for rights and protections as consistent with the criminal law of South Africa.

▪ Procedures

60. Is there a specific procedure to identify, analyse, relate, categorize, assess and establish causes associated with forensic data regarding cybercrimes?

The Cybercrimes Bill does not provide specific procedures for this however, it provides in section 55 that the cabinet minister responsible for policing must (a) establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes; (b) ensure that members of the South African Police Service receive basic training in aspects relating to the detection, prevention and investigation of Cybercrimes.

61. In case of transnational crimes, how is cooperation between the national law enforcement agency and the foreign agents regulated?

The ECT Act does not provide for that but it refers to the general provisions for jurisdiction of the courts ***(Section 90)*.**

Chapter 6 of the Cybercrimes Bill provides for Mutual assistance.

62. Are there any exceptions to the use of mutual legal assistance procedure to investigate the crime?

The ECT Act does not provide for Mutual Legal Assistance.

Chapter 5 of the Cybercrimes Bill provides for Mutual Assistance National Executive may enter into agreements

57. (1) The National Executive may enter into any agreement with any foreign State regarding:

(a) the provision of mutual assistance and cooperation relating to the investigation and prosecution of… [the offences provided for in the Cybercrimes Bill]

This includes exceptions in accordance with the ordinary principles of mutual assistance.

63. Does the national law require the use of measures to prevent cybercrimes? If so, what are they?

Neither legislation provides for specific preventative measures that should be taken regarding cybercrime.

▪ Obligations and Sanctions

64. What obligations do law enforcement agencies have to protect the data of the suspect, the accused and the victim?

Chapter 5 of the Cybercrimes Bill provides for the powers to investigate, search an access or seize. The duties and responsibilities of law enforcement are outlined in this chapter.

65. What are the duties and obligations of the National Prosecuting Authorities in cases of cybercrime?

The general rules pertaining to the National Prosecution Authority would apply. The prosecutor must carefully check the legality of the initiation of criminal cases and evaluate the submitted materials.

Section 52 (5) The National Director of Public Prosecutions must make available members of the National Prosecuting Authority:

(a) who have particular knowledge and skills in respect of any aspect dealt with in this Act; and

(b) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994, to the satisfaction of the National Director of Public Prosecutions, to provide legal assistance to the designated Point of Contact as may be

National Director of Public Prosecutions must keep statistics of prosecutions

56. (1) The National Director of Public Prosecutions must keep statistics of the number of prosecutions instituted in terms of Part I or Part II of Chapter 2, the outcome of such prosecution and any other information relating to such prosecutions, which is determined by the Cabinet member responsible for the administration of justice. (2) The statistics or information contemplated in subsection (1) must be included in the report of the National Director of Public Prosecutions referred to in section 22(4)(g) of the National Prosecuting Authority Act, 1998.

66. Does the law impose any obligations on service providers in connection with cybercrime?

Chapter 9

S54 Electronic communication service providers or financial institutions that become aware that their systems are involved in the commission of any offences in the Cybercrimes Bill are obligated to report offences no later than within 72 hours. They must also preserve evidence as far as possible.

67. To which extent can a legal person be held liable for actions in connection with cybercrimes?

The ECT Act applies to "a person" which is defined to include a public body. Presumably, the ordinary meaning of a person is understood to apply, which is both a natural and a juristic person.

Person means a natural or juristic person, section 1. Penalties (section 14, 22) apply to persons.

▪ Actors

68. What bodies implement the cybercrime legislation?

Section 80 – 84 The Cyber Inspector provided for in chapter XII of the ECT Act.

s26 (1) The Cabinet member responsible for policing, in consultation with the National Commissioner, the National Head of the Directorate, the National Director of Public Prosecutions and the Cabinet member responsible for the administration of Justice.

69. Is there a special public prosecutor office for cybercrime? If so, how is it organised?

There is no special public prosecutor office. The Cabinet member responsible for policing is required to work closely the National Director of Public Prosecutions for all matters relating to public prosecutions of cybercrime. For example, see –

70. Does the cybercrime legislation create any specific body?

Chapter 10, Section 53

Cyber response committee

Chapter _ Section _ Designated Point of Contact

4. Public Order

▪ Definitions

71. How are public order, threats to public order and the protection of public order defined?

RICA concerns electronic communications surveillance. It does not refer to anything related to public order.

72. Is the protection of public order grounded in constitutional norms?

---

73. What kind of measures are foreseen limit constitutional and legal rights?

Cybersecurity incident management system…social management systems [e.g. social unrest management/monitoring or surveillance]

74. What measures are taken by the government to control mass gatherings of people?

Regulation of Gatherings Act (note Section 12(1)(a) is declared unconstitutional/invalid)

Proposed: Regulation of Gatherings Act Amendment Bill *(not related to cybersecurity)*

75. What public authorities are responsible for implementation of the surveillance techniques?

---

76. What are the right and obligations of these public authorities?

---

77. On what legal grounds non-governmental actors could perform mass surveillance?

A telecommunication service provider must store communication-related information (30(1) RICA).

78. Is the execution of the measures adopted in cases of instances delegated to private intermediaries or implemented by public bodies what are the responsibilities of those private bodies?

---

5. Cyberdefence

▪ Scope

79. Is there a national cyberdefence strategy or is cyberdefence mentioned in the national defence strategy?

The Cyberwarfare Strategy is still being developed. Once developed, it will be presented to the Justice, Crime Prevention and Security (JCPS) Cluster Ministers for approval. It is earmarked for approval and partial implementation in the 2018/2019 fiscal year.

80. What is the legal status of the national defence or cyberdefence strategy?

It is still being developed.

81. What national laws or other normative acts regulate cyberdefence in the country?

None.

82. Is the country party of any international cooperation agreement in the sphere of cyberdefence ?

No.

83. Does the national cyberdefence strategy provide for retaliation?

The Department of Defence Annual Performance Plan (2017) states that it is aligned with the national policy regarding South Africa's posture and capabilities related to offensive information warfare actions.

84. Is there any specific framework regulating critical infrastructure?

The National Critical Infrastructure Bill.

▪ Definitions

85. How are national security and national defence defined?

Not defined in the NCPF.

86. How are cybersecurity and cyberdefence defined?

"Cybersecurity" is the practice of making the networks that constitute cyberspace secure against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them.

"Cyberdefence" is not defined.

87. How are threats to national security and cyberthreats defined?

There is no single definition.

88. How is a cyberattack defined?

NCPF does not include a definition of cyberattack.

89. Does the national law provide any other definitions instrumental to the application of cyberdefence legislation?

NCPF Definitions

"Cyber warfare" means actions by a nation/state to penetrate another nation's computers and networks for purposes of causing damage or disruption

"Cyber espionage" means the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, Governments and enemies for personal, economic, political or military advantage

"Cyber terrorism" means use of Internet based attacks in terrorist activities by individuals and groups, including acts of deliberate large-scale disruptions of computer networks, especially computers attached to the Internet, by the means of tools such as computer viruses

"Cyberspace" means a physical and non-physical terrain created by and/or composed of some or all of the following

▪ National Framework

90. Is cyberdefence grounded on the constitutional provisions and/or international law?

It is not stated.

91. Which specific national defence measures are related to cybersecurity?

The Cybersecurity strategy is still being developed.

92. Is there a national defence doctrine and does the law or strategy refer to it?

National cyber security framework, introduction 1.1.

93. What measures are mentioned in the national law and strategy in order to implement cyberdefence ?

Cyber-warfare

"In order to protect its interests in the event of a cyber-war, a cyber defence capacity has to be built. The NCPF thus promotes that a Cyber Defence Strategy, that is informed by the National Security Strategy of South Africa, be developed, guided by the JCPS Cybersecurity Response Committee."

It says nothing more on the issue of cyberdefence .

94. How can Internet users' online activities be limited for the reasons of protection of national security and cyberdefence ?

The NCPF does not specify this.

95. Does the national law or strategy foresee any special regime to be implemented in case of emergency in the context of cyberdefence ?

The NCPF does not.

- **Actors**

96. What actors are explicitly mentioned as playing a role regarding cyberdefence in the law or national cyber defence strategy or defence strategy?

The Department of Defence and Military Veterans (DOD&MV) has overall responsibility for coordination, accountability and implementation of cyber defence measures in the Republic as an integral part of its National defence mandate. To this end, the Department will develop policies and strategies pursuant to its core mandate.

97. Is there a specific cyber defence body?

The NCPF envisions the implementation of the JCPS Cybersecurity Response Committee.

98. What are the tasks of aforementioned actors?

They will presumably be specified in the National Cybersecurity Strategy.

7. BRICS Countries to Build Digital Sovereignty

Luca Belli

Abstract

This concluding chapter elaborates on one of the first considerations of this book: Brazil, Russia, India, China and South Africa are home to 3.2 billion people, or 42% of the world's population, and this means BRICS hold 42% of one of the most valuable resources on the planet: the personal data produced by those 3.2 billion individuals. This chapter argues that the BRICS grouping is increasingly aware of the economic opportunities brought by digital technology but also that "free" digital services provided by foreign corporations are not free. They are paid with one of the most precious national assets – *i.e.* data – and, ultimately, with national sovereignty. Based on the research conducted by the CyberBRICS Project, this text contends that BRICS countries are developing cybersecurity frameworks, and particularly data privacy regulations, as a strategic tool to reassert their digital sovereignty.[441]

7.1. Introduction

As we stressed in the first pages of this book, Brazil, Russia, India, China and South Africa are home to 3.2 billion people, 42% of the world's population[442]. These demographic data have very concrete impact on digital environments, creating enormous challenges and opportunities. In effect, BRICS countries hold 42% of one of the most valuable resources on the planet: personal data. The grouping is not only increasingly aware that they are the main data producers in the world and that the more people are connected, the more their wealth increases.[443] They also increasingly understand that free digital services offered by foreign corporations are not really free. They are paid with data and, ultimately, with sovereignty.

This understanding has been maximised by the true "scramble for data"[444], launched by foreign tech businesses that, like digital colonizers[445], have been manifesting remarkable interest – especially as regards the Brazilian, Indian, and Chinese markets[446] – rushing to offer "free" digital services, over

[441] An early version of this concluding chapter was originally published in openDemocracy. See 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/>.

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

[443] Research developed by the World Bank has demonstrated that 10% increase in broadband penetration can result in a gross domestic product (GDP) growth of up to 3.2%, with benefits ranging from the generation of services and jobs to an increase in family income. See World Bank (2016)
The Organization for Economic Cooperation and Development(OECD) and the Inter-American Development Bank (IDB) have echoed such results stressing that the benefits of the expansion of Interne penetration, generates greater availability and efficient use of services provided over the Internet, fostering social inclusion and productivity, and strengthening national governance. See OECD & IDB (2017).

[444] See Belli (2017d).

[445] The concept of Data Colonialism is eloquently explored by Couldry and Mejias (2018 & 2019).

[446] A telling example illustrating the conspicuous interest of technology giants in BRICS markets is the very aggressive and unsuccessful attempt by Facebook to introduce so-called zero-rated services in India through the Internet.org and Free Basics

recent years. Such services, usually designed to be as addictive as possible[447], aim at capturing the user attention and drilling as much data as they can out of entire populations that are increasingly seen as potential data wells.

The research conducted by the CyberBRICS Project shows that BRICS countries are increasingly considering cybersecurity frameworks, with particular regard to data privacy regulations,[448] and other digital policies as an essential tool to curb the power of foreign technology companies[449] and reassert their sovereignty.[450]

Importantly, the raise of digital sovereignty is not only a BRICS-specific issue but a more general trend and, perhaps surprisingly, amongst the most vocal proponents of the reassertion of digital or technological sovereignty it is possible to find a number of high-ranking European leaders.[451] Besides the five cybersecurity dimensions that we analysed in this book, the regulation of Internet access infrastructure, digital platforms – particularly those utilised for the digitalisation of public services – and new technological developments such as artificial intelligence play a key role in the reassertion of national sovereignty in the digital environment and have a direct impact on cybersecurity. As mentioned, in the first chapter of this book, these issues are extremely relevant and will be specifically addressed by forthcoming CyberBRICS research that must be considered in conjunction with this study.

7.2. Digital Sovereignty

The push towards digital sovereignty is frequently criticised as a Trojan horse for authoritarian measures. This is an explanation, but it would be tremendously naïve to think it is the only one. By putting the CyberBRICS research – included here and in the various analyses available online – in

initiatives. Facebook's zero-rating projects, aimed at sponsoring a limited set of applications, whose data consumption is not counted against the users' data allowance, have been prohibited by the Telecom Regulatory Authority of India, TRAI. The regulator *de facto* barred Facebook's plan arguing that, by sponsoring access to only a limited amount of applications, zero rating plans violate net neutrality principles, and "can prove to be risky in the medium to long term as the knowledge and outlook of users would be shaped only by the information made available through those select offerings". See TRAI (2016). Importantly, the purpose of the majority of zero-rating plans such as the aforementioned Facebook initiatives is to steer users' attention towards predefined services, thus capturing users' attention and, consequently, their personal data. See Belli (2017a). Belli (2018:69).

[447] See Eyal (2014).

[448] See CyberBRICS (2019).

[449] See BRICS Ministers of Communication (2019).

[450] Dedicated analysis on BRICS policies and strategies to deploy and reclaim digital sovereignty will be the object of a future publication of the CyberBRICS project.

[451] In her Political Guidelines for the Next European Commission, the European Commission President Ursula von der Leyen argues that "it is not too late to achieve technological sovereignty" in some areas of critical technology, including algorithms, blockchain, and quantum computing. See von der Leyen (2019:13). This statement is echoed by French President, Emmanuel Macron, stressing that "the battle we're fighting is one of sovereignty…If we don't build our own champions in all areas—digital, artificial intelligence—our choices will be dictated by others." See Propp (2019).

perspective, it becomes increasingly evident that the reassertion of sovereignty in the digital environment is a fundamental angle allowing the reader to find a common rationale for adoption of the policy and regulations analysed in this book.

Cybersecurity entails the definition and implementation of measures allowing to exert effective control over the digital world. Such necessity has becoming especially relevant in recent years, in light of an ample range of technology-related scandals – epitomised by the Facebook-Cambridge Analytica scandal and the Snowden revelations – that have tellingly demonstrated that total and casual reliance on foreign technology and services can create substantial costs in terms of loss of control over personal data, opening the door to manipulation of people and democracies.[452]

Besides stimulating the so-called "techlash"[453], the aforementioned events have led policymakers to realise that the extraction of personal data by foreign companies and concentration of such data into the foreign servers can jeopardise national (cyber)security, thus stimulating the raise of cybersecurity and digital sovereignty in political agendas.

Furthermore, when one considers the substantial economic and strategic value of personal data and the fact that they are immaterial "goods", the exportation of which cannot be properly taxed, it becomes understandable that the massive collection of BRICS citizens' data and subsequent processing in foreign servers have also the potential to undermine national fiscal systems.[454]When data are collected locally but processed oversee, generating value at the moment of processing rather than at the collection, it is particularly challenging to fairly tax this "new asset class."[455]

The capacity to collect and analyse data massively is not only lucrative. It has become an incredibly strategic asset. In this context, the popularisation of "free" social networks, the automation of industry, the advent of the Internet of Things and Smart Cities sound like truly fantastic innovations. But only if smartphone, factories, and all objects and infrastructures do not become tools for hacking, spying, meddling, and draining data out of digitally colonised countries.

From Beijing to Brasilia, the need to reassert control on the technology that is making our lives both easier and more fragile is therefore becoming a priority. As the 2019 BRICS Summit[456] unfolded in Brasilia, digital economy, cybersecurity, and cooperation on science, technology and innovation emerged as key issues around which BRICS leaders are building further synergy. The national frameworks scrutinised in this book and the most recent BRICS declarations expressively demonstrate

[452] As an instance, see the European Data Protection Supervisor's opinion on online manipulation and personal data (EDPS 2018).

[453] This term refers to a general mistrust of consumers and regulators regarding the activities and intentions of – especially large-sized and US-based – technology companies.

[454] See European Parliament (2019).

[455] See WEF (2011).

[456] See BRICS (2019c).

that BRICS leaders see digitalisation as new opportunity to enhance their cooperation "and expand and intensify partnerships already in progress including taking necessary steps for early setting up of the Digital BRICS Task Force."[457] At the same time, the grouping's leaders are well-aware that, when cybersecurity frameworks are nor effective and digital technology is not regulated, it can be exploited to undermine national sovereignty.

7.3. Serious Concerns

Half of these five countries' population is already online[458], contributing significantly to domestic and international economic activity[459]. The countries are working to welcome digital innovation[460], while sounding an alarm about cybersecurity and personal control of personal data. The governments are also aware that as more of their people come online, developing countries' national security and even sovereign power[461] may be at risk of hackers and foreign adversaries.

As a telling example in this sense, one can consider that, as recently as June 2019, the New York Times reported the US Cyber Command was stepping up "digital incursions" into Russia's electric power grid.[462] The clear provision – and open statement – that the US Cyber Command enjoys powers to "conduct clandestine military activity to deter, safeguard or defend against attacks"[463] illustrates that cyber operations can and are utilised for offence and intrusion purposes into any potentially vulnerable foreign systems. In this context, it is essential to consider that any digital service and connected system can be vulnerable to cyberattacks and, therefore, sound cybersecurity strategies and frameworks become an essential need.

As a result of such scenario, many of the BRICS nations are massively investing in their digital capabilities while developing legislation on "Internet sovereignty"[464], crafting new data protection frameworks and increasingly requiring tech companies to store data about a person in that person's home country[465]. Such policy and regulatory initiatives are becoming necessary as the BRICS – as

[457] See *ibid*., paragraph 53.

[458] See https://www.internetworldstats.com/stats.htm

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

[460] A variety of strategies, policies and programmes promoted by both public and private stakeholders in the BRICS have been discussed during a series of dedicated CyberBRICS events, analysing *i.a*. 5G and new digital infrastructures, data protection, cybersecurity frameworks, and Sino-Brazilian cooperation on Internet Governance. Detailed information, including video recordings of the seminars, are available at https://www.cyberbrics.info/category/events/

[461] See Borger (2013).

[462] See Sanger and Perlroth (2019).

[463] See *Idem*.

[464] For an analysis of the Russian Internet Sovereignty Law, see Shcherbovich (2019a & 2019b).

[465] For a discussion of the Indian policies aimed at sovereign control of data, see Basu, Hickok and Chawla (2019). See also the Russian, Chinese and Indian analyses in this book for a wider analysis and contextualisation of data localisation norms in those countries.

well as other countries – increasingly digitalise their economies, administrations and societies. Indeed, while risks determined by digital technology must be taken into account and minimised, BRICS leaders have realised that the ongoing digitalisation processes that they are steering have the potential to enormously reduce poverty, increasing the standards of life, providing access to knowledge and work opportunities to almost one and a half billion individuals.

7.4. Major Potential

The five BRICS countries are not turning away from technology's potential to make businesses more efficient[466], governments more accountable and give citizens cheaper communications, smoother transportation, more reliable electricity and cleaner environments[467].

China has the most ambitious approach of the five, making major investments in 5G networks, artificial intelligence[468] and high-tech manufacturing in a bid to be an even larger global technology power than it already is. Russia, close behind, is planning to serve 80% of its population with 5G wireless broadband Internet[469] service by 2025.

Brazil's efforts are more recent, but it has begun to computerise its government operations[470] and recently approved a plan aimed at boosting the adoption of the Internet of Things to automate industry[471]. After having approved the Internet Rights Framework (better known as *Marco Civil da Internet*) in 2014 and a new General Data Protection Law[472] in 2018, the tropical giant is now aiming at new business opportunities and improvement of productivity.

India is, at the time of this writing, finalising the adoption of a new Data Protection legislation while South Africa is crafting a series of policies aimed at reaping the benefits of the Fourth Industrial Revolution, a subject that, under the South African Presidency, was chosen as the overarching theme of 10th BRICS Declaration, issued at the conclusion of the 2018 Summit, in Johannesburg.[473]

[466] See ITU (2016).

[467] See ITU (2016).

[468] See South China Morning Post (2020).

[469] See Russian Business Today (2018).

[470] See Ministério da Ciência, Tecnologia, Inovações e Comunicações (2018).

[471] See Ministério da Ciência, Tecnologia, Inovações e Comunicações (2019).

[472] The CyberBRICS team elaborated an unofficial English translation of the new General Data Protection Law, better known by its Brazilian acronym "LGPD". See Belli *et al.* (2020).

[473] See BRICS (2018).

Critically, without modern and robust cybersecurity frameworks, the rights of 3.2 billion individuals may be at risk, businesses would face juridical uncertainty, and the digital dreams of the five developing nations could turn into real nightmares.

7.5. Giant Challenges for Giant Countries

The governments of the BRICS nations clearly understand that each of their citizens is a producer of personal data that, combined, are immensely valuable, and know that strong cybersecurity frameworks are key to protecting this economic resource. This is part of the reason India is so insistent on having data about Indian citizens stored on computers within India[474], rather than overseas. This also partly explains why Russia adopted Sovereign Internet Law[475], earlier this year, and updated its data protection legislation, introducing data localisation provisions, in 2017.

Although it is likely that sovereignty and business considerations, rather than fundamental rights ones, are at the origin of the various cybersecurity policy-elaboration efforts in the BRICS, it is undeniable that the establishment of sound regulations foster the protection of individual rights and the establishment of more sustainable digital environments. This consideration is becoming increasingly popular amongst the billions of people in the BRICS and many individuals are beginning to understand the potential value of their data, the need to regulate how they are used and prevent misuse, demanding high standards for data protection[476].

In China, a consumer rights protection organisation sued Baidu for collecting user data without consent.[477] In South Africa, the Information Regulator has just cautioned that large scale CCTV surveillance can violate privacy and contravene the Protection of Personal Information Act[478]. In addition to demanding bolder protection of their rights, consumers in around the world are starting to realise the importance of retaining control[479] over personal data, looking for more privacy enhancing technologies. In this perspective, improved cybersecurity becomes an asset to win competition in BRICS and non-BRICS countries alike.

Moreover, it is worth noting that BRICS countries are, simultaneously, amongst the most frequent targets of cyberattacks[480] but also some of the countries from which most cyberattacks

[474] See Basu, Hickok and Chawla (2019).

[475] See Shcherbovich (2019a & 2019b).

[476] See Samm (2019).

[477] See Wei (2019).

[478] See Mungadze (2019).

[479] For a perspective on the growing importance of data control in the Brazilian context, see Belli (2017b & 2017c). For a wider discussion of the concept of "data control by design" and its relevance to preserve individual rights to data protection online, see Belli, Schwartz & Louzada (2017).

[480] See Cybersecurity Insiders (2019).

originate[481]. The economic opportunities –in terms of both new markets and reduced costs due to potential attacks – and the strategic status of cybersecurity are jointly contributing to the elevation of this issue to the top of the BRICS governments' agendas.[482].

The findings of the CyberBRICS Project's research show that BRICS countries face common challenges. BRICS can also collaborate to develop shared, or at least compatible solutions. The elaboration and implementation of sound cybersecurity frameworks is a clear example of a quintessentially common problem that would immensely benefit from compatible and convergent policies. To this extent, the mapping exercise developed by this book is an essential tussle in order to allow the emergence of a new comparative approach identifying existing similarities and highlighting where BRICS countries would benefit from further convergence and cooperation.

However, it is also important to stress that policy making is only part of the work lying ahead. A monumental effort still must be done in terms of building digital capacities of BRICS nationals. People in the BRICS will only enjoy a strong and homogeneous level of protections and secure digital environment if their digital literacy is enhanced, while convergent digital policies are adopted by their leaders.

7.5. Enhanced Cooperation for Compatible Digital Policies

As the pioneering experience of the CyberBRICS project demonstrates, many digital policy elements are already spontaneously converging[483]. This is the case, for instance, of core data protection principles and rules[484]. Analysing existing regulation is paramount if we want to understand what elements of digital policies are already compatible. It is even more relevant in identifying good practices and proposing sustainable and fair solutions.

In recent years, BRICS governments have consistently stressed the value of enhanced cooperation on research and technological development and acknowledged the key role that research plays for their sustainable development and for their digital transformation.

To live up to their expectations, they should stimulate a virtuous circle of research and policy proposal, supporting the establishment of a BRICS cooperation mechanism aimed at fostering compatible digital policies. This is what BRICS leaders are aiming at by establishing the new BRICS Science,

[481] See https://cybermap.kaspersky.com/

[482] For instance, Brazil has currently developing a new cybersecurity strategy in compliance with Decree No. 9,637, of 26 December 2018, establishing the National Information Security Policy. See http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm#art6i

[483] As an instance, see the CyberBRICS interactive map comparing Data Protection across BRICS countries https://cyberbrics.info/data-protection-across-brics-countries/

[484] See *Idem*.

Technology and Innovation Work Plan 2019-2022[485] and the BRICS STI Architecture,[486] described in the first chapter of this book, as well as the setting up of the Digital BRICS Task Force,[487] mentioned above.

Modern and compatible frameworks are needed to protect individual rights and provide legal certainty for businesses. Given the BRICS appetite for 5G and IoT and data-angry technologies, cybersecurity could be a suitable testbed[488] to start enhancing digital policy cooperation and concretely implement the aforementioned initiatives.

In the absence of such cooperation, the reality of the policy elaboration may remain distant from the policy declarations. As this book demonstrates, the impact of an enhanced BRICS digital cooperation is potentially immense. The hope of this author is that this book will be a valuable support to the understanding and further exploration of the policies and regulations that will shape the next decade of digital evolutions: those of the BRICS.

7.6. References

Basu, Arindrajit, Hickok Elonnai & Chawla Aditya Singh (23 March 2019). **Unpacking policy moves for sovereign control of data in India.** <https://cyberbrics.info/unpacking-policy-moves-for-sovereign-control-of-data-in-india/>

Belli, Luca. (2017a). Net Neutrality, Zero-Rating and the Minitelisation of the Internet. Journal of Cyber Policy. Routledge. Vol 2. N 1.

Belli, Luca. (01 June 2017b). **Seus dados são o novo petróleo: mas serão verdadeiramente seus?** O Globo. <https://oglobo.globo.com/opiniao/seus-dados-sao-novo-petroleo-mas-serao-verdadeiramente-seus-21419529>

Belli, Luca. (14 October 2017c). Os dados pessoais e os escravos digitais. Nexo Jornal. <https://www.nexojornal.com.br/ensaio/2017/Os-dados-pessoais-e-os-escravos-digitais>

Belli, Luca. (15 Dec 2017d). **The scramble for data and the need for network self-determination.** In Open Democracy Available at: < https://www.opendemocracy.net/en/scramble-for-data-and-need-for-network-self-determination/>.

Belli, Luca. (2018). Zero-Rating and the Minitelisation of the Internet. In ARCEP (Autorité de régulation des communications électroniques et des Postes). The state of the Internet in France. <https://archives.arcep.fr/uploads/tx_gspublication/report-state-internet-2018_conf050618-ENG.pdf>

Belli, Luca. (09 Set 2019). **5G e IoT: BRICS precisam de cooperação em cibersegurança.** <https://cyberbrics.info/5g-e-iot-brics-precisam-de-cooperacao-em-ciberseguranca/>

[485] See BRICS (2019b).

[486] See BRICS (2019a).

[487] See *Idem*.

[488] See Belli (2019).

Belli, Luca, Laila Lorenzon, Luã Fergus and Walter Britto (January 2020). The Brazilian General Data Protection Law (LGPD). Introduction to LGPD and Unofficial Translation. CyberBRICS Project at FGV Law School. https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/

Belli, Luca. Schwartz Molly, Louzada Luiza, (2017). Selling your Soul while Negotiating the Conditions: From Notice and Consent to Data Control by Design. In Health and Technology Journal. Vol 5. N° 4. Springer-Nature. https://link.springer.com/article/10.1007/s12553-017-0185-3

Borger, Julian. (24 Sep 2013). **Brazilian president: US surveillance a 'breach of international law'**. The Guardian. Available at: <https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance>.

Brazilian Presidency of the BRICS. (2019). What is BRICS? http://brics2019.itamaraty.gov.br/en/about-brics/what-is-brics

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

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

BRICS. (November 2019c) Brasília Declaration. 11th BRICS Summit http://brics2019.itamaraty.gov.br/images/documentos/Braslia_Declaration_-_hiperlinks_como_est_no_site_28-11.pdf

BRICS. Ministers of Communication (2019). **Declaração da 5º Reunião de Ministros de Comunicações do BRICS - Brasília, Brasil, 14 de Agosto de 2019.** <http://brics2019.itamaraty.gov.br/images/documentos/Declarao_da_5_Reunio_de_Comunicao_dos_Ministros_do_BRICS.pdf>.

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

CyberBRICS (04 June 2019). **Seminar CyberBRICS: Cybersecurity, data protection and the digital future of the BRICS.** Available at: <https://cyberbrics.info/seminar-cyberbrics-cybersecurity-data-protection-and-the-digital-future-of-the-brics-2/>.

Cybersecurity Insiders. **List of countries which are most vulnerable to cyber attacks. Available** at: <https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/>.

Couldry, Nick and Mejias, Ulises. (2018) Data colonialism: rethinking big data's relation to the contemporary subject. Television and New Media. https://journals.sagepub.com/doi/10.1177/1527476418796632

Couldry, Nick and Ulises A. Mejias. (2019). The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism. Stanford University Press.

European Data Protection Supervisor (2018). **EPDS opinion on online manipulation and personal data.** Available at: <https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf>.

European Parliament (2019). **Impact of digitalisation on international tax matters.** <https://www.europarl.europa.eu/cmsdata/161104/ST%20Impact%20of%20Digitalisation%20publication.pdf>.

Eyal, Nir (2014). **Hooked: How to Build Habit-Forming Products**. Penguin Random House.

FGV Direito Rio (30 Aug 2019). **5G and the new digital infrastructures in the BRICS.** Available at: <https://direitorio.fgv.br/eventos/5g-and-new-digital-infrastructures-in-the-brics>.

Governo do Brasil. **Gabinete de segurança institucional**. Available at: <https://www.gov.br/gsi/pt-br>.

International Communication Union (2016). **Harnessing the Internet of things for global development.** Available at: <https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf>.

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

Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) (2018**). Brazilian digital transformation strategy**. Available at: <https://www.mctic.gov.br/mctic/opencms/digital_strategy>.

Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) (26 June 2019). **Decreto que institui plano nacional de Internet das coisas é publicado.** Available at: <https://www.mctic.gov.br/mctic/opencms/salaImprensa/noticias/arquivos/2019/06/Decreto_que_institui_o_Plano_Nacional_de_Internet_das_Coisas_e_publicado.html>.

Mungadze, Samuel. (16 September 2019). Information Regulator cautions private camera network operators. ITweb. https://www.itweb.co.za/content/kYbe9MXxPxdMAWpG

OECD (Organization for Economic Cooperation) and IDB (Development and Inter-American Development Bank). (2017). Broadband Policies for Latin America and the Caribbean: A Digital Economy Toolkit. Available at: http://www.oecd.org/internet/broadband-policies-for-latin-america-and-the-caribbean-9789264251823-en.htm

Propp, Kenneth (11 December 2019). Waving the flag of digital sovereignty. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/

Russia Business Today (30 Oct 2018). **Russia to reach 80% 5G covereage by 2025: report.** Available at: <https://russiabusinesstoday.com/technology/russia-to-reach-80-5g-coverage-by-2025-report/>.

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

Sanger David E. & Perlroth Nicole (15 June 2019). **U.S. escalates online attacks on Russia's power grid.** The New York Times. Available at: <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?smid=nytcore-ios-share>.

Shcherbovich, Andrey A. (27 Fev 2019a). **The Russian bill on Internet Sovereignty adopted by the State Duma in first reading.** Available at: <https://cyberbrics.info/the-russian-bill-on-internet-sovereignty-adopted-by-the-state-duma-in-first-reading/>.

Shcherbovich, Andrey A. (05 May 2019b). **Sovereign Internet Law signed by the President of Russia.** Available at: <https://cyberbrics.info/sovereign-internet-law-signed-by-the-president-of-russia/>.

South China Morning Post (2020). **Made china 2025**. Available at: <https://www.scmp.com/topics/made-china-2025>.

TRAI (Telecom Regulatory Authority of *India)*. February 2016. Prohibition of Discriminatory Tariffs for Data Services regulation, 2016. No. 2 of 2016. February 2016.

von der Leyen, Ursula (July 2019). A Union that strives for more. My agenda for Europe. Political Guidelines for the Next European Commission 2019-2024. https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

World Bank. (2016). World Development Report 2016: Digital Dividends. Washington, DC: World Bank. Available at: http://pubdocs.worldbank.org/en/391452529895999/WDR16-BPExploring-the-Relationship-between-Broadband-and-Economic-Growth-Minges.pdf

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

Wei, Han (9 January 2019). Baidu Sued Over Claim It Illegally Obtained Users' Data. Caixin. https://www.caixinglobal.com/2018-01-09/baidu-sued-over-claim-it-illegally-obtained-users-data-101195257.html